Records Management Journal

Information governance and ethics: information opportunities and challenges in a shifting world

Lead Guest Editors: Elizabeth Lomas and Basma Makhlouf Shabou
Assistant Guest Editor: Arina Grazhenskaya
Records Management Journal aims to facilitate the transfer of research findings and innovation in all aspects of records management into good practice. This refereed journal strives to publish research results, case studies and critical comment of value to records educators, students and professionals in both public and private sector organizations throughout the world.

GUEST EDITORS
Elizabeth Lomas
Department of Information Studies, University College London, London, UK
Basma Makhlouf Shabou
Department of Information Sciences, Geneva School of Business Administration, Geneva, Switzerland
Arina Grazhenskaya
Department of Information Sciences, Geneva School of Business Administration, Geneva, Switzerland

CO-EDITORS
Dr Fiorella Foscarini
Associate Professor, Faculty of Information, University of Toronto, Canada
E-mail fiorella.foscarini@utoronto.ca
Dr Elizabeth Lomas
University College London, UK
E-mail e.lomas@ucl.ac.uk

CONSULTING EDITOR
Dr Julie McLeod
Professor of Records Management, iSchool, Northumbria University, Department Mathematics & Information Sciences, Room 043, Pandon Building, Newcastle Upon Tyne, NE2 1XE, UK
E-mail julie.mcleod@northumbria.ac.uk

ISBN 978-1-78973-925-1
ISSN 0956-5698
© 2019 Emerald Publishing Limited

Guidelines for authors can be found at:
www.emeraldgrouppublishing.com/rmj.htm

Records Management Journal is indexed and abstracted in:
ABII/INFORM
ABII/INFORM Complete
ABII/INFORM Global
Business Source Alumni Edition
Business Source Complete
Business Source Premier
Computer Science Index
Computers and Applied Sciences Complete
Current Abstracts
Current Awareness Abstracts
Discovery
Emerald Management Reviews
INSPEC
Library and Information Science Abstracts
Library, Information Science and Technology Abstracts (LISTA)
Professional ABII/INFORM Complete
Professional ProQuest Central
ProQuest Central
ProQuest Curriculum Essentials
ProQuest Health Management
ProQuest Library Science
ProQuest Pharma Collection
TOC Premier

Emerald Publishing Limited
Howard House, Wagon Lane,
Bingley BD16 1WA, United Kingdom
Tel +44 (0) 1274 777700; Fax +44 (0) 1274 785201
E-mail emerald@emeraldinsight.com

For more information about Emerald’s regional offices please go to http://www.emeraldgrouppublishing.com/offices

Customer helpdesk:
Tel +44 (0) 1274 785278; Fax +44 (0) 1274 785201
E-mail support@emeraldinsight.com

Orders, subscription and missing claims enquiries:
E-mail subscriptions@emeraldinsight.com
Tel +44 (0) 1274 777700; Fax +44 (0) 1274 785201

Missing issue claims will be fulfilled if claimed within six months of date of despatch. Maximum of one claim per issue.

Hard copy print backsets, back volumes and back issues of volumes prior to the current and previous year can be ordered from Periodical Service Company.
Tel +1 518 537 4700; E-mail psc@periodicals.com
For further information go to www.periodicals.com/emerald.html

Reprints and permissions service
For reprint and permission options please see the abstract page of the specific article in question on the Emerald web site (www.emeraldinsight.com), and then click on the “Reprints and permissions” link. Or contact:
E-mail permissions@emeraldinsight.com

The Publisher and Editors cannot be held responsible for errors or any consequences arising from the use of information contained in this journal; the views and opinions expressed do not necessarily reflect those of the Publisher and Editors, neither does the publication of advertisements constitute any endorsement by the Publisher and Editors of the products advertised.

No part of this journal may be reproduced, stored in a retrieval system, transmitted in any form or by any means electronic, mechanical, photocopying, recording or otherwise without either the prior written permission of the publisher or a licence permitting restricted copying issued in the UK by The Copyright Licensing Agency and in the USA by The Copyright Clearance Center. Any opinions expressed in the articles are those of the authors. Whilst Emerald makes every effort to ensure the quality and accuracy of its content, Emerald makes no representation implied or otherwise, as to the articles’ suitability and application and disclaims any warranties, express or implied, to their use.

Emerald is a trading name of Emerald Publishing Limited
Printed by CPI Group (UK) Ltd, Croydon, CR0 4YY

FSC 10313604
Guest editorial

Information governance and ethics – information opportunities and challenges in a shifting world: setting the scene

The information governance context

Information governance (IG) is a multidisciplinary approach to managing information, which has emerged over the past decade and continues to develop. With the rise of new technologies, we have seen the value of information receiving greater prominence and increasingly being commoditized (World Economic Forum, 2011). Information is now often co-created across global boundaries and blurred personal and public spaces, with complex ownership and legal regimes impacting. In response, frameworks to underpin the delivery of information through time have increasingly acknowledged the diversity of professional expertise needed to support a wide range of information contexts, including, for example, archivists, digital curators, digital forensics experts, IT support, lawyers, librarians, records managers, software engineers and technical infrastructure engineers (Makhlouf Shabou et al., 2017). Some frameworks have re-envisioned their profession and rebranded it IG, e.g. COBIT 5 (ISACA, 2012), which aligns the IT sector with information security, and the ARMA Information Governance Maturity Model, which aligns records management with IG (ARMA International, 2010). Others have perhaps underplayed the role of IG, representing it only as a niche component of information delivery, for example, the CILIP Professional Knowledge and Skills Base model defines IG as delivery within the information rights law space (CILIP, 2019), which does denote its significance for legal and ethical information delivery. While each of these models articulates a valuable aspect of IG delivery, it is important not to ignore the bigger implications of IG. IG is an overarching domain that acknowledges wide-ranging needs and complex relationships to manage information for the benefit of society.

The evolution of information governance

The roots of IG lie in corporate governance agenda, which sought to ensure ethical frameworks for managing organizations (Willis, 2005, p.86-87). However, IG grew and evolved as the value of information as an asset was increasingly recognized from the 1990s, as established in the work of Robert Hawley’s KPMG IMPACT Committee (KMPG, 1995). New technologies have enhanced its value exponentially in the twenty-first century, and in turn this has exposed information to new cyber risks, highlighting the need for information security systems. In 2010, Lomas made the case for records management and information security agenda to be aligned under the banner of IG, ARMA developed an ARMA Information Governance Maturity Model and Deborah Logan (2010) wrote a powerful Gartner blog post developing corporate governance agenda to take account of the role and value of information:

Information governance is the specification of decision rights and an accountability framework to encourage desirable behavior in the valuation, creation, storage, use, archival and deletion of information. It includes the processes, roles, standards and metrics that ensure the effective and efficient use of information in enabling an organization to achieve its goals.

From 2011, Lomas provided masters-level IG teaching at Northumbria University, and Kerstin Ferguson-Boucher taught IG at Aberystwyth University; there is now a plethora of IG training and education on offer throughout the world. New bodies have evolved,
including the Information Governance Initiative (IGI), which acts as a leading IG “think tank.” In 2014, Smallwood and MacLennan provided separate texts on the subject of IG. A report published by the IGI in 2018 has evidenced the growth of IG roles crossing over domains, including analytics, audit, big data, business intelligence, business operations and management, compliance, data curation and stewardship, data governance, data science, data storage and archiving, e-discovery, enterprise architecture, finance, informatics, information security and protection, IT management, knowledge management, legal, master data management, privacy, records and information management and risk management (IGI, 2018, p. 17).

The themed issues on information governance
IG is still an emerging and conflicted space, with significant gaps in the delivery in practice. The editors of these two themed IG Records Management Journal issues have noted in their own research the need to extend the ethical delivery of IG and the complexity of IG (Makhlouf-Shabou et al., 2019). This is difficult when working in global spaces with different perspectives on national security and openness, citizen freedom and privacy and ownership. The articles delivered within these two themed issues on IG provide a platform for further discussion, developing and in some instances debating differing perspectives. The works are set across different national borders and contain academic and practitioner perspectives. They provide a strong discussion of the literature in this domain, as well as the underpinning definitions and complexities of IG delivery. We see discussions on professional/discipline boundaries, for example, between information security and records management (e.g. Brooks and Xie). In addition, we see discussions on national cases in terms of differences and synergies, for example, in respect of archival, appraisal, deletion and e-discovery decisions in China, South Africa, Sweden, the UK and the USA (e.g. Fan, Klett, Lappin, Netshakhuma, Odezimir and Xie). The roles within organizations and the expectations of stakeholders are further discussed, including aspects of culture and leadership at organizational and national levels (Daneshmandnia, Kabata, Mpho, et al.). The articles discuss accountability, openness and trust (e.g. Svärd, Shepherd et al. and Engvall), as well as the need for greater co-creation and participatory practices in complex spaces, including around the generation of records and captured memories for children in care (Evans et al. and Thiari). The challenge of new technologies are considered in a number of articles and specifically in the context of Blockchain by Hofman et al. In addition, Upward provides some new philosophical perspectives, repositioning the continuum within IG thinking. These articles challenge assumptions and argue for further research and debate in this sphere.

The future
Looking forward, as noted by Daneshmandnia, to date, models for IG have been limited to specific contexts and need extension; they have perhaps been too organizationally focused. In addition, as noted by Evans et al., there have been limits in terms of the extent to which co-creation has been enabled to generate information/records. As new technologies change our world, bigger ethical visions must be forged, taking into account old and emerging dangers. The holistic nature of IG provides opportunities to deliver frameworks that balance needs to ensure that advancement is not at the expense of society and to try to reach desperately needed international consensus and legal agreement. The articles within this issue demonstrate the complex and diverse nature of IG. To meet this challenge, the editors would posit a broader definition of IG in 2019 as:
Information governance provides a holistic ethical framework which takes into account a range of societal and individual stakeholder information needs. It enables a just process of information co-creation, sharing, management, ownership and rights including retention and deletion rights, economics, accountability and openness considering confidentiality, privacy and security needs. It transcends organizational, national and technological boundaries but takes into account diverse cultural, individual/family, community, organizational and societal needs. It is supported in its delivery by a range of practitioner expertise and citizen engagement.

Elizabeth Lomas

Department of Information Studies, University College London, London, UK, and

Basma Makhlouf Shabou and Arina Grazhenskaya

Department of Information Sciences, Geneva School of Business Administration,

Geneva, Switzerland

References

ARMA International (2010), Information Governance Maturity Model, ARMA, KS.

Further reading

Perspectives on the relationship between records management and information governance

Julie Brooks
School of History, University College Dublin, Dublin, Ireland

Abstract

Purpose – The increasing prominence of the use of the term information governance (IG) raises fundamental questions about the role and relevance of records management in today’s organisations. As a starting point, this paper aims to explore the relationship between records management and IG by considering both recordkeeping and non-recordkeeping perspectives.

Design/methodology/approach – The research discusses literature chiefly from 2013 to the present to shed light on how discussion of the relationship between records management and IG has evolved over the past few years.

Findings – A range of perspectives on the relationship between records management and IG was evident and, notably, a lack of direct engagement from the records management community. Taking the positive perspectives that emerged, IG was seen as an opportunity for records management. By contrast, others regarded it as a necessary successor to records management, the latter perceived as too associated with the paper era to be capable of meeting the organisational information needs of today. Equally, others were sceptical about the real difference IG offered, suggesting it was in part a rebranding exercise, which did not necessarily articulate anything fundamentally new.

Originality/value – Defining literature in the broadest sense, this paper offers a high-level review of some of the recent discussions that have taken place in a wide variety of contexts around the relationship between records management and IG. It includes journal articles, books, online discussions from professional forums and listservs, vendor contributions, opinion-pieces and blogs and in particular focuses on presenting a range of viewpoints from individuals operating within various information-related spaces, including records and information management, IG, and information technology. It is hoped that this preliminary research will encourage further engagement on the subject from recordkeeping professionals.

Keywords Information management, Records management, Information governance

Introduction

This review explores perspectives on the relationship between records management and information governance (IG) using contemporary literature from both recordkeeping[1] and non-recordkeeping perspectives following on from research by Hagmann (2013) exploring, “the still immature concept of IG from a records and information management perspective”. Suggesting that IG was becoming “a trendsetting container for capturing almost everything and nothing in the world of information management”, he considered the issue of “whether IG is just the newest buzzword or if it is actually becoming a new paradigm that will change the face of RIM.” This research analyses literature from around that time to the present to shed light on how opinions on the relationship between records management and IG have since evolved and aims to contribute to wider discussions about the role and relevance of records management in an increasingly broad information landscape. What impact, if any, has IG as a concept and an approach on the professional roles and boundaries of records...
professionals. Is it, as some suggest, a strategic enabler for records management, a natural and necessary evolution that better integrates the management of organisational records and other information assets, or is IG simply a passing buzz concept that can mean many things to many people?

Methodology
This review aimed to explore perspectives from records professionals and those outside the recordkeeping profession. Initial keyword searches using the terms “records management” and “information governance” were carried out using University College Dublin Library’s OneSearch and Google Scholar. These search terms yielded large amounts of literature, much of which was excluded on the basis that it did not address the relationship between the two fields. More specifically, the search term “records management and information governance” was applied and yielded a smaller, but more relevant body of literature. The same terms were also used to search records management listservs, one based in the UK and the other in the USA. Each listserv attracts active engagement from recordkeeping professionals and those interested in records and information management issues more widely. Because of the relative currency of the debates being explored, wider Google searching was applied using the same search terms, specifically to capture professional forums, opinion pieces, conference presentations and social media discussions. Records management and IG policy documents from specific organisations were excluded on the rationale that the focus of this research was opinions expressed by those involved in the records management, information management and IG spaces, and on the nature of debates on the subject and the reasons behind various standpoints.

Based on results from this initial set of searches, further searching was undertaken for specific writers. Citations, references and in the case of social media postings, responses to posts, were used to carry out further searching. While literature written before 2013 was largely excluded, the searches yielded relatively little earlier literature, reflecting the currency of the subject. The literature reviewed was limited to publications in the English language. The final set of literature included authors and publications based in the UK, the USA, Australia and Canada. This is not an exhaustive review, but rather, identifies trends and highlights areas of debate.

Defining records management and information governance
Any analysis of perspectives on the relationship between records management and IG is inevitably shaped by the definitions being applied to each term. The international records management standard ISO 15489-1: 2016 provides a benchmark definition which is widely recognised at least by the recordkeeping community, and describes records management as the:

Field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use and disposition of records, including processes for capturing and maintaining evidence of and information about business activities and transactions in the form of records.

It is recognised that the term records management is often used interchangeably with the term “records and information management”, reflecting a broadening perspective on the remit of records professionals. As recognised by Lomas (2010), records management has already undergone significant shifts in its evolution in order to remain relevant to the needs of organisations, not least in response to the challenges of electronic records.

Definitions of IG, still a relatively new term, have been nebulous. Silic and Back (2013) noted, “there is no commonly accepted definition of information governance” and according
to Parapadakis (2014), “the more we talk about it, the more vague it becomes, and the more confusing and overlapping the definitions get”. As Hagmann (2013) recognised, much of the focus on IG continues to come from the USA. Smallwood (2014) describes IG as “a super-discipline that includes components of several key fields: law, records management, information technology (IT), risk management, privacy and security, and business operations”. The Information Governance Initiative (2018), a US-based think-tank, describes IG as “the activities and technologies that organizations employ to maximise the value of their information while minimizing associated risks and costs.” In general, the key characteristics of these various definitions are their high-level nature and the breadth of their scope.

Perceptions on the relationship between records management and information governance

Two distinct disciplines or are boundaries blurred?

Lappin (2014a) posed the question:

Is records management being subsumed into information governance or is it a separate discipline that will help to shape information governance but will retain its own distinct identity and purpose?

In essence, much of the discussion around the relationship between the two deals with those questions in one way or another. Parapadakis (2018), reiterating his belief first expressed in 2014, emphasised the clear distinction between the two. Echoing the views of many across the IG space, Parapadakis drew a clear distinction on the basis that the:

Purpose of information governance is to define all aspects of how information is being managed.
The purpose of records management is to manage some of the aspects of that information.

Likewise, Dunn (2018) noted that, “it is important to understand that records management and IG are two separate tiers of scale. In fact, records management falls under the umbrella of information governance”. As Hagmann (2013) recognised, “records management then just becomes one decision domain and discipline under the umbrella of information governance” and this idea of records management as one component of a wider IG framework was one that recurred frequently across much of the literature reviewed. Records management operations and activities, as Saffady (2015) notes, “are performed within the strategic framework defined by information governance”. Smallwood (2014) is clear in the distinction he perceives between the two disciplines:

Records Management (RM) is a key impact area of information governance (IG) – so much so that in the RM space, IG is often thought of as synonymous with or a simple superset of RM. But IG is much more than that.

The end of records management?
The idea of an evolution away from records management and towards IG was another commonly occurring theme, with the role (if there was indeed a role) for records management being less clear. The Republic of Estonia Ministry of Economic Affairs and Communications (2014) outlined preparations for what it termed a move from records management to “holistic information governance” (something first proposed in a green paper in 2012). The reasons behind the shift were presented in detail with the key rationale in essence being the inadequacy of records management to meet current business needs.
There is still much duplicated and manual work done, paper-based logic is yet being copied to the electronic environment. At the same time, the necessary information is difficult to find and use.

Envisaging the implementation of this evolution, records management was nevertheless still recognised as one implementation strand in a broader framework. Echoing many of the views already noted across the literature, the Estonian paper described IG as “a complex, multi-component discipline”, and crucially emphasised that “Information governance IS NOT a synonym for records management”. Driving these changes was the need for improved service delivery in a digital era, underpinned by better access to, and sharing of, information amidst changing working contexts where records exist in multiple environments – “[...] such records differ significantly from traditional records.”

Prophecies of the demise of records management were evident in a range of perspectives from the IG space. Addressing the question “why is records management disappearing and being replaced by information governance?” Zarkout (2014) argued that:

The records management profession has struggled to translate the practices of the paper paradigm to the world of electronic information. The adoption of social, mobile and cloud have revealed gaps in many of the traditional records management applications, which are unable to capture content from these new sources and manage them. Simply put, records management has not been able to keep up with the velocity, volume and variety of formats for digital assets.

Harrelson (2018) regards the misconception that RIM professionals are “crotchety neighbours from Paperville” as a “branding” that while wrong is nonetheless pervasive and “a hurdle we deal with daily”. Indeed, the idea of records management being a concept too burdened with baggage from the paper world was mentioned by a number of authors, most notably those from outside the recordkeeping community. Hart (2014), in a post to his “Word of Pie” blog likewise emphasised that IG should not simply be seen as an updated term for records management because “if it simply becomes a term used in place of Records Management we will have wasted an opportunity. IG is different. It needs to be different. The rationale was a simple one: “Records management failed. We need a new approach”.

Whether records management was seen as an integral part of an increasingly strategic IG approach, or an outdated discipline which had “failed”, there was consensus across much of the literature that something else or something more was needed, precisely because records management had not, or indeed, by its very nature, could not, fulfil all of the complexities of an organisation’s information needs. In some cases, that was seen as submergence into a bigger information landscape, while for others, perhaps something more fundamental. Parapadakis (2018) has positioned records management as focussed on an organisation’s unstructured information (chiefly documents and emails), on average representing less than 20 per cent of the total information managed by an organisation. The idea of records management only fulfilling a part of the information needs of a twenty-first century organisation were echoed by a number of commentators. Woolen (2014) has suggested that “[...] the records management buzzword has died so, instead, I talk about information governance which, of course, includes records management”. Crucially, Woolen recognised that while records management is still very much there and a core part of wider IG agendas, there was, he maintained, a definite desire among some to move away from the terminology of records management.

What might being one cog in a bigger IG wheel mean for records management, and specifically for records managers? Among those who still recognised a clear role for records management within a wider IG framework, there was variance on the nature of the relationship between the two. With an emphasis across much literature on the idea of IG as the decision-making hub and strategic driver, with records management as one arm of
implementation, there is a sense of records management being perceived as largely operational in scope, arguably the very thing that the records management profession has striven for many years to dispel. Again, these opinions were expressed chiefly from outside the recordkeeping community – Gillin (2018) believed that “Records managers are responsible for carrying through on the guidelines laid out by governance professionals”, echoing the view of Dunn (2018) that while IG “refers to the strategic element of designing and organizing information management [...] [...] Records management represents the actual implementation of information management plans”. Yet as Haider (2018) notes, records and information management programs have always included “‘governance’ which includes strategic planning, policies, procedures, standards, guidelines, [and] audits [...]”. More recently, Tough and Mathews, in research underscoring the close relationship between recordkeeping and governance, proposed “governance recordkeeping” as an approach to “managing records and documents in the world of governance, audit and risk.” Crucially, this approach “considers record keeping as a governance function” with recorded information managed as a “strategic resource”.

Much of the literature regarded the positioning of RM as one part of a wider IG framework as a positive development for records managers, strengthening their hand by explicitly recognising their input while aligning them more formally with other key stakeholders. In other words, while on the one hand, records management was deemed to be insufficient on its own to fulfil an organisation’s information needs, it was at least now clearly valued as part of a wider information landscape. Indeed, after years of advocating for records management to be further up organisational agendas, being part of an IG framework had strengthened its position by recognising its role within a more strategic information framework. As noted, another key advantage recognised in much of the literature was that IG strategically positioned records managers alongside a range of other vital stakeholders and allies – including IT, legal, risk, information security, privacy, compliance and business unit heads – those who previously the records managers may have had to forge alliances and relationships with on their own initiative. For Haider (2018), achieving constructive collaboration with IT professionals has been, and remains, one of the greatest challenges for records managers. Yet, meaningful collaboration may prove elusive if, as Harrelson (2018) asserts, records management, by being too often perceived as increasingly irrelevant in the digital age, sits on an unequal footing with IT.

Adding value to records management?
Far from seeing the slow demise of records management either for being outdated or through absorption into IG frameworks, Franks (2013) similarly regards IG as a means of strengthening and validating records management. Indeed, she has argued that, “Records management is essential to information governance” and, moreover, “because of their broad understanding of the flow of information across the enterprise, records professionals are in a unique position to contribute their knowledge and skills to this initiative”. Thus, far from diminishing the contribution of records managers, IG has the potential to enhance it. Wiler (2014) reiterated this view while emphasising the need for records professionals to engage with IG “because it represents a tremendous opportunity for you to catapult yourself into a strategic leadership role”. Like other writers, Franks and Wiler viewed IG as a strategic enabler by providing a framework to bring together a range of relevant stakeholders and, crucially, being able to “provide context to discussions of an integration of information management, risk management and records management considerations”. As Sloan (2014) noted, “The salient feature of the information governance approach is that it compels
organizations to take a broad, inclusive view of information issues, in addressing compliance, risk and value”.

The emphasis on collaboration and changing organisational contexts was at the fore of comments made by Ardern (2016) in a personal reflection on her forty year career in archives and records management and the changes in that time in a Canadian context, in which she considers “how we have evolved from records management to information governance”. Charting developments in technology, privacy laws, and approaches to risk, amongst others, Ardern observed that:

[...] information governance is a response to a changing workplace, hugely impacted by technology and requires collaboration between several groups to ensure consistency and reduce duplication of effort in managing information resources.

Echoing other writers, she argued that:

Records and information management skills sets are being enhanced and expanded alongside other professions such as legal, privacy, risk, and IT, driven by a need to address what are truly enterprise-wide issues.

She notes that “Records management has changed, not gone away, because there is still a need to manage records as evidence of business decisions and transactions”, but, crucially, recognised that the environment in which records management operates has changed, and will continue to change, requiring increasing collaboration between stakeholders within an organisation. As expressed across much of the literature reviewed, that collaborative environment may be most effectively provided within an IG context.

Keirstead (Graves, 2015) sees IG “as a contemporary, unified way of articulating the value of an effective Information Management program to any organization.”, with its main strength being potentially.

The way in which it can bring different partners to the table who might, in the more traditional and stratified world of the information professions, not necessarily be working together or indeed talking to each other[2].

Bridges regards this kind of integrated framework as essential:

As it is no longer practical to produce information policies, to develop and implement security controls and to operate and support key information management services in isolation of each other.

As Lomas (2010) has noted, in the UK context, the National Health Service (NHS), for whom patient confidentiality is paramount, has been at the forefront of embracing broader IG approaches to information management, encompassing “concepts of records management, information security, public accountability and legal compliance”. Similarly, Lappin (2015) sees the value of IG in its potential “to create synergies” between the various component disciplines under the IG umbrella “and to enable them to become more than the sum of their parts.” The latter statement seems key to the opportunities of an IG approach for records management.

Therefore, recognition of the changing context in which organisations operate and the idea that records management is no longer able to fulfil all of an organisation’s information requirements, emerged as a strong theme in the literature consulted. For some, such as Losey (2015), “old-time record keepers with their long complex retention schedules and harsh top down rules” alongside their “classify and control approach” seem an anachronism. Others have taken a more nuanced stance, recognising that records management still has value to offer – the key is that it embraces new approaches. One of the few recordkeeping
voices to directly address the relationship between records management and IG, and to engage in debate with the IG community, Lappin (2014b) discussed the changes taking place in approaches to records management, including “in-place” records management, growing interest in the possibilities of automation to reduce the burden on the end user, and recognition of the need to manage all information, irrespective of whether a record. Lappin characterised these as part of a new “information governance approach to records management”.

An example of how more holistic IG approaches to managing information in organisations has the potential to strengthen records management comes in the area of information security, in practice something not typically under the remit of records managers despite its centrality to information management. As demonstrated by Lomas (2010), limitations with ISO 15489 may in part be addressed by closer alignment with other information standards such as ISO 27001:2005 Information Security Systems Management Requirements, which addresses the balance between access and security. For Lomas (2010):

> Information governance solutions and thinking, which balance risks, present many of the practical answers for the development of records and information management systems within the context of current and future challenges.

Lomas regards these new approaches as essential as records management faces a paradigm shift as increasing quantities of organisational information exist outside of the organisational firewall creating unprecedented challenges for organisational control and accountability. Lappin (2014b) has positioned the growth of IG as yet another evolutionary phase in the wider history of records management, which he argues, has always been characterised by periods of coherent and less coherent responses to various disruptive technological changes.

**Bringing together the strengths of each?**

While Lappin (2014b) recognised several strengths in approaching records management with an IG lens, including an enhanced focus on accountabilities to external stakeholders, he also warned of potential weaknesses, not least a lack of focus on the day to day needs of end users. Given the predominance of people and cultural issues in successful electronic records management as demonstrated by McLeod (2010) and Bailey (2014), Lappin’s concerns are significant. Similarly, Oliver and Foscarini (2014) have advocated an information culture approach to records management, emphasising the need for RIM solutions that are more sensitive and nuanced to differing organisational and information cultures and information preferences. Yet, the focus of much of the discussion around IG appears decidedly organisation-centric and top-down. Indeed, the focus on tighter, more effective organisational governance reflects the increasing emphasis on compliance and risk which are central to IG. The main drivers for IG as identified by the Information Governance Initiative (2018) were “external regulatory, compliance, or legal obligation”, followed by a “desire to mitigate risks associated with data that could have been defensibly deleted”, with “external trigger events/incidents such as a law suit, investigation or data breach”, following close behind. Interestingly, more positive drivers such as supporting good business practice, mining value from organisational information and problem solving were lower priorities. The lessons learned by records management in attempting to successfully manage electronic records, not least in balancing the needs of the organisation with those of end users, could prove valuable to IG.

Taking a different standpoint, Carlis (2015) suggested that the “discipline of records management has evolved to the point where it now encompasses information management...
and governance”. Moreover, Carlis regarded this as “empowering and strengthening the records management function, which increasingly is being viewed as vital to the success and safety of businesses as well as their customers and other stakeholders”. Indeed, not only was a successful IG programme built upon good records management, but that IG was in essence “records management plus”. Crucially, and in direct contrast to a number of other vendor/industry perspectives, Carlis positioned IG ideas as actually widening the records management remit, rather than pigeonholing it within relatively narrow confines alongside a number of other information disciplines. In some respects echoing Lappin, “Records management plus” was defined as expanding the “traditional definition of records management” to encompass the entirety of an organisation’s information infrastructure, including “unstructured data, business transactions, social media, legal holds, eDiscovery demands and metadata”.

While some aspects may be new, many believe that, to a lesser or greater extent, IG builds upon existing records management principles. Medina (2015), far from seeing the demise of records management, regards IG “[…] as another attempt to re-brand” records management and:

To bring other aspects of information management that began far after RM practices began, under the same roof. But if you look under the hood, the engine is STILL basic records management, with increased horsepower […] and a few other bells and whistles[3].

Similarly, Stephen Howard cited in the context of a series of blogs by Graves (2015) exploring the concept of IG, identified IG as “a useful portmanteau concept” but ultimately “not new”[4]. Discussing his “core sense” of the term, Howard emphasised the idea of aligning information management with “wider organizational strategy […]. to be implemented via policy and standards with a clear chain of accountability”. Interestingly, Howard believed that it was precisely “information governance’s inherently flexible definition” that had “enabled its adoption by a wide variety of professions and disciplines”.

**New directions?**
The National Archives of Australia (NAA) – a country which has been so central in shaping and defining the recordkeeping theories of the past 30 years – defines IG as:

An approach to managing information assets across an entire organisation to support its business outcomes. It involves having frameworks, policies, processes, standards, roles and controls in place to meet regulatory, legal, risk and operational requirements. Information governance is an essential element of corporate governance that must be aligned with business outcomes and risks.

Where once NAA focussed on records and information management, the term IG has taken precedence, indeed, the term records management has all but disappeared from its extensive resources on managing information. Interestingly, though, the facets of building a strong IG framework that are identified by NAA are very similar to those long-familiar to records managers – securing senior management support; understanding the external and internal operating environments of an organisation; aligning information strategies to the business need; and embedding a culture where information is valued, to name but a few. Alongside shifts in Australia, it is notable that in the US, the professional forum provided for some twenty years by the records management listserv recently passed to a newly established IG GURU® news and community site aimed at “IG professionals”.

Returning to Smallwood’s definition of IG as “a super-discipline that includes components of several key fields”, the use of the word “components” seems a subtle but potentially significant point. For records management, the logical corollary to this is
ambiguity around the role of the records manager. Indeed, Smallwood (2014) envisages that “This unique blend calls for a new breed of information professional who is competent across these established and quite complex fields”. Related debates reflecting frustrations and sensitivities around professional identities have been evident in recent posts to the USA records management list-serv. The publication of the latest edition of ARMA International’s Job Descriptions for Information Management and Information Governance prompted Smith (2018) to lament that ARMA had “taken records out of the records and information management profession. Once again the IG push is taking the profession in the wrong direction”. Haider (2018), responding to a publicity statement for the Managing Electronic Records [MER] Conference 2018 stating “The records management silo mentality ends here!”[5], expressed her increasing frustration with “technology vendors” and “IG gurus” “slinging arrows at records and information managers and insinuating that RIM is only useful for developing a records retention schedule”. Notably, Haider challenged the idea (apparently implicit in MER and IG much of the discussions on the RM/IG relationship) of treating electronic records as something completely distinct from paper records – “The only thing different is the tool used to create and store the records”. Defending the continued value and relevance of the records manager in today’s information landscape, Lueders (2017) has argued that:

Our training and experience [..] empowers us to make and defend the difficult decisions that we need to make. No other group of people – and certainly no new, vaguely-defined profession – will ever confidently destroy massive volumes of information and then wilfully and effectively defend their actions if they are ever questioned. Professional records managers stand alone in this capacity.

Conclusion
While much of the literature reviewed recognised IG as offering something new and distinctive, some perspectives were more sceptical, questioning whether IG was little more than a rebranding exercise. Among those who recognised it as something new and distinct, differences emerged between those who took the view that IG had the potential to strengthen and add value to records management, and those who saw IG as a distinct discipline in its own right, in many cases, superseding records management. A range of perspectives from recordkeeping and non-recordkeeping backgrounds saw IG as having the potential to broaden and support records management, while many agreed that IG was built upon many of the fundamental principles of records management. For those who saw IG as the necessary successor, records management was perceived to be too synonymous with the paper era to be truly capable of meeting organisational needs today. Far from seeing IG as strengthening records management, it was seen as replacing a discipline no longer fit for purpose. In this sense, this paper identifies a distinction between discussions of an IG approach to records and information management characterised by a more holistic way of managing records and information (in a sense, viewing IG as another stage in the ongoing evolution of records management) and advocates of IG, a formally defined super-discipline requiring a new kind of information professional. Related to this, sensitivities were apparent around professional roles and identities.

Perhaps unsurprisingly, those who advocated most strongly for the continued relevance and value of records management in the twenty-first century information landscape were generally those writing from a records and information management background. A more diverse range of voices coalescing around the IG space were, in general, quicker to question records management’s role and relevance. For many, IG offered a more holistic and
comprehensive approach for organisations struggling with oversight of information creation and use across a myriad of complex information environments. As Fleming (2013) has observed, “In today’s world, the problems are exponentially more complex and the solutions extend far beyond traditional RIM concepts”\(^1\). At the same time, many saw records management as an integral part of IG, recognising that fundamental records management principles underpin IG. If, as the definitions emphasise, IG is about a multidisciplinary approach to minimizing the risks while maximising the value of organisational information, then, arguably, the truly new and valuable characteristic of IG is its focus on meaningful collaboration in meeting information challenges. As McGovern (Graves, 2015) has commented, “Information Governance is informed by, builds on, and leverages lessons learned from established practices. The different terms we use reflect different lenses, perspectives, domains, and insights gained”\(^6\).

The findings also highlight that, with a few notable exceptions, there has been a lack of direct engagement from the records management community in the debates that have played out in recent years. Lappin (2014a) has wondered:

> Does this new wave of information governance form part of a wider change in [the] records management paradigm? Are we seeing a new model of how records management should be tackled?

Perhaps these fundamental questions can only be truly answered over time, as the records management and IG spaces each continue to evolve. What is clear is that a broad range of interests are offering comment on records management, many of those voices coming from outside recordkeeping. With much of the discussion space dominated by commercial interests, vendors and those working within the IG space, it is imperative, therefore, that the recordkeeping profession proactively engage with and contribute to these debates.

Ultimately, while opinion varied on the relationship between records management and IG, and specifically on the relevance of records management, the literature reviewed suggested widespread agreement on the complexities of today’s information landscape and the need for organisation-wide, innovative approaches. Ultimately, whether the focus of activities is IG or records/information management, the goal (and the challenges) remain largely the same – supporting an organisation to manage, secure, access and exploit its information in complex digital environments across a myriad of locations. However, how the goals are achieved and the challenges met, and crucially, by whom, remain contested ground.

**Notes**

1. The term “recordkeeping” is used here to describe the management of current and historical records. Specifically, the term ‘records professional’ encompasses the work of both records manager and archivist, but in the context of this paper relates chiefly to the work of the records manager, defined by the International Council on Archives Multilingual Archival Terminology database as “a person, professionally educated, trained and experienced, responsible for the effective and efficient delivery of records management services to meet an organisation’s requirements”\(^2\).

2. Keirstead is one of a number of records and information professionals quoted in the context of questions posed by records professional Chris Graves and detailed in his blog post ‘Policy driven integrated decisions’, to his Red Sea Dispatches blog, Open Shelf, 1 December 2015. Available at http://open-shelf.ca/151201-policy-driven-decisions/. The blog was one of a series exploring the concept of IG.
3. See Medina’s comments posted 26 May 2015 in reply to Lappin’s blog post of 20 May 2015, ‘Records management is wanted dead or alive’, Thinking Records blog. Available at https://thinkingrecords.co.uk/2015/05/20/records-management-is-wanted-dead-or-alive/


5. In a reply to Haider’s comments, Seth F. Williams, representing the MER Conference, directed a statement to ‘the records manager community’ seeking to clarify the intended meaning of the silo mentality advertisement slogan – see his post of 15 March 2018. Available at https://lists.ufl.edu/cgi-bin/wa?A2=ind1803c&L=RECMGMT-L&P=3886


References


Further reading


Corresponding author
Julie Brooks can be contacted at: julie.brooks@ucd.ie
The influence of organizational culture on information governance effectiveness

Ali Daneshmandnia

Long Island University CW Post College of Liberal Arts and Sciences, Brookville, New York, USA

Abstract

Purpose – This paper aims to explore the impact of organizational culture on information governance (IG) effectiveness at higher education institutions (HEIs). IT professionals, such as chief information officers, chief technology officers, chief information security officers and IT directors at HEIs were surveyed and interviewed to learn about whether organizational culture influences IG effectiveness. Several IG activities (processes) were identified, including information security, the function of an IG council, the presence of a Record Information Management department, the role of a compliance officer and information stewards and the use of an automated system or software to identify and maintain information life-cycle management.

Design/methodology/approach – This study was conducted using Cameron and Quinn’s (Cameron and Quinn, 2011) competing value framework. To evaluate organizational culture, using the competing value framework, four types of organizational culture profiles were used: collaboration, creation/innovation, controlling/hierarchy, and competition/result-oriented. The methodology included quantitative and qualitative techniques through the use of content analysis of data collected from participants. IT professionals, such as chief information officers, chief technology officers, chief information security officers and IT directors at HEIs were surveyed and interviewed to learn about whether organizational culture influences IG effectiveness.

Findings – Findings revealed organizational culture may influence IG effectiveness positively, especially from cultures of competition/result-oriented and control/hierarchy. Qualitatively, it also emerged that competition/result-oriented and control characteristics of organizational culture were perceived by IG professionals to produce more accurate information. One of the characteristics of organizational culture that became evident in the current study, coming from more than one subject, was the challenge in IG due to the presence of information silos. Trust, on the other hand, has been highlighted as the glue which can enable and drive governance processes in an organization.

Research limitations/implications – The current study was conducted based on HEIs. While the current study serves as a baseline for studying IG in other institutions, its results cannot be generalized for other type of institutions. The results cannot be generalized for other types of not-for-profit or for-profit organizations. Many of the characteristics of the sample data were specific to HEIs. For instance, financial, manufacturing and health-care institutions present challenges inherent in those institutions.

Originality/value – Trust has been highlighted as the glue which can enable and drive governance processes in an organization. Respondents of current study have indicated that trust serving several different factors toward IG effectiveness, including freedom to speak freely in the meeting about impact of organizational culture on IG, willingness of executives of administration, particularly the CIO, to communicate IG matters to institution, sharing information and being transparent, entrusting help desk staff and technical supervisors so users can communicate with them and share their concerns and perceiving “feeling of trust” in the organization, which would benefit the institution, allowing stakeholders to collaborate and work together to overcome issues when facing IG challenges.

Keywords Organizational Culture, Information Culture, Chief Information Officer (CIO), Information Governance effectiveness, Information Governance of Higher Education Institution, Information Governance Processes

Paper type Research paper
Introduction
This study intends to explore the impact of organizational culture on information governance (IG) in private and public higher education institutions (HEIs). Part of a broader study of IG at HEIs, it discusses the impact of IG determinants. This study is a survey of chief information officers (CIOs) and other key information officers. Those participants who responded to the questionnaire and who were willing were individually interviewed. The participants’ institutions were all members of the Middle State (Mid-Atlantic as of 2013) Region on Higher Education, better known as the Middle State Commission on Higher Education (MSCHE).

The role of the CIO in promoting and communicating IG will be discussed. HEIs, much the same as health-care organizations, capture an abundant amount of confidential information. Shortcomings and gaps that apply to IG in HEIs will be identified and solutions, from the position of the key information officers (e.g. CIOs), will be explored. Finally, this study can reveal IG characteristics that might be specific to HEIs, characteristics that otherwise might not be recognized.

Governance has been defined as “the exercise of authority of the distribution of power” (Valaskakis, 2001, p. 47). Governance has also been discussed in terms of structures, legal relations, authority patterns, rights and responsibilities and decision-making processes (Birnbaum, 1988).

Perri (2001) explains that one of the most important features of good governance is judgment. Good governance has the following core components: accountability, participation, predictability, transparency, and efficiency (Burns, 2004). As policymakers make use of technology in exercising governance, the key challenge is to select and manage those technologies to cultivate the skill of judgment among policymakers (e.g. the CIO). Governance of information requires the capabilities of decision-making and authority. It also requires tools or techniques to oversee communication and monitor IG in the HEIs.

People research, develop, manage and regulate IG with the aid of technology. Thus, IG as it relates to activities that take place in an organization is concerned with the following:

- promotion of technique (technological and organizational innovations);
- identification of risks according to key players (stakeholders, CIO, etc.); and
- employment of rules to govern information practices as they correspond with internal and external guidelines.

Promotion of technique refers to technological innovations in managing and maintaining oversight of IG. These techniques are usually information policies and computer systems that are interconnected and present opportunities in gathering information and applying and controlling governance. These techniques, however, do not replace people who are overseeing implementation of IG. Ultimately, key individuals such as the CIO use judgment and foresight to deploy IG.

HEIs manage student funds and must follow similar compliance requirements as health-care institutions in regard to keeping information (belonging to students, faculty and other employees) confidentiality, privacy and security. Additionally, HEIs are faced with the emergence of Big Data, and they must manage raw data effectively. Big Data brings both opportunity and cost. Organizations are increasingly faced with the decision of what to keep and what to dispose of when information is determined no longer to have business value and how to reduce the risk of liability.

Kooper et al. (2011) emphasize IG involving three actors: the creator of information, the receiver of information and the governing actor. All three are needed to implement IG;
however, the governing actor, will interact between creator and receiver within the information environment or “transaction.” Kooper et al. (2011) maintain that the element of sense making involves the governing actor and the information environment.

Organizational culture and IG in higher education institutions
To analyze the IG of an HEI, it is important to identify the source of information and the internal and external factors that influence its governance. Comprehensive frameworks can further improve the processes of IG (Parikh, 2001). Smallwood (2014, p. 87) maintains that determining prioritization in building a best practices IG framework requires careful consideration of organizational culture, management style and business goals. A shared and transparent collaboration among all stakeholders, particularly the CIO, CISO (chief information security officer), IT director, compliance officers and other administrators (e.g. VP of finance, VP of student services, bursar and registrar) will ensure an effective framework for the institution. Smallwood emphasizes that the CIO, in particular, should disseminate policies and communicate via different modes, including email, blogs, social media and mobile platforms. CIOs can and should collaborate with their peers from other institutions regarding IG policies and frameworks.

What is organizational culture? Researchers refer to assumptions about and the understanding of day-to-day workplace activities (Deal and Kennedy, 1982); attitudes and behaviors that signify the organizational working environment (Hofstede 1980); and a “deeper level of basic assumptions and belief that are shared by the organization” (Schein, 1985). Capelo (2012) defines it as a role in organizations that concerns internal interaction, the feeling of belonging (or not) and commitment regarding the creation of a competitive environment, and the development of the social glue that bonds the organization together. Cameron and Quinn (2011) explain that organizational culture is a predictor of other organizational outcomes such as effectiveness. They emphasize that culture has been defined as a lasting set of assumptions, belief and values that describe organizations and their members.

Giordano explains that to establish and implement successful IG in an organization, a data stewardship community must be carefully defined, respecting organizational culture to ensure acceptance. What is more, Information Lifecycle Management (ILM) policy should be based on culture and organizational structure (Giordano, 2015). Organizational culture addresses the ability with which that organization adopts change in order to implement IG. Overlooking this factor can lead to unsuccessful implementation of IG. Giordano views this as part of change management in an organization.

Information culture explains the relationship between individuals and information in organizations (Curry and Moore, 2003) and includes values, beliefs and codes of practice toward information management (Wright, 2013). Values given to information and attitudes toward it are signs of Information Culture (McMillan et al., 2012; Curry and Moore, 2003; Oliver, 2008; Davenport and Prusak, 1997; Jarvenpaa and Staples, 2001). Oliver (2008) examined information culture using three case studies of universities in Hong Kong, Australia and Germany. His finding revealed that recognition of social and organizational requirements influences managing and governing information. In other words, information culture is influenced by “attitudes towards and values of information.” (Oliver, 2004). Additionally, he found out that requirements established by governmental agencies for information management such as copyright, freedom of information, played a “key role” in information culture. Wright (2013) investigated information culture in government organizations and concluded that a culture of collaboration and openness resulting in
information sharing ensures more informed decision-making, and Svard (2014) also found that information culture influences the record management practices.

A CIO or information steward can leverage the existing organizational cultural to influence business and IT stakeholders on educating and communicating IG policies. Goh (2002) maintains that organizational culture can facilitate knowledge transfer towards problem solving within information technology. In the current study, researcher use the competing values framework, which evaluates organizational culture of an organization divided into four quadrant, each "representing a distinct set of organizational effectiveness" (Cameron and Quinn, 2011, p. 39). The competing values framework will be used to evaluate organizational culture, which will contribute in drafting the map (profile) of an organization’s cultural profile, which is shown in Figure 1.

To assess the level of IG processes in an HEI, several elements have to be measured to establish which ones best represent the status of IG in the organization. However, researchers (Peterson, 2002; Ribbers et al., 2002) argue that, when aligned with the organizational context of stakeholders’ experiences, and taking into account analysis of cost, benefit and risk, IT performance is characterized by a high level of IT processes. Additionally, many researchers (Giordano, 2015; Smallwood, 2014; Ballard et al., 2014) suggest that an organization’s having an information stewardship program, a chief information security officer (CISO), a RIM program, a compliance officer (or office of compliance) and an enforced ILM contribute to effective IG performance. In this study, the process of IG is operationalized in terms of the following elements: presence of IG council (IGC), presence of a chief information security officer (CISO), presence of a RIM department, presence of a compliance officer (caretaker), information steward communication and collaboration and the presence and use of software (an integrated ILM system) to automate identification of electronic and paper records eligible for destruction. Factor analysis was

Source: Cameron and Quinn (2011)
conducted to assess which of the above elements are indicators. The first four IG processes were presented to the subjects in the questionnaire in a “YES/NO” format, while the last two processes were presented in Likert scale. Table I presents the elements of the IG process:

### Research questions

In an attempt to identify determinants of IG effectiveness, the following research question guides this study:

**RQ1.** Is organizational culture at HEIs correlated with perception of IG effectiveness?

Organizational culture was operationalized using OCAI, a competing values framework, to determine the four different culture types: collaborative, creative, competitive and control. The results of the current study in regard to organizational culture indicate that participants regarded the result-oriented characteristic as a common theme and some even regarded result-oriented as a core value, as they consider their organization data driven. Results in the current study are similar to findings using Cameron and Quinn’s Competing Values Framework (2011, p. 91); higher scores are reported for the “market quadrant” (compete and result-oriented) of the culture profile for service-based industry participants.

### Design of the study

This study was divided into two phases: Phase 1, a questionnaire, which was both quantitative and qualitative in approach, and Phase 2, which was qualitative only and involved the interview of subjects who had taken part in Phase 1 and expressed interest in further participating.

The population for Phases 1 and 2 were the key information officers (CIO, CISO, system analyst, network managers, system programmers, help desk manager, archival manager and other IT management positions) of all colleges and universities in the Middle State Commission of Higher Education (MSCHE, as of 2013, Mid-Atlantic) member states. MSCHE is recognized by the US Secretary of Education to accredit all colleges and universities for the region (MSCHE, 2014). Additionally, MSCHE is recognized by the Council for Higher Education Accreditation (CHEA) to accredit postsecondary institutions. CHEA is a national advocate for self-regulation of academic quality with approximately 3,000 degree-granting colleges and universities as members (CHEA, 2015). The researcher builds a population frame from the population of all MSCHE institutions in its region covering Delaware, DC, MD, NJ, NY, PA and Puerto Rio).

Table II shows the breakdown of HEIs by state:

All 568 institutions were used. The key information officers (CIOs, CISOs, project managers, help desk managers, archival managers, systems programmers/managers,

### Table I.

<table>
<thead>
<tr>
<th>IG Process elements</th>
<th>Scholarly literature</th>
</tr>
</thead>
<tbody>
<tr>
<td>Presence of CISO</td>
<td>Abu-Musa (2010)</td>
</tr>
<tr>
<td>Presence of IG council</td>
<td>Giordano (2015)</td>
</tr>
<tr>
<td>Presence of information Stewards (communication) or RIM’s policy advisory committee</td>
<td>Giordano (2015), Smallwood (2014), Ballard et al. (2014), Kaczmarek (2014)</td>
</tr>
<tr>
<td>Presence of ILM (automated-software)</td>
<td>Giordano (2015), Logan et al. (2013)</td>
</tr>
<tr>
<td>Records Information Management</td>
<td>Kaczmarek (2014)</td>
</tr>
<tr>
<td>Using IG framework (GARP, IGRM)</td>
<td>Discovery (2014), Smallwood (2014)</td>
</tr>
</tbody>
</table>
network managers, compliance manager and other information management positions (within IT departments) were asked to participate in this research study.

**IG processes at HEIs**
Six elements were identified as parts of the process of IG in HEIs. These appeared as Question 1 and 2, and they are referred to as Process of IG. In the current study, IG process consists of six different parts:

1. information security management (spear headed by CISO);
2. presence of an IG council;
3. presence of a Record Information Management department;
4. presence of a compliance or chief compliance officer;
5. identification of information stewards and their collaboration in regard to IG; and
6. automation of identification (often accomplished through use of software) of information records eligible for destruction or Information Lifecycle Management (ILM).

Processes 1 through 4 were to invoke responses of either Yes or No. One change that made results richer, was suggested in the pilot study by a participating CIO; Negative responses to survey Question 1, concerning the presence of a CISO, governance council, RIM department and chief compliance officer, were expanded to three levels: “No, but we are in the process of selecting/forming one,” “No, but we are considering selecting/forming one,” and “No, nor do we have a plan to select/form one.” This suggestion was also present in Williams and Hausmann’s (2014) study.

In Phase 2, 15 participants who indicated their willingness to take part in semi-structured, one-on-one interviews among those who took part in the survey were selected. Anonymity of participants was strictly enforced. In this study, Directed Content Analysis was instrumental, as it involved the use of codes and categories relevant to the focus of the study (Berg, 2009, p. 341). SPSS was used to analyze data from the survey, and Atlas.ti qualitative data analysis software was used to conduct qualitative content analysis.

Independent variable organizational culture was measured using Likert and categorical scales. A total of 168 subjects responded to the survey, of which 126 completed the survey in full. However, all 168 subjects answered the first two questions that evaluated the dependent variables. Of these survey subjects, 15 were interviewed, and these interviews were recorded, transcribed and analyzed.

The following is the map of the current study (Table III):

<table>
<thead>
<tr>
<th>State</th>
<th>No. of HEIs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delaware</td>
<td>10</td>
</tr>
<tr>
<td>District of Columbia</td>
<td>25</td>
</tr>
<tr>
<td>Maryland</td>
<td>58</td>
</tr>
<tr>
<td>New Jersey</td>
<td>54</td>
</tr>
<tr>
<td>New York</td>
<td>213</td>
</tr>
<tr>
<td>Pennsylvania</td>
<td>157</td>
</tr>
<tr>
<td>Puerto Rico</td>
<td>51</td>
</tr>
<tr>
<td>Total</td>
<td>568</td>
</tr>
</tbody>
</table>

Table II. Number of member institutions by state
Phase 1 identifies the collection of data using the SurveyMonkey.com website, using Middle State Commission of Higher Education (MSCHE) to identify subjects. Use of EDUCAUSE constituents’ group. Email web-based survey. Preparation of data collected, performing quantitative analysis using various tools and recruiting subjects for interviews. Phase 2 was conducting qualitative analysis on data from the interview transcripts and Phase 3 concerned discussing the findings and offering a new IG effectiveness model.

Findings and discussions
Results indicate that organizational culture showed positive correlation with perception of IG effectiveness. Several themes were identified including collaboration, entrepreneurial spirit, competitive and results-oriented environment, structured and controlled processes and trust. Structured and controlled emerged as dominant characteristics among HEIs.

Participant demographics
The principal subjects of this study were CIOs of HEIs. However, other IT professionals were also included – Associate CIO (8), Chief Technology Officer (CTO) (2), Chief Information Security Officer (CISO) (2), IT Directors, Compliance Officers and IT project managers (3) (Table IV).

Note that four of the CIOs have vice president titles, such as VP of Information Technology (Figure 2).
Almost 30 per cent of survey participants were female, which is much higher than the 9 per cent of IT management positions and 14 per cent top IT executive positions reported in Silicon Valley (Warner, 2014). The highest percentage of respondents was 45 to 60-year-olds. The current study revealed that 41 per cent of participants report to a CIO, 18 per cent report directly to a president or chancellor, followed by 10 per cent to a CFO, 9 per cent to a provost and 21 per cent to others. The “Others” list comprises the following positions: chief operations officer, CISO, chief technology officer, senior VP of organizational effectiveness and director of IT.

Survey summaries of statistics
The first question is a nominal question, measuring IG process (Appendix 1) (Table V). Table VI shows the results:

Table IV. Survey participants by title

<table>
<thead>
<tr>
<th>Title</th>
<th>(%) of responses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chief Information Officer (CIO)</td>
<td>39</td>
</tr>
<tr>
<td>Associate CIO</td>
<td>6</td>
</tr>
<tr>
<td>Chief Information Security Officer (CISO)</td>
<td>13</td>
</tr>
<tr>
<td>IT Director</td>
<td>19</td>
</tr>
<tr>
<td>Compliance Officer</td>
<td>4</td>
</tr>
<tr>
<td>IT Project Manager</td>
<td>4</td>
</tr>
<tr>
<td>Help Desk Manager</td>
<td>2</td>
</tr>
<tr>
<td>Others:</td>
<td>15</td>
</tr>
<tr>
<td>Information Security Manager</td>
<td>7</td>
</tr>
<tr>
<td>Project Manager</td>
<td>1</td>
</tr>
<tr>
<td>Chief Privacy Officer</td>
<td>1</td>
</tr>
<tr>
<td>University Record Officer</td>
<td>1</td>
</tr>
<tr>
<td>IT Budget Director</td>
<td>1</td>
</tr>
<tr>
<td>System Analyst</td>
<td>2</td>
</tr>
<tr>
<td>Chief Architect</td>
<td>1</td>
</tr>
<tr>
<td>Total</td>
<td>108</td>
</tr>
</tbody>
</table>

Figure 2. List of titles as champions of IG

The histogram in Figure 3 indicates a right skewness, with a spike in the middle, indicating a neutral position. Information stewardship and ILM, showed \( \text{Mean} = 3.2, \text{SD} = 1.47 \), and \( M = 2.12, SD = 1.31 \), respectively, indicating more agreement (Figure 3) in the
case of the presence of an ILM program, the finding reveals exactly the opposite, indicating that HEIs are lacking in ILM programs.

Organizational culture \((M = 16.45, SD = 4.04)\) slightly tilts toward agreement with a spread of 4.04. This could indicate that the institution taking part in the survey may have an overall, higher than usual cultural interaction in connection with IG (Figure 4).

The Cronbach’s alpha test of reliability (internal consistency) was performed on organizational culture variable, and the results showed that the reliability coefficient for four items belonging to organizational culture was 0.7, which is acceptable. (Cronbach, 1951).

**Results of research question: determinants of IG effectiveness in higher education institutions**

The purpose of this research question was to learn about what characteristics of the HEI organizational culture would influence the IG of HEIs. Table VII shows the breakdown of responses for Question 1, the IG processes at HEIs (Figure 5).

As indicated in the chart above, the highest percentage belongs to presence of CISO, 68 per cent, followed by presence of a compliance officer at 53 per cent, presence of an IG committee at 46 per cent, and presence of a RIM department or program at 34 per cent. These findings reveal the importance that HEIs give to information security and compliance...
Figure 3. IG process information steward (Left side) and presence of Information Lifecycle Management (Right side)

Mean = 3.2
SD = 1.47
N = 187

Mean = 2.12
SD = 1.47
N = 187

Information governance effectiveness
measures. The last two IG processes, 5 and 6, active collaboration of information stewards and use of automated procedures (software) for ILM system, respectively, could not have been assigned as “Yes” and “No” since both collaboration and use could vary from institution to institution; therefore, these two processes were presented as Likert data (Figure 6).

As indicated in the above graph, a total of $85(M = 3.18, SD = 1.3)$ participants or 51 per cent, indicated that they have at their institutions information stewards who actively collaborate with IT or a RIM department regarding IG (Figure 7).

On the other hand, only 32 respondents or 20 per cent indicated that they have ILM in an effort to automate the identification of paper and electronic records eligible for destruction. This percentage of respondents is the lowest of all IG processes that were investigated in the current study (Figure 8).
Figure 8 shows a highly negative response in regards to the use of automated ILM systems. The results shown in Table IX indicate that 114 respondents or 67 per cent maintained that they do not have an automated procedure in the form ILM software for electronic and paper records, compared to only 20 per cent or 32 participants who indicated automated procedures of ILM practices established for e-records and paper records. Computer-assisted technology is a good approach for ILM (Smallwood, 2014); however, there are still many issues to be resolved, including auto-gathering software that can follow guidelines as to what information to select, support for interoperability, and access mechanism (being software and/or hardware). Thus.

**Interviews**

Transcripts of interviews, which lasted from 45 min to almost 2 h, were coded by the researcher with the help of Atlas.ti (2016) software. Researchers (Miles and Huberman, 1994; Dent, 2011; Berg, 2009) have indicated that arrangement of codes will be subjective and may impact outcome, but as suggested by Miles and Huberman (1994), the researcher of the current study has tried to minimize bias by starting with a list of codes that are explicitly...
Is there a positive correlation between organizational culture and the perception of IG effectiveness?

Survey results

Four factors were associated with organizational culture: A- The organization is a welcoming place, B- The organization is dynamic, C) The organization is -oriented, and D- The organization is controlled and structured (Figure 1). Descriptive statistics reveal the following information (Table VI and Figure 9).

Trust has the highest mean ($M = 4.92, SD = 1.42$), which is closely clustered around the mean, indicating the most agreed upon characteristic of organizational culture in the HEI followed by Result Oriented ($M = 4.08, SD = 1.49$), Entrepreneurial characteristics ($M = 3.82, SD = 1.47$), and lastly, the Controlled characteristics ($M = 3.56, SD = 1.51$) showing a higher spread. Many respondents agreed that trust served as glue in the context of organizational culture. The entrepreneurial and dynamic characteristics of HEIs showed a gap in this regard, which emerged as a bimodal (NIST.gov, 2013), perhaps indicating that many organizations did not embrace entrepreneurship, and that there are those who highly welcome entrepreneurship. Result-oriented characteristics of organizational culture emerged as a well-rounded bell curve, indicating that the distribution is normal and, that participants regard the result-oriented characteristics as a common theme in regard to organizational culture.

The above research question (Is there a positive correlation between organizational culture and the perception of IG effectiveness?) was tested first by producing the cross tabulation between variable IG process, which is nominal, and organization culture, an interval variable. The Eta nominal by interval correlation was completed (Tedford, 2007) to learn about the effect size of organizational culture on the nominal variable of IG process.

The Eta correlation is a measure of association that was used as a test for this question to determine the nominal by interval association between the dependent variable IG processes (Table XI) and independent variable, organizational culture (four types A-D). Eta squared is

![Figure 8. Use of ILM software](image)
the proportion of the total variance that is attributed to an effect (Cramer, 2003). Results are presented in Table XI (Table VII):

Eta varies from 0, no effect, to +1, perfect association. In regard to impact of organizational culture on the last two processes of IG, information stewards and automated ILM, a Pearson correlation revealed that there a significant effect exists with a weak coefficient, where Pearson correlation \( R \) is 0.283 and \( p = 0.001 \). So based on the ETA in Table XI, we see that the effect size is not greater than 0.5, but this is not entirely insignificant. This is a case where we have a significant \( p \) value but a small correlation coefficient. Forest (2017) maintains that \( R^2 \) shows variability and even a low \( R^2 \) coefficient, indicating that a

noisy, high variability can have a significant trend. The trend indicates that the predictor variable still provides information about the response even though data points fall further from the regression line.

**Collaboration and team efforts**

One of the characteristics of organizational culture that became evident in the current study, coming from more than one subject, was the challenge in IG due to the presence of
<table>
<thead>
<tr>
<th>IV DV</th>
<th>Q1A-Presence of CISO</th>
<th>Q1B-Info governance council</th>
<th>Q1D-Chief Complaint officer</th>
<th>Q2-Info Stewards AND use of ILM SW</th>
<th>Results (accept/Reject hypoth.)</th>
</tr>
</thead>
<tbody>
<tr>
<td>OC-3A Collaborative/trust</td>
<td>( \eta = 0.175 )</td>
<td>( \eta = 0.144 )</td>
<td>( \eta = 0.166 )</td>
<td>( \eta = 0.147 )</td>
<td>ETA Square Nominal by Interval effect size</td>
</tr>
<tr>
<td>OC-3B Creative/Entrepreneurial</td>
<td>( \eta = 0.185 )</td>
<td>( \eta = 0.285 )</td>
<td>( \eta = 0.265 )</td>
<td>( \eta = 0.210 )</td>
<td>ETA Square Nominal by Interval effect size</td>
</tr>
<tr>
<td>OC-3C Compete/Result-Oriented</td>
<td>( \eta = 0.104 )</td>
<td>( \eta = 0.182 )</td>
<td>( \eta = 0.108 )</td>
<td>( \eta = 0.252 )</td>
<td>ETA Square Nominal by Interval effect size</td>
</tr>
<tr>
<td>OC-3D Controlled</td>
<td>( \eta = 0.175 )</td>
<td>( \eta = 0.148 )</td>
<td>( \eta = 0.258 )</td>
<td>( \eta = 0.311 )</td>
<td>ETA Square Nominal by Interval effect size</td>
</tr>
<tr>
<td>OC-All four items</td>
<td></td>
<td></td>
<td></td>
<td>0.283 Coefficient ( p = 0.001 ) value</td>
<td>Accepted, ( p = 0.001 ) Significant, low correlation</td>
</tr>
</tbody>
</table>
information silos. An information silo is defined as information stored and processed redundantly each with its own set of policies, which will lead to “inconsistency” (Vayghan et al., 2007). A few subjects discussed the efforts made to collaborate across their institutions despite the silo nature of information.

Concerns were also expressed by CISOs, attributing the lack of control over IG to “the silo nature of things.” One solution that Linda, a CISO, discussed, to alleviate this problem at the root, was the introduction and hiring of a director of IG. Linda stated that despite her efforts in collaboration with the CIO to connect across silos through initiatives that reach out to various department directors to pierce the silos and create an inter-operational information platform, HEIs need someone in charge, who starts from negative territories, breaking down existing barriers. Another subject, Suzanne, a CIO who was excited about IG processes and functions within her institution, explained that prior to her appointment about three years earlier, “...everything [operational and strategic decisions] went to the cabinet in a very silo fashion, and the parts and divisions do not work together well outside of their VPs division.” She empowered her staff through the spirit of teamwork. They work together to solve problems, and the team members develop close relationships across all the divisions of the college.

Participants emphasized that the foundation of IG initiatives was providing continuous collaboration of faculty, staff, and students.

It is very important for me to get them [faculty, staff and students] ample opportunity to express their opinions about IG policy... The liaison committee that I have has faculty representation and students and staff on it.

This CIO asserted that the process of IG was based on the culture that existed at her institution, an inclusion process. She highlighted that trust and transparency in her interaction and collaboration with the HEI community are major enablers in IG functions. Lack of communication was seen as lack of trust, particularly on behalf of faculty.

Lori, a compliance and record manager, explained that in her institution collaboration and innovation are considered a major cultural shift that her institution is committed to. However, she maintained that the shift in culture has not made the IG processes easier at her institution since interconnection across information platforms has not taken place. She cited lack of a specific information policy as the main obstacle to having a solid IG practice:

But the goal is to physically let people do what they're going to do and ask for forgiveness later, which I don't think really helps much from the governance perspective because nobody wants to make these decisions and nobody wants to restrict anything.

Creative and entrepreneurial
Interviewees expressed having an entrepreneurial culture within their organizations; however, the effect of that culture was not shared by most interviewees. For instance, Tony, a CTO, explained that his institution embraced scientific discoveries, and this promoted independent thinking, leading to more discoveries. When asked if his institution promoted an independent structure in IG governance, his answer was firmly negative.

Michael, a CIO, explained that he considers an entrepreneurial and creative culture as a policy in his institution:

We always challenge ourselves or, at least, I challenge all my staff, in that every year I expect one or two unique things to come out of them, something that no one else is doing, [something] that changes the way we utilize data or the way we work with people or how we deploy technology.
He also emphasized that he funded employees’ creative ideas and would encourage them to make prototypes of their creations. Michael displayed an involved entrepreneurial and innovative approach to all things, including IG. He mentioned that he had come from a management position at Stanford University, and that he had been on the job for over thirteen years. He had created a position of director of the Institutional Research (IR) and Consulting department and upgraded this position to a vice president who reported directly to the president rather than to the CIO. This allowed senior management to participate directly in IG processes. In the context of this study, the director of IR and Consulting was similar to IG Council director. This innovative move can be considered equal to the creation of an IG office. Another of Michael’s innovative strategies was to send IT staff to different departments (e.g., registrar, bursar) to serve as a liaison and learn the business of that department, making the IT individual business savvy, specializing in specific activities of the institution.

However, the entrepreneurial spirit was not evident in all interviewees. Only two subjects discussed embracing a creative approach to IG. One interviewee, a compliance officer, asserted, despite the institution’s reputation of promoting innovation, that governance was difficult since “IT does not know what is going on around the campus at any given time.” One of the reasons was the top-down approach to IT management. A few interviewees asserted that their IT department was going through a transition, from a decentralized to a centralized approach. Ann, a CIO, explained that her institution was going through a contraction, moving away from decentralization to a centralized state. She emphasized that her institution’s organizational culture demonstrated more controlled and structured characteristics than any of the other three organizational culture characteristics on which current study focuses.

**Competitive and result-oriented**

In regard to the result-oriented characteristic of the organizational culture of HEIs, some interviewees considered this characteristic as a core value since their organizations are science and data driven. They explained that making decisions based on data is a major part of their culture. The result-oriented characteristic leads IT authorities and staff to take charge to provide accurate information and take corrective action on any possible inaccuracies. In the case of some interviewees, this aspect of the culture is communicated when IT staff are hired. The IT department’s mission emphasizes the development of employees’ commitment to end-results. Michael explained that to support the mission of his department and to focus on being result-oriented, he tries to hire people with a PhD, MBA and field certifications and has high expectations for them. To enforce this attribute of organizational culture, those who indicated their commitment to results all indicated they have a review policy that identifies what particular IT staff have done to advance in their career.

Another sign in the current study of the result-oriented culture that prevailed was the presence of an Effectiveness Department. Marisol, an associate CIO, explained that her institution has started to invest in a department that would evaluate the accomplishments of actors in individual departments, including faculty, staff, and even upper management, to assess their progress. The Effectiveness Department was formed with IG in mind, to evaluate progress and, more importantly, governance of information in regard to compliance and risk management, and its findings were made available to the concerned parties. Another CIO maintained that the emergence of IG processes in her institution has created a sense of belonging for the IT staff. Prior to engaging in IG under the direction of the CIO, her staff lacked self-confidence and went to the cabinet for most of their IG-related decisions,
including security, complaisance, and IT governance. Thus, a commitment to contribute to the IG of the institution based on the accomplishments of IT staff, reveals the competitive and result-oriented characteristics of the organizational culture of the institution.

Structured and controlled
The Controlled aspect of organizational culture was supported by most participants. A few interviewees discussed the nature of IT departments as centralized and decentralized. This was particularly evident at larger HEIs that had major research arms. In one particular case, a CIO explained that a major restructuring of executive management had taken place, and that the president of the university had been changed. A substantive change instituted by this president and CIO was to implement a shift back to centralized control of the IT department. Many CIOs in this study perceived leeway and freedom in management as a contradiction to IG. Central control of IT represented a culture of control in many subjects’ positions. Another CIO, Roberto, explained, “We run centrally, so, yes, we are involved.” This notion was particularly evident in the case of information security. Roberto indicated that when central control is exercised on functions of IT, specifically on information security, the chance of having a “shadowy system” running within the information spectrum of the organization is removed.

Another CIO, Mary, while she characterized her institution’s culture as having a “centralized/decentralized control”, she explained that her institution was moving away from “extraction to a contraction stage” of IG due to budget constraints. She was from a state-run institution, and she emphasized the pressure due to the constraints of state funding. Mary explained that her institution in its current state of IG lacks trust. Steve, an IT compliance officer at a community college, explained that the culture of control is essential to ensure that an institution is in compliance in all aspects of IG. He emphasized that control is run centrally to include all affiliated community colleges.

Finally, according to the subjects of the current study, the culture of control is embedded in IT policies. Steve, an IT compliance officer, explained, “Historically, policies around IG are reckoned by central IT.” He emphasized that in an effort to improve IG policy implementation and assist IT to review policy, executive management have taken sole control from central IT to a wider university representation. This change of direction represents a culture of control inspired by collaboration.

Unfortunately, the issue of leaving policy to each director to enhance or revise was raised by several interviewees in the current study; such a practice can lead to disparate policy interpretation by these directors.

Conclusion
Study results indicate that result-oriented and controlled organizational culture was effective or at least perceived. Though some IT professionals at HEIs indicated that entrepreneurship was important for them and that several tactics were used to infuse IG within their organizational culture, this was not evident among the majority of the participants. This study provides indications of what measures HEIs need to take to build “a strong sense of accountability” as an effective information culture approach in building IG effectiveness. A result-oriented culture was evident when participants discussed “change to provide accurate information,” “[creating] positive change in the organization,” and “[getting] together to fight for success and solve problems”.

Results from this study confirms Oliver’s (2008) findings regarding the presence of information silos as a major concern related to the information culture of HEIs, which was discussed by many CIOs who took part. They also explained that they tried to break the
barriers by reaching out to various department heads and getting people excited and involved in IG. However, a large majority of participants, 91 per cent, indicated implementation of an Enterprise Resource Management (ERP) system as a solid approach to remove silos, a major improvement toward IG, as reported by Oliver.

Another important finding showed that automated information lifecycle management (ILM) is in its infancy in IG at HEIs. This was not a major surprise, as, currently, record information management (RIM) programs are not commonly established at HEIs. Some institutions indicated their inability to progress in RIM is connected to the culture of the organization; for instance, the culture is “to keep everything.” Specific policies relating ILM and RIM were not present in many institutions, creating a major obstacle in IG, as, in many instances, destruction of documents is left to individual departments to decide. Furthermore, the study showed that CISOs’ interaction with ILM is minimal; despite that, 68 per cent of the institutions had a CISO role within their IT department.

Some CIOs from smaller HEIs were successful in building effective collaboration both among their staff and throughout the institution. However, this success was not reported by everyone, particularly those from medium and large institutions, where the creation of an IG director was a needed measure to remove silos. Connecting with faculty, staff, and students is essential in creating an inter-operational platform where data can move across different parts of the organization. This task was made possible by creating various committees with representation from faculty, students, and staff. Breaking down silos was a requirement for institutions, particularly for the larger ones, in order to use innovation as a cultural shift in the organization and have a positive effect on IG processes. The current study’s findings confirm that, much like in healthcare (Brailer, 2005), interoperability is the key to breaking down information silos. However, besides use of technology, which will provide network and data interoperability, the presence of an organizational culture that nourishes collaboration, trust, and inclusion serves as an important vehicle in effective IG.

The last aspect of organizational culture was Structured and Controlled, with which participants indicated a strong affiliation by discussing “[a] strong value toward shared governance,” “culture as centralized,” “highly controlled and structured,” “the CIO developed policies on how IT is going to be structured,” and “standardized control makes it easy to do that [IG].” This element of organizational culture was revealed strongly in both quantitative and qualitative parts of the study, which confirms findings of other researchers (Cameron and Quinn, 2011; Capelo, 2012; Giordano, 2015). They found the controlled and structured aspect of the institution an aspect of organizational culture to solve problems, which is highly encouraged by executives.

References
Berg, B.L. (2009), Qualitative Research Methods for the Social Sciences, Pearson, Boston.


Further reading


Corresponding author
Ali Daneshmandnia can be contacted at: Daneshmandnet@gmail.com
Appendix 1

List of code families and affiliated codes, created using report tool of Atlas.ti

### Code Family: H1B - Organizational Culture
Created: 2016-06-08 18:58:01 (Super)
Codes (28): [Best Practice: communication/training of IG with college community] [OC- of HEI - culture of diversity] [OC- of HEI telephone preferred over email] [OC- Culture is my favorite topic] [OC- Governance can transform the culture of HEI] [OC- IG is bringing people together] [OC- of HEI problems exist] [OC- of HEI collaborative, sharing] [OC- of HEI Communication leads to trust] [OC- of HEI-entrepreneurship] [OC- of HEI-IG policy] [OC- of HEI-Role of trust building effective IG] [OC- of HEI faculty perspectives] [OC- of HEI sense of community/family exist] [OC- of HEI_result oriented] [OC- of HEI_D organization is controlled and structured] [OC- of HEI_Data driven] [OC- of HEI role of trust in building effective IS practices] [OC- of HEI_social justice values] [OC- of HEI_contribute directly to effective IG governance] [OC- of HEI_culture of happiness] [OC- of HEI_Glue_loyalty] [OC- PROMOTE compassion] [OC- promotes excellence] [OC- Trust and accountability] [OC-promoting One University] [OC-transition state from less trust to more trust]
Quotation(s): 162

### Code Family: H2 - Presence of CISO, about CISO
Created: 2016-06-09 12:02:35 (Super)
Codes (6): [Chief Information security officer (CISO) presence] [CISO needed to manage info security] [CISO professional involvement/capacity] [CISO, External partnership initiatives] [CISO, external partnership IS as service] [executive IS approach]
Quotation(s): 42

### Code Family: H2 - RIM Program in place
Created: 2016-06-09 12:03:08 (Super)

### Code Family: Best Practice
Created: 2016-06-09 12:06:52 (Super)
Codes (2): [FISMA: Federal Info Security Management Act] [IG strategies: Communication and collaboration with CIO outside groups (Educause, NJH)]
Quotation(s): 9
### Information Governance Process

In the following table, please check the Yes or No box next to each item (only one response per statement please).

<table>
<thead>
<tr>
<th>No. of Question</th>
<th>Question</th>
<th>YES</th>
<th>No, but we are in process of selecting/forming one</th>
<th>No, but we are considering selecting/forming one</th>
<th>No, nor we have plan to select/form one</th>
</tr>
</thead>
<tbody>
<tr>
<td>1A</td>
<td>In our institution someone has been appointed to be responsible for Information security, Chief Information Security Officer (CISO)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1B</td>
<td>At our institution we have an Information Governance council</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1C</td>
<td>Does your organization have a Record Information Management (RIM) program?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1D</td>
<td>Does your institution have a Compliance officer, or Chief compliance officer?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>No. of Question</th>
<th>Question</th>
<th>Total disagree</th>
<th>Somewhat disagree</th>
<th>Neither agree nor disagree</th>
<th>Somewhat agree</th>
<th>Totally agree</th>
</tr>
</thead>
<tbody>
<tr>
<td>2A</td>
<td>In our institution have information stewards, who actively collaborate with IT, Record Information Management (RIM) or Information Governance department (if exist).</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2B</td>
<td>Our organization automated identification (often accomplished through software) of paper and electronic records eligible for destruction (e.g., boxes stored off-site, files stored on-site, Electronically Stored Information (ESI))</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Organizational culture**

3. Please state your agreement with the following statements by selecting from 1 (totally disagree) to 7 (totally agree) (only one response per statement please):

A. The organization is a welcoming place. The glue that holds the organization together is trust.
   - 1- Totally disagree,
   - 2- Mostly disagree,
   - 3- Somewhat disagree,
   - 4- Neither agree nor disagree,
   - 5- Somewhat agree,
   - 6- Mostly agree,
   - 7- Totally agree,

B. The organization is a dynamic and entrepreneurial place. People are willing to stick their neck out and take risks.
   - 1- Totally disagree,
   - 2- Mostly disagree,
   - 3- Somewhat disagree,
   - 4- Neither agree nor disagree,
   - 5- Somewhat agree,
   - 6- Mostly agree,
   - 7- Totally agree,

C. The institution is very result oriented. A major concern is with getting the job done. People are very competitive and achievement oriented.
   - 1- Totally disagree,
   - 2- Mostly disagree,
   - 3- Somewhat disagree,
   - 4- Neither agree nor disagree,
   - 5- Somewhat agree,
   - 6- Mostly agree,
   - 7- Totally agree,

D. The organization is very controlled and structured place. Formal procedures generally govern what people do.
   - 1- Totally disagree,
   - 2- Mostly disagree,
   - 3- Somewhat disagree,
   - 4- Neither agree nor disagree,
   - 5- Somewhat agree,
   - 6- Mostly agree,
   - 7- Totally agree.

(continued)
18. Who sponsors or "champions" information governance within your institution? Please choose all that apply.

[ ] Board/Executive Management Team
[ ] Chief Executive Officer/Director General
[ ] Chief Information Officer
[ ] Legal/Compliance Officer
[ ] IS/IT Manager Internal
[ ] Auditor Records
[ ] Manager Other (please specify)

Part 2: Basic Information and demographics

19- Size of Institution (number of students) (based on Carnegie Classification):

[ ] Very small two-year (VS2)- fewer than 500 Full time Equivalent (FTE)
[ ] Small two-year (S2)—at least 500 but fewer than 2000 FTEs attend this two-year institution.
[ ] Medium two-year (M2)—at least 2000 but fewer than 5000 FTEs attend this two-year institution.
[ ] Large two-year (L2)—at least 5000 but fewer than 10000 FTEs attend this two-year institution.
[ ] Very large two-year (VL2)—10000 or more FTEs attend this two-year institution.
[ ] Very small four-year (VS4)—fewer than 1000 FTEs attend this four-year institution.
[ ] Small four-year (S4)—at least 1000 but fewer than 3000 FTEs attend this four-year institution.
[ ] Medium four-year (M4)—at least 3000 but fewer than 10000 FTEs attend this four-year institution.
[ ] Large four-year (L4)—more than 10000 FTEs attend this four-year institution.
[ ] I do not know.

20- Please identify type of institution (select only one):

[ ] Public Institution
[ ] Private Institution, not-for-profit
[ ] Private Institution, for-profit

21- What is your institution’s Carnegie foundation ranking? (Please select one)

[ ] Research Universities (RU/VH) very high research activity
[ ] Research Universities (RU/H) - high research activity
[ ] Doctoral/Research Universities (DRU)
[ ] Master's Colleges and Universities
[ ] Baccalaureate Institutions

22- Please indicate which of the following accreditation agencies does your institution belongs to:

[ ] Middle State Commission on Higher Education
[ ] Department of Higher Education of respective state
[ ] New England Association of Schools and Colleges
[ ] Others Please list____________________________________________________________

23- Please select one of the following titles as your main title in your institution:

[ ] Chief Information Officer
[ ] Associate CIO
[ ] IT Director
[ ] Chief Security Information Officer (CSIO); Compliance Officer
[ ] VP of Finance and Facilities
[ ] IT Project Manager
[ ] Help Desk Manager
[ ] Other: Please specify: _______________________

24- Please indicate who you report to in your institution.

[ ] President/Chancellor
[ ] Chief Financial Officer
[ ] Provost
[ ] Information Officer (CIO)
[ ] Chief

25- Number of years in the profession (Please check one)

[ ] 1-9
[ ] 10-19
[ ] 20-29
[ ] 30 & more
[ ] No Answer

26- Age (Please choose one)

[ ] <18
[ ] 18-29
[ ] 30-44
[ ] 45-60
[ ] >60

27- Gender

[ ] female
[ ] Male

28- What is highest degree that your institution offers?

[ ] Associate
[ ] Baccalaureate
[ ] Master
[ ] Doctoral
[ ] Post-Doctoral

29- Would you be willing to participate in the interview section of this research?

[ ] Yes
[ ] No, If YES, Please kindly email researcher
The defensible deletion of government email

James Lappin, Tom Jackson, Graham Matthews and Ejovwoke Onojeharho
Loughborough University, Loughborough, UK

Abstract
Purpose – Two rival approaches to email have emerged from information governance thought: the defensible deletion approach, in which emails are routinely deleted from email accounts after a set period of time; and the Capstone approach, in which the email accounts of important government officials are selected for permanent preservation. This paper aims to assess the extent to which the defensible deletion approach, when used in conjunction with efforts to move important emails into corporate records systems, will meet the needs of originating government departments and of wider society.

Design/methodology/approach – The paper forms the first stage of a realist evaluation of policy towards UK government email.

Findings – The explanation advanced in this paper predicts that the routine deletion of email from email accounts will work for government departments even where business email is inconsistently or haphazardly captured into records systems, provided officials have access to their own emails for a long enough period to satisfy their individual operational requirements. However the routine deletion of email from email accounts will work for wider society only if and when business email is consistently captured into other systems.

Originality/value – The paper looks at the policy of The National Archives (TNA) towards UK government email and maps it against the approaches present in records management and information governance thought. It argues that TNA’s policy is best characterised as a defensible deletion approach. The paper proposes a realist explanation as to how defensible deletion policies towards email work in a government context.

Keywords Archives, Records management, Automation, Information governance, Electronic mail, Realist evaluation

Paper type Research paper

Method
This paper forms the first stage of a realist evaluation of archival policy towards UK Government email.

Realist evaluation is a logic of enquiry developed by sociologists Ray Pawson and Nick Tilley (Pawson and Tilley, 1997). Pawson and Tilley argue that in the social world, a policy or programme achieves its intended outcome only if targeted stakeholders respond to it in ways intended by policymakers. If policymakers misread the reasoning and likely reactions of targeted stakeholders, then the policy may have unwanted effects (Pawson, 2006, pp. 27-28).

The UK National Archives (TNA) advises government departments to capture important emails into corporate records systems whilst routinely deleting email from email accounts.
This paper presents an initial theory of how government departments are likely to react to such a policy. It asks whether they are likely to give:

- an intended response (taking serious and effective steps to ensure that important emails are captured into record systems, and promptly deleting emails from email accounts); and
- an unintended response (making token efforts to capture important emails into record systems, whilst retaining emails within email accounts for a period judged sufficient to satisfy the operational needs of individual officials).

Realists believe that no policy works for all stakeholders in all circumstances. This paper asks whether, in current circumstances, TNA’s policy towards government email is likely to work for government departments and whether it is likely to work for stakeholders seeking to hold those departments to account.

Scientific realists believe, after Popper, that scientists in both the physical and social sciences make advances by developing new theories and by exposing the predictions made by those theories to test (Pawson, 2013, pp. 3-5 and p. 9). Realist evaluation is a theory-driven evaluation method in which the researcher first develops an initial “programme theory” of how the policy under evaluation works and then exposes that theory to test.

This paper maps TNA’s policy towards government email against the broad approaches to email present in records management and information governance thought and argues that it is best characterised as a defensible deletion approach. The explanation presented in this paper was built through an exploration of the points of contention between the defensible deletion approach and the alternative Capstone approach that was adopted by the US National Archives and Records Administration (NARA) in 2013 (NARA, 2013). The points of contention are compiled from rival ideas found in the professional discourse on archival policy towards email.

This approach to building an initial theory through examining points of contention in an existing policy debate was recommended by Pawson as a way of ensuring that research was relevant to the questions upon which policymakers have to make decisions (Pawson, 2013, pp. 165-167).

This paper develops an initial explanation of how defensible deletion policies towards government email work and sets out ways in which this explanation could be tested.

**Records management perspectives**

*Records management perspectives on how correspondence should be organised*

The 1990s saw academics and practitioners working to establish record-keeping approaches to support organisations in coping with the digital revolution that was being ushered in by the widespread adoption of email.

David Bearman argued that record-keeping requirements arose from business activities, and that email accounts were problematic to manage because they typically contained correspondence from a mixture of different business activities. He stated that:

> We cannot make any progress in managing electronic mail unless we can make the system identify the business transaction involved (Bearman, 1994).

Bearman’s insistence that records be linked to the business activity that they arose from was mirrored in the DIRKS methodology for the design and implementation of record-keeping systems. The methodology was developed in Australia in the early 1990s and was later embedded in the International Records Management Standard (ISO 15489). Step B of the DIRKS methodology involved the analysis of an organisation’s activities and the construction
of a hierarchical business classification scheme. The methodology was maintained and updated well into the twenty-first century (State Records Authority of New South Wales, 2003).

Luciana Duranti (1997) argued that one of the functions of a record system was to create an “archival bond” between the different records of an organisation, by which every single document in the system had a relationship with all other documents within the system. Both Boudrez (2006) and Grandi (2011) used Duranti’s theory of the archival bond to argue that important emails should be saved into a records system organised by a business activity where they can be related to all other records arising from the same instance of a particular business activity.

The electronic records management system model

Duranti and her University of British Columbia project team collaborated with the US Department of Defense to produce the US DoD 5015.2 standard, which outlined the functional requirements of electronic records management systems (Department of Defense, 1997).

The electronic records management model became the standard approach for government bodies in societies such as the US, UK and Australia. In the first decade of the twenty-first century, many government bodies in these administrations aimed to implement electronic records management systems on a corporate-wide basis and instructed their officials to move important emails into those systems. Since that time, however, the approach has come in for widespread criticism.

Baron and Attfield reported that:

Anecdotal experience with DOD Standard 5015.2 applications has shown that many individuals do not reliably save, tag, drag or drop most of their email into electronic folders set up with well-intentioned archival purposes in mind. The compliance rate starts off low in this regard, and is invariably getting lower – simply due to massive volumes of information now confronting us all. Having to perform extra key strokes, no matter how few, on any substantial percentage of electronic communications during the working day, means the equivalent of having to pay a transactional toll per communication, in terms of lost time, energy and productivity. Few individuals wish to pay the price on a consistent and comprehensive basis, hence a world of incomplete if not haphazard recordkeeping (Baron and Attfield, 2013, p. 583).

Don Leuders worked as a records management consultant, specialising in DoD 5015.2 electronic records management system implementations. He became a strong critic of the electronic records management system approach. In a 2015 blogpost, he argued that:

Manual email records management solutions will fail to be adopted by end users 100 per cent of the time. Short of sticking a gun to their head, no information worker is ever going to manually declare and classify email records (Leuders, 2015).

In 2015, Sir Alex Allan, in his review of UK Government’s digital records, found that the instruction to officials to move email into electronic records management systems “seems to have been complied with even less rigorously than for other records” (Allan, 2015 p. 10).

In 2010, in the pages of this journal, James Lappin described the vacuum in records management thought and practice left by the decline and fall of the electronic records management system approach and asked “What will be the next records management orthodoxy?” (Lappin, 2010). In fact, the new paradigm that emerged to fill the vacuum has gone under the name of information governance and does not think of itself as a records management paradigm.
Information governance perspectives

Information governance can be seen at one and the same time as:

- an umbrella discipline that contains records management as one of its component disciplines, alongside other disciplines such as data protection/privacy, data governance etc.;
- an evolution of records management in which records management is updating itself to adapt to the digital age; and
- a rupture with records management that seeks to abandon certain records management beliefs deemed unsuitable for the digital age.

A look at some of the landmark outputs of information governance thought and practice documents such as the Electronic Discovery Reference Model and Information Governance Reference Model (Duke Law, 2018), NARA’s Electronic Records Management Automation Plan (NARA, 2013), the ARMA Information Governance Maturity Model (ARMA International, 2013) and the Sedona Conference Principles and Commentary on Defensible Disposition (Sedona Conference, 2018), reveals key differences between the concerns and ambitions of records management writers of the 1990s and the concerns of information government writers of the second decade of the twentieth century.

Notably absent from the above information governance outputs is:
- any insistence that records be organised by business activity; and
- any attempt to distinguish between records and non-records or between records systems and non-record systems.

In their place comes:
- a recognition that any and every information system holds information that needs to be governed in accordance with information governance principles; and
- a belief that only automated techniques can scale up to managing the volumes of content created and received by twenty-first century organisations.

The information governance perspective does not require that organisations attempt to concentrate their records within one corporate records system. It acknowledges that records are likely to be kept in a variety of business applications that hold a variety of information from a variety of different activities in a variety of formats. The information governance response to this situation has been to focus on developing high-level principles that can be applied in a variety of different environments.

ARMA’s Information Governance Maturity Model evolved out of their ‘Generally Accepted Record-keeping Principles’ (GARP). One of the eight GARP principles states:

An organization shall maintain its records and information for an appropriate time, taking into account legal, regulatory, fiscal, operational, and historical requirements (ARMA International, 2017).

Two rival policy approaches to email have emerged from information governance thinking:

1. the defensible deletion (also called defensible disposition) approach, by which emails are routinely deleted from email accounts after a set period of time; and
2. the Capstone approach, where the email accounts of important government officials are selected for permanent preservation.
Neither of these two approaches is perfect, and the preference expressed in many of the documents cited above is for automated solutions if/when they become serviceable. The next section looks at the existing state of play with automation, before looking at the two policy approaches in more detail.

The search for automated approaches
Automation is a broad term. There are many different potential purposes for the deployment of automation in relation to email and many different automation methods to support those purposes.

Brogan (2009) and Baron and Attfield (2013) have regarded the simple act of capturing each email into an email archive as “automation”. NARA categorised the Capstone approach as an automated approach (NARA, 2013, p. 11), presumably because it captures emails as records without end-users having had to take any action.

Any development of an automated capability to identify and classify important emails would offer the prospect of bringing back to life the electronic records management system model and the ambition of integrating emails with other records arising from the same business activity. However, commentators seem to have little confidence that a corporately scalable analytics, machine learning and/or search capability has yet emerged to automatically identify and classify important emails.

Leuders writes:

Automated record classification using content analytics products doesn’t work for emails [. . .]. Even the best content analytic products require a minimum level of information to ‘understand’ and classify any item with an acceptable level of confidence. And given the extreme brevity and routine informality of most emails, the truth is they can very rarely be classified successfully in any real-world implementation (Leuders, 2015).

In 2017, the UK Cabinet Office wrote:

Some have argued [. . .] that it would be more effective to automate information management completely and remove general civil servants from the process. Although appealing, this is currently unfeasible in practice: technology (specifically the inability of analytics tools to identify context) is not powerful enough to remove any need for proper naming and saving (Cabinet Office, 2017, p. 15).

The defensible deletion approach to email
The defensible deletion approach to email is based on the belief that emails accumulated in email accounts are of low value but high risk to the originating organisation, and that it is in the organisation’s interests to delete them as soon as is operationally practical, whilst exempting from deletion emails for which there exists an ongoing legal obligation to retain.

Defensible deletion and information governance
The Sedona Conference stated that:

The effective, timely, and consistent disposal of physical and electronic information that no longer needs to be retained should be a core component of any Information Governance program (Sedona Conference, 2018).

They stated three principles for the defensible disposition of information:

(1) When a legal retention or preservation obligation is absent, organisations may dispose of their information.
When designing and implementing an information disposition program, organisations should identify and manage the risks of over-retention.

Disposition should be based on information governance policies that reflect and harmonise with an organisations’ information, technological capabilities and objectives (Sedona Conference, 2018).

The rationale behind the defensible deletion of email

Turner (2014) quotes two cases where US courts had declined to take sanctions against an organisation that had been unable to produce email correspondence requested by the other party because they had deleted it under a routine deletion policy. He argued that deletion of information was likely to be acceptable by a court provided it was “neutral, systematic and universally applied” and provided legal holds were applied when required.

An example of a defensible deletion approach to email in a government context was provided in a listserv post by a practitioner (Records Management UK listserv, 2015). The practitioner vividly described the inconvenience, cost and risk to an organisation of retaining email in email accounts:

We brought in email archiving here to save £1m in storage costs (e-storage is cheap, eh?). We later brought in a seven-year deletion rule for archived emails because the archive could not cope with the quantity of emails, as well as our compliance and legal teams, who were having to plough through millions of rubbish emails for Freedom of Information, Data Protection Act or e-discovery. We advise that emails of value must be saved outside the archive in the relevant shared storage area (but with only two records managers, we cannot monitor or enforce this).

The approach of the above organisation is better characterised as a defensible deletion approach than an electronic records management system approach. The organisation was asking its officials to move important emails into record systems, but no confidence was placed in the adequacy of the capture of important emails into corporate records systems or shared areas. The justification for the routine deletion of email was the cost, risk and inconvenience of the retention of emails beyond the seven-year period.

The Capstone approach to email

The ideas behind the Capstone policy

In a 2011 presentation, Jason Baron, the then NARA’s Director of Litigation, set out a new policy approach to email, which later became known as the “Capstone” approach.

Baron proposed that all emails created or received by senior officials be designated for permanent preservation. One downside of retaining the email account of a senior official permanently is that the email account is likely to contain personal and trivial mail. Baron proposed that:

Agencies concerned about over-inclusion of email of a personal or truly ephemeral nature could allow for staff to delete emails from the in-box for a limited period of time (e.g. 60 or 120 days) with any emails remaining then automatically captured as permanent (Baron and Attfield, 2013 p. 587).

National Archives and Records Administration’s Capstone policy for the email of federal agencies

In August 2013, NARA announced its Capstone policy on email, via a bulletin issued to heads of US federal agencies. The bulletin asked agencies to schedule the email accounts of
officials at or near the top of an agency for permanent preservation and allowed agencies to determine for themselves whether those officials could delete non-record, transitory or personal email from their accounts (NARA, 2013).

In NARA’s own Capstone implementation, they identified 48 roles as being Capstone roles and gave those 48 officials a “safe harbor” period, during which they could delete emails they regarded as personal or trivial, prior to emails being archived (Sullivan, 2014).

The Capstone retention schedule
In April 2015, NARA issued a Capstone retention schedule to federal agencies (NARA, 2015). The schedule set out three retention rules for federal email:

- (1) Email in the email accounts of senior officials should be retained permanently.
- (2) Email in the email accounts of other officials (with the exception of officials in support and administrative roles) should be retained for seven years.
- (3) Email in the email accounts of support and administrative roles should be kept for three years.

Key features of the Capstone approach
Three distinct features of the Capstone approach are that it:

- (1) endeavours to make email accounts manageable, whereas the electronic records management system approach and the defensible deletion approach had both argued that email accounts were unmanageable;
- (2) focusses end-users on identifying trivial and personal email to be deleted from email accounts, whereas previous approaches had focused end-users on identifying important emails to move into a records system; and
- (3) makes no attempt to assign emails to the business activity that they arose from—email accounts are subject to retention rules that are based on the roles carried out by the account holder.

Policy towards UK Government email
TNA has kept an unchanged policy to email throughout the past two decades, that important emails should be moved into corporate records management systems whilst emails in email accounts should be subject to routine deletion. During this time, the thinking of TNA towards information management in general has changed considerably, in line with a general shift from records management to information governance thinking.

In the first half of the first decade of the twenty-first century, TNA policy on email drew its justification from the electronic records management system approach. At the time, TNA was running a certification regime for electronic records management system products, and belief in the electronic records management system model was strong amongst the practitioner community, the vendor community and the academic community.

In the second decade of the twenty-first century, belief in the electronic records management system model faded, and TNA’s policy on email now appears to draw its justification from a defensible deletion logic. TNA’s latest restatement of its email policy came in 2016, when it issued its guidance principles on the auto-deletion of email (TNA, 2016). These guidance principles were sandwiched between two important reports: Sir Alex

Sir Alex Allan found the capture of email into government electronic records systems to be ineffective and recommended that the government consider adopting a Capstone approach to email (Allan, 2015, p. 10). The Cabinet Office in response made no denial that the capture of emails into record systems was ineffective, but rejected Allan’s Capstone recommendation on the grounds that the selection of important email accounts for permanent preservation was likely to cause personal and trivial correspondence to be retained longer than necessary. In the opinion of the Cabinet Office, this over-retention would be contrary to UK data protection principles, the General Data Protection Regulation and UK public records legislation (Cabinet Office, 2017, p. 10).

TNA’s Guidance Principles state that “under an auto-deletion rule information of value must be identified and not deleted” (TNA, 2016). However, nowhere in the Guidance Principles is there a mention of any mechanism that would make deletion of emails from an important email account conditional upon adequate capture of correspondence from the account into an electronic records management system.

There is one paragraph that deals with capture:

Automatically capture emails – Implement technologies that integrate your email and EDRM solutions. Solutions that allow emails to be dragged and dropped or automatically captured into the corporate records area will assist in allowing users to comply with your records management and retention policies (TNA, 2016).

We have seen that the Cabinet Office, writing a year after these guidelines, had no faith that the process of record capture could be automated. “Drag and drop” is a manual process rather than an automated process, and Allan had found the capture of email into record systems to be ineffective despite the deployment of “drag and drop” by many government departments.

**Exploring the points of contention between the defensible deletion and Capstone approaches**

*The proportion of email correspondence that needs to be treated as a record*

There is little significant difference between the defensible deletion and the Capstone approach when they are applied to the email accounts of officials that are not dealing with matters of which government departments/agencies are expected to keep a permanent record. Both approaches would typically result in the deletion of the contents of such email accounts after a relatively short number of years.

There is a very significant difference between the defensible deletion approach and the Capstone approach when applied to the email accounts of officials that are dealing with matters of which government departments/agencies are expected to keep a permanent record. In the continued absence of automation:

- a defensible deletion approach is likely to result in the deletion of most of the contents of such accounts after a relatively short number of years (saving only those emails which have, by exception, been moved to a corporate record system or placed under some sort of legal hold); and
- a Capstone approach is likely to result in the permanent retention of most of the contents of the email accounts of such officials (saving only those emails which have, by exception, been identified as personal or trivial).
When applied to the email accounts of officials in important government roles, defensible deletion, in the absence of automation, is likely to result in an under-retention of correspondence of historic value. At the time of writing, the predominant method for identifying important emails is to ask officials to move such emails into a corporate record system. This method has been sharply criticised by commentators, as related above, and evidence suggests it is inadequate for the task.

A Capstone approach would also be dependent on the judgement of officials – this time to identify trivial and personal items of correspondence. We can anticipate that it would in most cases result in an over-retention of trivial and personal email (although it is also possible that in some cases, officials may be tempted, or instructed, to use the safe harbour period to delete politically contentious correspondence).

In adjudicating between a Capstone policy and a defensible deletion policy, the key judgement to be made concerns the extent to which email correspondence has value (or lacks value). This question can be formulated as follows: is society likely to need, for the purposes of historical accountability, to have the major part of the correspondence of the key officials of its administration retained permanently? Or would the retention of a minority of the correspondence of key officials suffice?

Different perceptions of the value of email
The views of information governance commentators, archivists and records managers are sharply divided when it comes to the question of the extent to which email correspondence has value.

The listserv post quoted above spoke of the millions of “rubbish emails” that cluttered up the organisation’s email archive (Records Management UK listserv, 2015).

Leuders holds a similar view of the lack of value possessed by email in email accounts:

Very few emails actually hold any real long term value ... in reality, all but an extremely small number of emails at almost any given organization are worthless soon after they are sent. Yep, worthless. What’s more, with a few simple, strategic records management policies in place, those few emails could likely be eliminated, too (Leuders, 2015).

Leuders holds that emails are not only worthless but also potentially dangerous:

People tend to write really stupid stuff in emails. Far more idiotic stuff then they would write anywhere else (Leuders, 2015).

However, there is evidence that those elements in society who seek to hold the government to account regard email accounts as a valuable record. Andrew Waugh, policy manager for the Public Record Office of Victoria in Australia, wrote that:

Evidence of the value of email systems as record systems can be found in any modern governance or accountability investigation, such as a royal commission, audit report, ombudsman’s investigation, or even in investigative journalism. Without exception, emails form the key planks of a modern investigation and feature prominently in the final report. In 2012, the then Victorian Auditor General and Victoria’s Deputy Ombudsman, independently, told a seminar of Victorian records professionals that, while their investigators looked at the records [in electronic records management systems], the smoking gun was always in the email (Waugh, 2014).

The difference in viewpoint between Leuders on the one hand and the Victorian Auditor General on the other can be identified as a simple difference of interest: an auditor is looking for smoking guns, whilst a records manager is working for organisations who may be concerned about what smoking guns lurk unnoticed in their email servers.
Cox identified back in 2008 the possibility of a divergence of interests in relation to email correspondence with records managers, thinking of their own organisations' interests, wishing to destroy correspondence in email accounts after a relatively short time; and archivists, thinking of society's interests preferring to protect and preserve important email accounts (Cox, 2008).

In the next section, this paper hypothesises that the polarisation of views on the value of email is a consequence of the fact that the switch of correspondence medium from hard copy to email radically increased the cost and risk to originating organisations of keeping correspondence. This cost and risk is born by originating organisations, not by external society. It hypothesises that from society's point of view, the value of correspondence appears to be undiminished after the move from hard copy correspondence to email.

Towards an explanation for differing perceptions of the value of email

The disintermediation and decomposition of correspondence

The coming of email in the 1990s brought with it the “3vs” – volume, velocity and variety – which Laney (2001) argues characterises information in the digital age. Email disintermediated correspondence, collapsing the time and space between sender and recipient and removing the intermediaries between them.

This disintermediation increases the velocity of correspondence by allowing recipients to reply to an email within minutes. Any increase in the velocity of correspondence leads to an increase in the volume of correspondence exchanged within any one day, month and year. In effect, correspondence is decomposed into smaller units.

This paper hypothesises that greater the velocity of correspondence, the less time individuals have to think about what they are writing and the less guarded each individual item of correspondence becomes.

It can therefore be expected that the correspondence of any given senior official poses a greater risk to a government department after the coming of email than would the correspondence of a similar senior official before the coming of email.

The value of email in aggregation

This paper makes the hypothesis that the total value of the correspondence exchanged by a senior official after the coming of email is neither significantly greater nor lower than the total value of all the correspondence exchanged by a similar senior official before the coming of email.

This hypothesis can be tested in a thought experiment. The hypothesis implies that if the UK had decided to exit the European Union prior to the coming of email (e.g. in 1989), the historical value to society of the correspondence of a senior official working on aspects of UK strategy for the exit would have been neither greater nor lesser than the historical value of the email correspondence of an official charged with a similar task in 2016.

The average number of items of correspondence exchanged per day has been exponentially larger after the adoption of emails than before. It can therefore be predicted that the average value of each item of correspondence is exponentially smaller after the adoption of email than before.

If this theory of the decomposition of correspondence is true, then two consequences logically follow:

1. The email correspondence of a senior official may still have immense value in aggregation, even while individual emails within the account lack any appreciable value of their own. The perception of Leuders that emails are worthless is not therefore in contradiction with the perception of the Victorian Auditor General that email accounts are more valuable to an investigation than are corporate record systems; and
Any approach that seeks to identify emails of exceptional importance to move into a record system is unlikely to enable the adequate reconstitution of the business correspondence of a senior official.

**Predicting the reaction of government departments to The National Archives policy towards email**

*The possible reactions open to government departments*

An archival policy advising government departments to move important emails into corporate record systems whilst deleting those emails that remain in email accounts could result in one of three responses from government departments, only one of which is the intended response. The department could:

1. take serious and effective steps to move business emails into corporate record systems accompanied by the short-term deletion of email from email accounts;
2. make token efforts to move business emails into corporate record systems, accompanied by the routine deletion of email from all email accounts; and
3. make token efforts to move business emails into corporate record systems accompanied by the retention of some, most or all email accounts as records.

The next section attempts to identify whether government departments are likely to routinely delete emails from email accounts and then attempts to predict whether departments are likely to take serious steps to move business emails out of email accounts.

**The deletion of email from email accounts**

Email accounts are the first method of organising correspondence in the history of government record-keeping that does not allow an official new-to-post to view the correspondence of their predecessor (refer to Zhang, 2015, for a history of the organisation of correspondence in the USA). The fact that personal correspondence is typically present in individual email accounts means that the email account of any official cannot usually be made accessible to their successor.

Waugh wrote that the time periods set for the deletion of emails from email accounts are usually absurdly short and certainly not based on any analysis of the functions the records support (Waugh, 2014). TNA stated in 2016 that the period after which UK Government deleted emails from email accounts varied from department to department but was “currently ranging from 90 days to four years” (TNA, 2016, p. 2).

The deletion of the correspondence of, say a senior government economist, after four years or less does indeed look to be an “absurdly short” period when compared with how long the correspondence of such an official is likely to have been kept before the coming of email. However, there is a pragmatic reason behind this absurdity. The retention of an email account, even of a very important official, gives no benefit to a government department for day-to-day operational purposes once the individual email account holder has left his/her post.

This paper hypothesises that:

- Government departments are indeed likely to delete emails routinely from email accounts as intended by the TNA’s policy, but for different motivations than TNA intends.
- The deletion will be carried out irrespective of how low a percentage of business correspondence is captured into corporate record system or other shared areas.
The deletion happens not because the department is confident that business email is adequately captured into corporate records systems, but because the department knows that the retention of email in email accounts brings them no operational value once an individual official has left his/her post.

**The capture of business emails into corporate record systems**

The findings of Sir Alex Allan's review of government digital record-keeping (Allan, 2015) suggest that the UK Government departments have not taken effective steps to move important emails into record systems. One way of interpreting this would be to argue that the hypothesis advanced in this paper (that the email correspondence of an important official has value in aggregate) must be wrong on the following grounds:

- If a record is important enough to have permanent value to society, it will also be important to the originating government department, at least in the short to medium term.
- The willingness and ability of government departments to function with only a tiny minority of their business correspondence being captured into a record system implies that only a tiny minority of an official’s correspondence is needed as a record.

An alternative reading, however, is that the reason why government departments have not taken effective steps to capture business emails into record systems may be because their officials are able to refer to emails in their email accounts for all or most of the period in which their correspondence is likely to be of most use to them, namely, the two years after the correspondence is sent and received. In this hypothesis, government departments are using email systems as record systems, without treating them as record systems.

Baron and Attfield described this phenomenon when they wrote about email archive tools. These tools enabled organisations to store the bulk of the contents of email accounts outside of their live email servers by simply capturing every email sent or received into the archive. Baron and Attfield argued that an email archive would be perceived to be an institution’s state-of-the-art records management scheme, and it would be increasingly difficult to convince end-users to continue any semblance of other means of record-keeping in the face of the knowledge that email archiving exists (Baron and Attfield, 2013, p. 583).

Baron and Attfield predicted that emails in email archives would be like “fireworks” – very important for a short period of time, but leaving no permanent trace behind them. They ascribe this to:

> The desire on the part of institutions to save everything for the here and now, but to delete (almost) everything after a prescribed period of years (Baron and Attfield, 2013, p. 583).

Baron and Attfield’s explanation fits in with the hypothesis advanced in this paper that the bulk of an official’s correspondence is needed as a record of their work.

The coming of email, coupled with the trend of increasing access-to-information rights for citizens, has substantially increased the total cost, inconvenience and risk to government departments of keeping the business correspondence of an official, without increasing the total value of that correspondence.

The value of the correspondence of an official to their government department. Tends to degrade over time. It can be hypothesised that the point in time at which the cost and risk to a department of retaining business email correspondence outweighs the value to them of
keeping that correspondence arrives far quicker after the coming of email than it did before the coming of email.

If a government department was to succeed in moving business email correspondence into a corporate record system, then that correspondence would be governed by retention rules that are comparable to those set for pre-email correspondence. It can be hypothesised that this would result in the department having to retain correspondence long after its cost and risk exceeded its value to them.

The instruction to officials to move important emails into corporate record systems has survived in UK Government and elsewhere long after the records management beliefs that underpinned it have disappeared. This paper hypothesises that the instruction has survived because it imposes little or no burden on officials. They have no need to comply with the instruction because they have access to correspondence in their email accounts for as long as they are likely to need it. Their department is unlikely to try to enforce the instruction (e.g. by deleting emails from email accounts after a very short time period) as enforcing it would add to their cost and risk by capturing a higher volume of email into records systems.

Towards a realist explanation of The National Archives policy towards UK Government email

An initial explanation

The initial realist explanation advanced in this paper is that government departments will for the most part regard business email correspondence as a cost, a risk and a liability. They will therefore refrain from making serious efforts to move the bulk of business email correspondence from email accounts into record systems for fear of simply transferring the cost and risk from one system to another. They will instead allow officials to keep emails in their email account for as long as they need them for their individual operational needs.

The initial explanation hypothesises that the following:

- A majority of the email correspondence of key officials, and in particular a large majority of the sent items, are business emails.
- Injunctions to officials to move important records into a record system currently result in only a tiny minority of items of business correspondence being moved into a record system.
- Even when automated techniques become available, government departments are unlikely to apply them to the task of identifying business email and moving it into record systems as any such application of automated techniques would result in a very large and very unwelcome increase in the volume of email captured into corporate record systems.

Exposing the explanation to test

The paper concludes with what, from a realist evaluation point of view, is the most important part of the paper, the part that exposes the proposed explanation to test by making specific predictions about observable reality.

The initial explanation advanced in this paper may be tested by establishing:

- The proportion of sent emails captured into corporate record systems: The explanation predicts that a very small percentage of sent items are captured into government records systems.
• **The length of time government departments allow emails to remain in email accounts**: The explanation predicts that government departments rarely, if ever routinely, delete correspondence in a short enough time to incentivise officials to move emails to record systems.

• **Whether the routine deletion of email from email accounts is conditional on adequate capture of business email into record systems**: The explanation predicts that government departments will continue with routine deletion even when they know that they are not consistently capturing business email into corporate record systems.

• **The extent to which government departments use automated methods to identify important emails and move them to a record system**: The explanation predicts that government departments will rarely choose to apply automated technologies such as machine learning, auto-classification or analytics to the identification of important emails, even when the department is applying such technology to other types of records.

### References


ARMA International (2017), “Generally accepted recordkeeping principles”.


Cox, R.J. (2008), *Personal Archives and a New Archival Calling: Readings, Reflections and Ruminations*. Duluth, MN.


Corresponding author
James Lappin can be contacted at: j.lappin@lboro.ac.uk

For instructions on how to order reprints of this article, please visit our website: www.emeraldgrouppublishing.com/licensing/reprints.htm
Or contact us for further details: permissions@emeraldinsight.com
A must for agencies or a candidate for deletion

A grounded theory investigation of the relationships between records management and information security

Sherry Li Xie

School of Information Resource Management, Renmin University of China, Beijing, China and Center for Digital Records Management Research, Beijing, China and Key Laboratory of Knowledge and Data Engineering, Ministry of Education of China, China

Abstract

Purpose – This paper aims to report on a study that aimed at analyzing the relationships between information security and records management (RM), both as programs/functions established in organizations. Similar studies were not found in relevant literature.

Design/methodology/approach – The study used the classic grounded theory methodology. Pursuing the general curiosity about the information security-RM relationship in organizations, the study selected the United States (US) Federal Government as its field of entrance and followed the process of the classic grounded theory methodology that starts from the letting of the emergence of the research question to the formulation of a substantive theory that answered the question.

Findings – On the emergent question that why, despite the legislative establishment of agency RM programs and the use of the term records in their work, the US Federal Government information security community considered RM a candidate for deletion (CFD), the study coded the truncated application of the encompassing definition of records as the underlying reason. By this code, along with its three properties, i.e. limitations by the seemingly more encompassing coverage of information, insufficient legislative/regulatory support and the use of the terms of evidence and preservation in the records definition, the CFD consideration and the associated phenomena of unsound legislative/regulatory conceptualization, information shadow, information ignorance and archival shadow were explained.

Research limitations/implications – The study results suggested the data for subsequent theoretical sampling to be the operational situations of individual agency RM programs.

Practical implications – The rationale presented in the study regarding the encompassing nature of records and the comprehensive scope of RM program can be used for building strong RM business cases.

Originality/value – The study appears to be the first of its kind, which examined the RM–information security relationship in a very detailed setting.

Keywords Records management, Information security, Archival shadow, Information ignorance, Information shadow, Records definition

Paper type Research paper

Introduction

Information security and records management (RM) appear to be two different activities as indicated by their objects of concern (i.e. records and information) and the concerned aspects

This study is supported by the Fundamental Research Funds for Central Universities and the Research Funds of Renmin University of China (15XNL032).
While the relationships between the concerned aspects are highly contingent, depending on how the term management is specified, the objects of their concern can be viewed as related. A general view from the RM standpoint is that records constitute a portion of information, or records are a special type of information. As exemplified by the definition of records in the ISO standard on RM, records are “information created, received and maintained as evidence and as an asset by an organization or person, in pursuit of legal obligations or in the transaction of business” (ISO, 2016). Curiosity arises logically regarding the relationships between the two activities as to how they treat each other in the context of organization. This paper reports on a study that aimed at exploring such relationships, as no ready knowledge in literature was found. When searching peer-reviewed records journals, only one relevant article surfaced, which promoted the idea of integrating information security and RM in achieving information governance (Lomas, 2010). When searching the databases of Web of Science and Academic Search Premier, a few hits returned, but all of them are about security/protection of medical/health records in digital environment. The present study takes a general view toward the relationships between information security and RM in organizations and chooses the US Federal Government as its primary source of data. It used the classic grounded theory method (CGTM) as developed by Glaser and Strauss (1967) and Glaser (1978, 1992, 1998, 2001) and applied in the Record Nature project (Xie, 2013). The chosen methodology guided the organization of the paper, which follows the CGTM process. It starts with the emergence of the research question and ends with the substantive theories conceived as the answer to the question.

The classic grounded theory method process – letting the question emerge
As a basic tenet, CGTM disallows researchers from working with research questions that were conceived based on literature review. A general interest on any social phenomenon is enough for researchers to get into the field for inquiries regardless whether there is existing research. This is not to ignore existing research, thus risking the possibility of “reinventing the wheel”, but to treat it as one type of data, in accordance with the CGTM principle “all is data”, and compare it, at a later stage, with memos (i.e. ideas, thoughts and conceptual constructions) produced in the CGTM process. Comparison is the main analytical technique used by CGTM, which, at its core, does the same for data just as any other comparative analyses. What makes the CGTM comparison unique is the requirement that it needs to be in operation constantly and it should not be restrained by, for example, the types of data or the stages of the research process. The approach of getting into the field (physical and/or virtual) with a general interest serves the purpose of keeping as much as possible an open mind and letting the real, specific question emerge. Real, specific questions typically emerge when intimate knowledge of the field has been developed. For the present study, the status of information security in the US Federal Government is such intimate knowledge required for question(s) to emerge.

Information security in the US federal government
Information security in the US Federal Government is a subject regulated by law. According to the current FISMA (Federal Information Security Modernization Act of 2014, which amends the Federal Information Security Management Act of 2002), information security means “protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction to provide integrity, confidentiality and availability” (Office of the Law Revision Counsel of the USA House of Representatives, 2014). As one main mechanism to assist its implementation, FISMA requires NIST (National Institute of Standards and Technology) to develop pertinent standards and guidelines,
including minimum security requirements for federal information systems (NIST, 2018a). NIST has so far published three types of materials:

2. a series of Special Publications (i.e., SP 800 publications); and
3. an online Glossary.

The overarching approach for FISMA implementation is a “risk-based” one, conceived as a Risk Management Framework (RMF), which “brings together all of the FISMA-related security standards and guidance to promote the development of comprehensive and balanced information security programs by agencies” (NIST, 2018b). There are currently three SPs regarding the RMF approach: 800-39 Managing Information Security Risk: Organization, Mission and Information System View (2011), 800-30 Rev.1 Guide for Conducting Risk Assessments (2012) and 800-37 Rev.1 Guide for Applying the RMF to Federal Information Systems: a Security Life Cycle Approach (2010 with 2014 updates). A Risk Management Project for implementing FISMA is undergoing at NIST, including the revising of 800-37 Rev.1 (NIST, 2018b). Figure 1 depicts the six steps of the security life cycle in relation to the NIST standards and SP 800 publications, all under the guidance of RMF.

The 800 SPs in the Figure are:

1. 800-60 Vol.1 Rev.1. Guide for Mapping Types of Information and Information Systems to Security Categories (2008; 800-60 Vol.2 Appendix);

![Figure 1. RMF Security Life Cycle](image-url)

*Source: Adapted from (NIST, 2015)*
These two FIPSs and six SPs, along with the NIST Glossary and the NIST Computer Security Resource Center website, were used as the base for exploring the status of records and RM with respect to the community of information security (hereafter, the base publications). The NIST (2017) glossary contains terms extracted from FIPS, the SP 800 series, and the Committee for National Security Systems Instruction 4009 (CNSSI-4009). It is a necessary companion resource to these FIPSs and SPs because of its comprehensive inclusion of terms and the sources/contexts it provides for each term.

The emerging question
The exploration of records and RM in relation to the US Federal Government information security field was done by keyword searching the terms “record” and “records management” in the above base publications. The singular form of record ensured that the returned hits had included all words (n.) with a beginning of record, i.e. record, records, recording and recordkeeping. No alternative expressions for RM were attempted because of the consideration that RM in the US Federal Government is regulated by congressional laws; its expression as such should be rather standardized. The search results revealed that the term record appeared in all eight documents, yet the term “records management” did not appear once.

A search for “records management” in the NIST Glossary found out that it was listed as a term in the glossary, with a definition pointing to the US Federal Records Act and the National Archives and Records Administration (NARA), the agency designated as the administrator of the Acts, and, an acronym, candidate for deletion (CFD). Because the glossary did not provide any explanations for the acronym, the search continued on the source of the term, CNSSI 4009. CNSSI 4009 was developed by the Committee on National Security Systems (CNSS) Glossary Working Group, which released its most recent version in 2015. While it was developed by a group affiliated to a committee on national security systems, the CNSS Glossary was intended to be the mechanism that resolves “differences between the definitions of terms used by the Department of Defense (DoD), Intelligence Community (IC), and Civil Agencies (e.g. National Institute of Standards and Technology [NIST])”, thus “enabling all three to use the same glossary” (CNSS, 2015). The acronym CFD is spelled out in this Glossary as “candidate for deletion” and the candidacy is because of the “obsolete” status of the term. The reason that there is CFD, not actual deletion, is because a new term has not yet been proposed. As the Glossary explains it, “without the (CFD) term, rationale and possible linkage to a new term, users of the glossary would have no indication the term is outdated or has been replaced by a new term” (CNSS, 2015). Applying this to the term RM, it is clear that the Working Group, while uncertain about the replacement, it is certain about the deletion. The term “records” is also listed in the Glossary, yet without a
CFD next to it. Then, why is this? Why is RM a CFD in the view of the field of information security yet the term “records” is considered still necessary?

**The classic grounded theory method process – tracing and coding data**

To address the emerging question, data additional to the above identified ones were traced, following the CGTM technique theoretical sampling. Theoretical sampling is the technique of sampling that, broadly speaking, possesses two characteristics:

1. alignment to the guidance of the emerged question(s); and
2. following of the lead of observations, results of comparisons, hypotheses etc. generated in the process.

It can be repeatedly applied until the discovered codes, i.e. conceptual categories, are considered saturated. In the present study, the various leads that directed the theoretical sampling process include observations noted, along the line of parsing the usages of records and RM (if any), regarding the base publications (i.e. open coding and memoing), sources to the entry information security in the NIST Glossary, including those to the terms close to information security, i.e. IT (information technology) security, computer security, information systems security and cybersecurity, as well as the SPs in the NIST Publication Library that contain information security in their titles but are not referenced by any of the base publications. Data so traced include laws, regulations, (non-base publication) NIST SPs, NISTIRs (NIST Interagency Report) and NIST SP drafts. Drafts were not initially coded given the fact that the final versions may contain significant changes. They were eventually coded because of the observation that the current 800-16 Information Technology Security Training Requirements: a Role- and Performance-Based Model was published in 1998, and its new version was released as a draft in 2014, entitled 800-16 Rev.1 (DRAFT) A Role-Based Model for Federal Information Technology/Cybersecurity Training. By including drafts in the data corpus, insights regarding NIST’s attitude toward updating its publications were developed. For example, FIPS 199 and FIPS 200, while published in 2004 and 2006, respectively, are not being updated with urgency, which was given to publications concerning the RMF, i.e. 800-37, 800-53 and 800-160 (NIST, 2018c). In total, around 43 data sources were sampled and some of the illustrating examples are listed below:

1. **Laws**
   - 44 USC 21 National Archives and Records Administration;
   - 44 USC 29 Records Management by the Archivist of the United States and by the Administrator of General Services;
   - 44 USC 31 Records Management by Federal Agencies;
   - 44 USC 33 Disposal of Records; and
   - 44 USC 35 Coordination of Federal Information Policy.
     - Subchapter I – Federal Information Policy; and
     - Subchapter II – Information Security (FISMA).
2. **Regulations**
   - 36 CFR XII National Archives and Records Administration.
     - Subchapter B – Records Management
     - Part 2001 – Controlled Unclassified Information (CUI).
The classic grounded theory method process – conceiving substantive codes

All identified NIST publications, i.e. the base publication and the traced SPs and NISTIRs, in a total number of 28, were open coded to let the status of records and RM (if any) emerge. The coding focused on understanding the meanings of the terms records and RM in these
data and their usages in the given contexts. The occurring frequencies of the terms were also noted, which yielded the result as: 5 made no reference to either records or RM, 5 mentioned RM (including 1 that did not use records), and 22 used records. These numbers in general confirmed principally the initial observation that RM rarely occurred in the field of information security and the usage of records was much more common. The specific numbers, i.e. how many occurrences in one particular publication, and the information regarding where they occurred, were memoed together with the effort of understanding the usages of the two terms in texts. The understandings gained from individual data sources were then compared with each other and at the same time, pertinent laws and regulations. This process led to the emerging of the following substantive codes:

1. unsound legislative/regulatory conceptualization
2. shadows over agency RM program, which includes:
   - The information shadow.
   - The archival shadow.

\textbf{Unsound legislative/regulatory conceptualization}

As noted above, both information security and RM in the US Federal Government are regulated by congressional laws. The laws regarding information security and RM, like other enabling statutes in general, provide, usually as the first order in business, concepts and conceptual relationships as the necessary foundation on which other orders stand. Specifically, they are necessary for agencies to establish pertinent programs and execute them, and, more pertinent to the present study, to delimitate the boundaries between agency programs so that divisions of responsibilities are clear and collaborations for common goals are possible. The definition of information security and RM are seemingly clear when stating about the respective objectives, as one focusing on the protection of information and
information systems via the provision of integrity, confidentiality and availability (quoted above) and the other on “adequate and proper documentation of the policies and transactions of the Federal Government and effective and economical management of agency operations” (44 USC § 2901(2)). However, questions arise when it comes to the objects of the “protection” and “management”, i.e. information and information system, and records, which, worth being pointed out, are also the objects of the respective laws. The term records is legislatively defined as “all recorded information, regardless of form or characteristics, made or received by a Federal agency under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the USA Government or because of the informational value of data in them” (44 USC § 3301(1A)). FISMA, however, does not define information, and for information system, it applies the definition from the Federal Information Policy law, which defines information system as “a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information (44 USC § 3502(8)). While “information resources” is defined, which reads as “information and related resources, such as personnel, equipment, funds, and information technology” (44 USC § 3502(6)), information – despite of its usage in the definition of information resources – is not defined, and the lengthy definition of “information technology” provided by Title 40 USC §11101.(6) does not appear to help understand information. The definition of information, indeed, federal information in this context, was finally located in the regulation issued by the Office of Management and Budget (OMB), the administrator of the Federal Information Policy law. In OMB Circular A-130 (2016 revision), Managing Information as a Strategic Resource, federal information is defined as “information created, collected, processed, maintained, disseminated, disclosed, or disposed of by or for the Federal Government, in any medium or form” and information is defined as “any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, electronic, or audiovisual forms”. Similarities are not difficult to be spotted out when comparing the definitions of (federal) records and federal information; both rely on the term information, both include all media and form and both are in tight relationship with the operation/business of the Federal Government. There should not be strong objections to the assessment that the qualifier, “created, collected, processed, maintained, disseminated, disclosed, or disposed of by or for the Federal Government”, in the definition of federal information means fundamentally the same as the qualifier, “made or received by a Federal agency under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor”, in the definition of records. If there are any doubts about the terms “preserved” and “maintained” (assuming others are sufficiently self-explanatory), then the definition of “preserved” should be able to clear it. According to 36 CFR §1222.10 How should agencies apply the statutory definition of Federal records?, the term preserved means “the filing, storing, or any other method of systematically maintaining documentary materials in any medium by the agency” and it “covers materials not only actually filed or otherwise systematically maintained but also those temporarily removed from existing filing systems” (USA, 2018a, 2018b, 2018c). It is hard to dispute that the “any other method of systematically maintaining” covers the “maintained”. The only difference appears to be on the justifications for preservation in the definition of records, which offers two, and “maintained” in the definition of federal information, which offers none. The two reasons warranting the preservation/maintenance of records are one, “as evidence of the organization, functions,
policies, decisions, procedures, operations, or other activities of the USA Government” and two, “or because of the informational value of data in them”. It is not difficult to judge the second reason as entirely applicable to the maintenance of federal information; it is, however, not so obvious with the first one. 36 CFR §1222.10 defines quite a few key words used by the definition of records, it, however, does not define evidence. Nonetheless, because of the use of “or” in connecting the two reasons, the second reason alone should be able to permit the conclusion that federal information is not different from federal records in any fundamental ways. After all, if it is not for the “informational value of data” in information (i.e. “any communication or representation of knowledge”), why the Federal Government maintains it? This conclusion, along with the fact that the attempt to find explanations on the differences between federal information and federal records was in vain, raised questions about the soundness of the conceptual establishment regarding key – indeed, the most basic – concepts in these laws and regulations. What impact would this have on the implementation of programs?

Shadows over agency records management program
The US Federal agencies are mandated legislatively to “establish and maintain an active, continuing program” for the management of records (36 CFR §3102; hence “a must for agencies” in the title of this paper). Such established agency RM program can be described as possessing two major characteristics: encompassing in scope (in terms of covering the information types in agencies) and comprehensive in support (“agency business”, a term used by NARA RM regulations). Among the objectives set for such a program, “accurate and complete documentation of the policies and transactions of the Federal Government” is listed in the first place (§ 2902.). It appears that the expression “accurate and complete” is not identical to the one used in the definition of RM (36 CFR §2901.2) or the one in the section of General Responsibilities for RM (36 CFR §2904.), both of which utilize “adequate and proper” when referring to documentation. The two expressions, however, are in fact identical by virtue of the definition of “adequate and proper documentation”, which explains it as “a record of the conduct of Government business that is complete and accurate” (emphasize added). To meet this requirement, agencies are required to prescribe the creation and maintenance of records that:

- document the persons, places, things or matters dealt with by the agency;
- facilitate action by agency officials and their successors in office;
- make possible a proper scrutiny by the Congress or other duly authorized agencies of the Government;
- protect the financial, legal and other rights of the Government and of persons directly affected by the Government’s actions;
- document the formulation and execution of basic policies and decisions and the taking of necessary actions, including all substantive decisions and commitments reached orally (person-to-person, by telecommunications or in conference) or electronically; and
- document important board, committee or staff meetings (36 CFR §1222.22).

These documentation requirements, together with the stipulations on the record status of working files and copies of records (36 CFR §1222.12), and those on nonrecord materials, i.e. library and museum material, extra copies of documents and stocks of publications and of processed documents (36 CFR §1222.14), renders the encompassing nature of agency RM
program. Adding to it, there are requirements specifying conditions for nonrecord materials to turn to records and the inclusion of the management of nonrecord materials into RM program.

The comprehensive nature of agency RM programs in supporting agency business is first reflected in the RM responsibility structure. To support agency operation, the RM program is required to be formally structured, with the head of the agency assuming “general duties” (36 CFR §3101.), a Senior Agency Official for Records Management (SAORM) assuming agency-wide RM responsibilities (OMB and NARA, 2012) and Records Officer with appropriate authority to coordinate and oversee implementation of the agency comprehensive RM program principles (36 CFR §1220.34(a)). Similarly, in the RM regulations issued by GSA (General Services Administration) – which shares the RM overseeing responsibilities with NARA at the government-wide level – a RM office and a qualified records manager is required to be designated to “develop and implement agencywide RM programs” (41 CFR §102-193.20(a)) (USA, 2018a, 2018b, 2018c). Note that, the terms “agency-wide”, “agencywide” and “comprehensive” are used to describe the jurisdiction of the RM program, which is different from the requirement “assign records management responsibilities in each program (mission) and administrative area” (36 CFR §1220.34(d)). An agency-wide RM program aims at the RM aspect of the agency’s entire business, and “program (mission) and administrative area” RM programs are means to that end.

This comprehensive nature is also clear in the requirements on how these responsibilities should be discharged. For example:

- issue a directive(s) establishing program objectives, responsibilities, and authorities for the creation, maintenance and disposition of agency records (36 CFR § 1220.34 (c)); and
- ensure incorporation of recordkeeping requirements and records maintenance, storage, and disposition practices into agency programs, processes, systems, and procedures; (36 CFR §1220.34(d)).

However, this comprehensive nature of agency RM programs is shadowed by the focused attentions on information and archives.

The information shadow. Neither the characteristic of being encompassing or comprehensive was discernable in the coded information security data, which overwhelmingly used the term (federal) information and information system. Such usage may not be a problem as long as the understanding exists that an agency-wide RM has a vital role to play in information security. That is not the case. The RM program was greatly shadowed by information. Not only there are only five times of mentioning of RM but also the mentioning showed little understanding of the nature of an agency RM program. Agency RM programs were viewed as for “a particular business function” (NIST, 2008a) or for “certain controls” (NIST, 2018d) and their role in information security is to be consulted as one of the functional groups such as the Freedom of Information (FOI) unit and the human resources (HR) office at the “Security Planning” phase, because their insights “may be useful” (NIST, 2008b). Agency RM programs are fundamentally different from FOI units and HR offices because, for one, there are no statutory requirements for their controls to be incorporated into “agency programs, processes, systems, and procedures” (36 CFR §1220.34(d)). This information shadow is also illustrated by:

- Restricted ways of using the term records: with the overwhelming presence of information, the occurrence of records is generally rare. For the majority of the data,
records occurrences were with one- or two-digit numbers. Records occurred 1712 times in 800-53A Rev.4. Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans (NIST, 2014), simply because the document repeated the same usages over and over in specifying information for the said assessment. Overall, the predominant ways of using records were in the forms of “audit records”, “system of records” and “documents or records”. According to the NIST Glossary, audit record refers to an individual entry in an audit log related to an audited event, and an audit log is a chronological record of information system activities, including records of system accesses and operations performed in a given period. The term system of records, as defined by the US Privacy Act (5 USC §552a, 1974), can be understood as the equivalent of personal data in the EU GDPR, which is also the reason for expressions such as “records about individuals”. The use of “documents or records” was unable to be parsed because the term document is not defined by NIST or CNSS, and the definitions found in NARA-related statutes and regulations, i.e. Title 44 USC 15 and the Controlled Unclassified Information Regulation (32 CFR §2002), were not referenced. Sparsely, records also appeared in such forms as training records, access records, payroll records, criminal records, etc. indicating a strong sense of a particular type of information.

- Missing RM role in NARA’s CUI Regulation: CUI standards for Controlled Unclassified Information, the subject regulated by Executive Order 13556 – Controlled Unclassified Information. According this EO, CUI refers to “unclassified information throughout the executive branch that requires safeguarding or dissemination controls, pursuant to and consistent with applicable law, regulations, and Government-wide policies” (The White House, 2010). The term unclassified here is used to separate CUI from classified national security information, regulated by Executive Order 13526 Classified National Security Information and the Atomic Energy Act. The relationship between CUI and RM is that NARA is designated as the “Executive Agent to implement this order and oversee agency actions to ensure compliance with this order”. Through its Information Security Oversight Office, NARA issued its CUI Regulations, incorporating five NIST publications including FIPS 199, FIPS 200, SP 800-53 and SP 800-171. All these publications were data sources identified by the present study, with the only exception 800-88, Guidelines for Media Sanitization, which was not sampled as relevant. Being also the EA responsible for overseeing the Federal Government RM program, NARA exhibited, however, no intention to rely on existing agency RM programs to manage CUI. Instead, it requires agencies to establish a CUI program, to designate a CUI senior agency official and to implement, conceptually, the CUI Order and its CUI Regulation via the newly defined concept document. Starting with referring document as “any tangible thing which constitutes or contains information”, the definition continues to display a long list of specific types of document, so long that it makes the entire definition to need 252 words. All of these types, however, can be easily argued as qualifying the statutory definition of federal records, without even needing to invoke the sub-provision in the definition that gives the power to the US Archivist (i.e., the head of NARA) for determining records status. According to Title 44 USC §3301.(b), The Archivist’s determination whether “recorded information, regardless of whether it exists in physical, digital, or electronic form, is a record as defined in subsection (a) shall be binding on all Federal agencies”. The RM program
is not mentioned (at all) and records are subordinated to thing that “constitutes or contains information”. Once again, information takes over records.

In some occasions, the information shadow expanded to the degree that no agency RM program can even be spotted, thus the code information ignorance. The code information ignorance was used to capture the following properties:

- role of records officer/records manager not recognized;
- function of Records filing/classification not recognized;
- RM controls similar (if not identical) to Security Properties not recognized;
- RM-SDLC integration not recognized by information security-SDLC integration; and
- no impact of electronic records.

Role of records officer/records manager not recognized. Records officer was not mentioned in any of the documents’ groups of target audience, which typically list quite a few. Even in SP 800-160 Vol. 1, which used “Multidisciplinary Approach” in its title and listed eight groups of target audience, records officers were nowhere to be found. The multidisciplinary approach refers to the inclusion of – among others – information management and knowledge management, but not RM. The same goes with the overarching information security implementation approach, i.e. the RMF, which included information owner but not records officers. Defined as “an official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, classification, collection, processing, dissemination, and disposal” (NIST, 2011), information owner was identified as one of the key participants in the RMF process, assuming the primary responsibility of security categorization and play a supporting role in security control implementation, security control assessment, monitoring security control monitoring, etc. (NIST, 2010 with 2014 updates). Comparing this information owner with the RM regulations, it is rather clear that the duties assigned to information owner were completely covered by RM requirements (36 CFR §1220.34(c) and 36 CFR §1220.34(d, emphases added), and more:

1. a comprehensive RM program provides policies and procedures for ensuring that:
   - records documenting agency business are created or captured (36 CFR §1220.32(a));
     - Identify and prescribe specific categories of records to be systematically created or received and maintained by agency personnel in the course of their official duties (36 CFR §1222.24(a)(1)).
   - records are organized and maintained to facilitate their use and ensure integrity throughout their authorized retention periods (36 CFR §1220.32(b)); and
   - records are available when needed, where needed, and in a usable format to conduct agency business (36 CFR §1220.32(c)).
2. each program must develop recordkeeping requirements that identify: policies, procedures and strategies for ensuring that records are retained long enough to meet programmatic, administrative, fiscal, legal and historical needs as authorized in a NARA-approved disposition schedule (36 CFR §1222.26(e)); and
3. all Federal records, including those created or maintained for the Government by a contractor, must be covered by a NARA-approved agency disposition authority (36 CFR §1225.10).
Function of records filing/classification not recognized. FIPS 199, also the first step in the RMF, is about calculating security category (SC) for information and information system. As the calculation of SC for information system is based on the SCs of all information in the system, it is omitted here for further discussion. The calculation of SC for information is based on the concept of information type and the three security properties, i.e. confidentiality, integrity and availability, and can be illustrated as \( \text{SC}_{\text{information type}} = \{(\text{confidentiality, impact}), (\text{integrity, impact}), (\text{availability, impact})\} \), where the acceptable values for potential impact are low, moderate, high, or not applicable (NIST, 2004). The key in this process is information type as it is the interplay between it and the three security properties that determines the impact values. According to FIPS 199, an information type is “a specific category of information (e.g. privacy, medical, proprietary, financial, investigative, contractor sensitive, security management) defined by an organization or, in some instances, by a specific law, Executive Order, directive, policy, or regulation”. From a RM viewpoint, the file or classification system of records should be able to serve satisfactorily this purpose. Even if the identification of information type for security needs to be somewhat different, the records classification can at least serve as the foundation for the identification of information types.

RM Controls similar (if not identical) to Security Properties not recognized. FISMA’s definition of information security includes definitions for its three properties:

- **Integrity** means guarding against improper information modification or destruction and includes ensuring information nonrepudiation and authenticity.
- **Confidentiality** means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information.
- **Availability** means ensuring timely and reliable access to and use of information.

The requirements contained in these properties are sufficiently covered by RM requirements, in particular those imposed on electronic RM. In general, agencies are mandated “to create and maintain authentic, reliable, and usable records and ensure that they remain so for the length of their authorized retention period” (36 CFR §1220.32). For records in electronic information systems, authenticity, integrity, usability and reliability are required to be established as necessary RM controls. According to 36 CFR §1236.10:

1. Authenticity refers to controls to protect against unauthorized addition, deletion, alteration, use and concealment.
2. Integrity refers to controls, such as audit trails, to ensure records are complete and unaltered.
3. Usability refers to mechanisms to ensure records can be located, retrieved, presented, and interpreted.
4. Reliability refers to controls to ensure a full and accurate representation of the transactions, activities or facts to which they attest and can be depended upon in the course of subsequent transactions or activities.

In addition, 36 CFR §1236.20(b)(4) concerns the maintenance of “records security”, which requires the prevention of “unauthorized access, modification, or deletion of declared records” and the assurance “that appropriate audit trails are in place to track use of the records”.

None of the coded information security data made any references to these RM controls and requirements.
Records management–system development life cycle integration not recognized by information security-SDLC integration. SDLC stands for system development life cycle, an approach used for implementing information security controls. A security control is “a safeguard or countermeasure prescribed for an information system or an organization designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements” (NIST, 2013 with 2015 updates). Under the overarching guidance of the RMF, security controls are selected based on the security categories of information type (thus, information systems as well) and implemented via the integration of the controls into the five phases of SDLC, i.e. initiation, development/acquisition, implementation/assessment, operations/maintenance and disposal (NIST, 2008; 2010, 2014). RM requirements are also required to be integrated into the phases of SDLC. Title 36 CFR §1236.12 stipulates that, as part of the capital planning and systems development life cycle processes, agencies must ensure:

- That RM controls are planned and implemented in the system; and
- That all records in the system will be retrievable and usable for as long as needed to conduct agency business (i.e. for their NARA-approved retention period).

As stated above, RM controls are similar, if not identical, to information security requirements and both integrations for example, to be involved in the system development process as earlier as possible. The information security field, however, made no reference to the RM-SDLC integration, and the RM program or the records officer was not mentioned in its “key security roles and responsibilities in SDLC” (NIST, 2008c) or “key participants in the risk management process” (NIST, 2010 with 2014 updates).

No impact of electronic records. The US Federal Government was one of the pioneers recognizing electronic records, which has evolved, in the records definition, from hiding in the express of “regardless of form or characteristics” only to also in the explicit statement that records include “information created, manipulated, communicated, or stored in digital or electronic form” (44 USC §3301.(b)). The coding discovered that electronic records appeared only in laws, regulations and government-wide policies, e.g. the act Coordination of Federal Information Policy (44 USC 35), both the NARA and GSA RM regulations and the OMB Circular A-130, not, however, in any of the NIST data sources. Even with the most relevant area, i.e. information systems, no indications that there was any awareness of electronic records – which reside in information systems – were discoverable. For example, 36 CFR §1220.34(e) stipulates that, “Integrate records management into the design, development, and implementation of electronic information systems” and 36 CFR §1236.10 requires that “Agencies must incorporate controls into the electronic information system or integrate them into a recordkeeping system that is external to the information system itself”.

The archival shadow. The code archival shadow is used to capture the observation that between NARA’s authorities of agency RM supervision and archival responsibility, the latter appears to be much more regarded than the former. For illustrating purpose, the term archival responsibility here refers to NARA’s duties/concern of identifying permanent records and securing them as national archives, indicated by such words as “schedule”, “transfer” and “disposal/disposition”. Three specifications supported this code. First, legislative regard. In all four statutes concerning records, including the one entitled RM by Federal Agencies (44 USC 31), the archival concern is easily noticeable. Indeed, the term records is defined in the law entitled Disposal of Records ((44 USC 33), not in Chapter 31 or Chapter 29 RM by the Archivist of the USA. The same goes with the NARA RM regulations as evidenced by both the larger number of sessions regulating the archival concerns and the
archival intention in the sessions addressing indeed representative agency RM activities such as creation, maintenance and use.

Second, the agency regard. With the same information shadow, more than 20 per cent of the data sources showed the awareness of the archival responsibility than that of agency RM requirements, indicated by the usages of “record retention policy”, “historical records” and “archiving federal records”.

Third, the NARA regard. As presented above, agency RM was denied any part in NARA’s CUI Regulation. It, however, does not overlook the archival responsibility and regulates on “transferring records”. According to the requirements, authorized CUI holders may destroy CUI when “Records disposition schedules published or approved by NARA allow” (NARA, 2016). One example from NARA developed concepts can be used as an indication as well, i.e. temporary records. Temporary records was defined as those determined by the Archivist “to have insufficient value to warrant its preservation by the National Archives and Records Administration” (36 CFR §1220.18). The term and its definition served NARA’s purpose of standing out permanent records, the future national archives, but at the same time, created a sense of being temporary and unwanted for the absolute majority of the agencies’ records. Compare it with the often-seen statement about information: information is the lifeblood of [an organization, a country and society]. Cannot live without it.

The classic grounded theory method process – identifying core variable and formulating substantive theory
Emerging from the above coding is the idea that the application of the records definition was truncated. In other words, the encompassing nature of the definition did not find itself any manifestations in the information security world. This idea was determined to be the core variable to the present study because of its constant emergence in the process of opening coding. The selective coding surrounding it supported the determination, the *truncated application of records definition* was thus established, with the following properties:

- limitation by the seemingly more encompassing coverage of information;
- limitation by insufficient legislative/regulatory support; and
- limitation by the use of the terms evidence and preservation in the records definition.

*Limitation by the seemingly more encompassing coverage of information*
Whenever information appeared, records yielded, without their definitions being consulted and carefully compared. The much longer definition of records – which meant to signal rigor and to demonstrate significance – seemed to produce a counter-effective impression that records are just one type of information. Conversely, information was defined as vaguely as possible, covering all the territories in which there are human activities. As records are “recorded information” with long sentences of qualifiers, it is simply logically correct to use information in all occasions. To use records for situations where topics regarding NARA-approved retentions or transferring of records to NARA’s Electronic Records Archive were involved, was to mechanically respond to pressing regulatory requirements. As demonstrated by the following statements:

- Federal information is an asset of the Nation, not of a particular federal agency or its subordinate organizations. In that spirit, many federal agencies are developing
policies, procedures, processes and training needed to end the practice of
information ownership and implement the practice of information stewardship.

- Information stewardship is the careful and responsible management of federal
  information belonging to the Nation as a whole, regardless of the entity or source
  that may have originated, created or compiled the information. Information
  stewards provide maximum access to federal information to elements of the Federal
  Government and its customers, balanced by the obligation to protect the
  information in accordance with the provisions of FISMA and any associated
  security-related federal policies, directives, regulations, standards and guidance
  (NIST, 2010 with 2014 updates).

As such, information was set to take all, and the vagueness of it was called to help.
NARA seemed to be fine with this information predominating situation as no data on
any invoking of 44 USC 3301.(b) was located.

Limitation by insufficient legislative/regulatory support
Although the records laws are referenced in FISMA, and RM activities are included in 44
USC 35 Coordination of Federal Information Policy and OMB Circular A-130 Managing
Information as a Strategic Resource, the records definition was not sufficiently supported by
these records-relevant laws and regulations. If the encompassing nature of records was fully
acknowledged, then FISMA should have established the information security field as
subordinated to agency RM programs, and the coordination of federal information policy
should have been put under the umbrella name of RM, not that of information resources
management (44 USC §3501(3)). The concept of information resources management appears
to be incredibly cumbersome as information resources include “information and related
resources, such as personnel, equipment, funds, and information technology” (44 USC §3502
(6)) – basically everything needed for an agency’s operation. If the encompassing nature of
records was fully acknowledged, then OMB Circular A-130 should not have added to the
entangled information resources management the term information management, which,
contrary to an innocent speculation that the adding was meant to decompose the overly
crowded scope of information resources management, was defined as “encompass[ing] both
information itself and the related resources, such as personnel, equipment, funds, and
information technology”. Upon a closer look at how these information resources are
managed, both the specified functions of the OMB Director (44 USC §3504(a)(1)(B)) and the
specified responsibilities of federal agencies (44 USC §3506(b)(1)) were centered on
information, indeed federal information, thus the same as federal records. For example,
agencies are required to:

- reduce information collection burdens on the public;
- increase program efficiency and effectiveness; and
- the integrity, quality and utility of information to all users within and outside the
  agency, including capabilities for ensuring dissemination of public information,
  public access to government information, and protections for privacy and security
  ((§3506(b)(1)).

All of them are addressed by RM requirements, yet RM is treated as only a “component” of
information resources management (OMB, 2016).
Limitation by the use of the terms evidence and preservation in the records definition

Evidence is the term used in the records definition to display the significance of records (and by logic extension, of RM) and it is a common approach used by the records profession to draw attentions from RM stakeholders. The use of this term is considered one cause to the truncated application, because no definition was provided for it either in the records statutes, the RM regulations or the OMB Circular A-130. Without a definition, agencies are left to their own interpretations when applying the records definition. Highly unlikely, agencies would contact NARA or consult the ISO RM standard for understanding a word that, first, appears to be common, and second, is not explained in the definition session of the RM regulations (i.e. 36 CFR §1220.18) where all terms considered key to agency RM programs are explained. It is also highly unlikely that agencies would study the session on how to apply the definition, i.e. 36 CFR §1222.10, so hard that they could tease out, from the key words explained there, the meaning of, or the intention of using, the word evidence in the definition. In the case of the ISO RM standard, which the NARA RM regulations are “in conformance with” (36 CFR §1220.3), it is only in its 2016 edition that the term evidence is defined. The common understanding of evidence is to view it as possessing fact-proving ability legally or administratively, which was evident in the coding. In that information overwhelming world, evidence-certain type of records was visible still – with “audit records” being the most telling example. In fact, the term records in some of the data sources cannot be said as the application of the statutory records definition. Among the 29 data sources, 19 did not provide records definition, which were assumed as applying the statutory records definition except the 6 that did not use the term records in their texts. For the 10 that do provide records definitions in their glossaries, 1 cited the dated definition (i.e. FIPS 200, which is understandable given the fact that it is being updated), 2 – both are 2018 drafts – cited the current version of the definition and 7 employed the records definition invented by the information security field itself. Yes, it is 70 per cent. According to 800-53A Rev. 4 (NIST, 2014), records means “the recordings (automated and/or manual) of evidence of activities performed or results achieved (e.g. forms, reports, test results), which serve as a basis for verifying that the organization and the information system are performing as intended” (emphasize added). It is clear that records here are tied to the notions of, first, concerning “done deal”, thus excluding those produced in the process of getting things done and those always up and running such as the databases of information systems, and second, concerning formal inspection, which, however, constitutes only a small portion of the day-to-day operation. As a result, the information that qualifies the definition of records remained to be information, not records.

The term preservation in the records definition was defined (36 CFR §1222.10(5)) and its definition – which is rather general and encompassing – partially enabled the comparison between the definitions of records and federal information. However, this general and encompassing nature (i.e. by any meaningful ways of placing records somewhere by the reason of work) encountered a habitual understanding of preservation, which was interpreted narrowly as “long-term preservation”, something to be done at the end of a process. As evident in the following examples:

- […] Together with records preservation, [the attention to the management of Federal Government records] helps protect the Federal Government’s historical record (OMB, 2016).
- Agencies […] to encourage recipients of Federal funding […] to prepare data management plans that describe data to be created in funded programs and approaches for long-term preservation and access to created data (OMB, 2016).
• Disposal. Activities conducted during this phase ensure the orderly termination of the system, safeguarding vital system information, and migrating data processed by the system to a new system, or preserving it in accordance with applicable RM regulations and policies (NIST, 2008).

The explanations to the question, Why is RM a CFD in the view of the information security field yet the term "records" is considered still necessary? can thus be formulated as:

(1) Although the records definition was encompassing in scope, its application was significantly truncated because of:
   • first, the effort required to accurately interpret its meanings, compounded by the fact that records is also an everyday term; and
   • second, the no sign of strong will to push the definition through the Federal Government from the records side, or to push back the invasion of information, legislatively, by policy or by implementation;

(2) As a result, although the term records is still convenient to use, RM can be let go:
   • It is clear that the fate of RM hinges on records. Their volume, location and form of existence all play a role in determining the necessity and importance of their management. When records were reduced to a much smaller group, placed at the end of the performance and restrained from the diversity of digital forms, the necessity of RM faded.
   • A fading RM program witnessed the information security field ignoring its existence and starting their programs from scratch. They defined key concepts in FISMA that were already in records laws (with the same legislative intentions) and analyzed the relationships between information and agencies’ business, which the RM program should have done a long time ago. The point became, however, if they were able to do, and did, the job of RM, why would not they feel that RM was not in need, thus a CFD? Agency RM program may be a “must” in laws, but not to them.

Conclusions and suggestions
Guided by the framework of the classic grounded theory methodology, the present study endeavored to discover explanations/theories for the question emerged in the process of deepening a general curiosity, i.e. why did the information security program in the US Federal Government view the RM program a CFD, despite that, records, the object of the RM program, was not deemed as such? The discovery concluded on the idea that it was the truncated application of the records definition that had given rise to this phenomenon. Two factors were reasoned as predominately responsible: the significant effort required to accurately interpret the meaning of records and the lack of strong will to push the application of the definition. The truncated application of records definition caused the reduced comprehensiveness of agency RM programs, incurring in the establishment of the information security program without a sufficient appreciation of the RM program as a precondition. The running of the information security program as an entirely new undertaking, unaware of the assistance that could come from the agency RM program, suggested, eventually, the agency RM program’s CFD stance.

The invasion of information into the RM world is not a new phenomenon, and the status quo is typically “co-existence in peace”. The expression RIM, standing for records and information management, has been increasingly seen in the records field, yet it seems never
to appear in any information fields (including the field of information security), which makes one wonder the longevity of that peace. By the logic established in this study, the information security program should operate under the policy direction of the agency RM program, as the latter has a broader mandate for operation, covering both information and security. RM programs have also traditionally associated themselves with strategical thinking and analytical skills, which are readily applicable to the strategical planning and business analyses needed by the information security program. Thus, the information security program should only be specialized in evaluating the technique aspects of security controls and in inputting their evaluation to the overall decisions made by the RM program. Because such logic is not in plain sight, changes from the RM side should be considered. As the first change at the policy level, the present study proposes the modification of the records definition to be a more straightforward one such as any information that is any part of any operation of any entity. Such a definition encapsulates still the defining characteristics of records (with some being implicit due to the ubiquitous use of digital technologies) and at the same time, amplifies the encompassing intention nature of a records management programs. It thus offers improved utilities to organizational records management programs in terms of delineating their jurisdictions and in communicating with their non-records management colleagues. This is not to say that a change of the wording of the records definition will automatically make the job of records management easier. To do a good records management job in today’s organizational and societal environment, more will be needed for renewing records management theories and for advancing professionals’ technological preparations. It is the belief of this study, however, such an upfront and encompassing definition of records should be able to serve as the first aid to such end.

References


Further reading


Appendix 1. Wordlist (in alphabetic order for all parts)

Part I applied classic grounded theory method terms

CGTM refers to the research method originally developed by Glaser and Strauss in their book The Discovery of Grounded Theory: Strategies for Qualitative Research (1967) and subsequently elaborated by Glaser in his works such as Theoretical Sensitivity (1978), Emergence vs Forcing: Basics of Grounded Theory Analysis (1992), Doing Grounded Theories: Issues and Discussions (1998), The Grounded Theory Perspective: Conceptualization Contrasted with Description (2001), etc. According to Glaser and as showed in the titles of these works, there is only one grounded theory method. The adding of “classic” to it is the way of the general GTM community trying to distinguish it from other “versions” such as the one developed by Strauss with Corbin and the one by Charmaz. A strict application of CGTM in the RM field is The Record Nature project (Xie, 2013). The CGTM core principle and techniques are:

- **All is data**: meaning that the collection of data serves solely the need of theoretical sampling, thus irrespective of data types or collection boundaries.
- **Constant comparison**: meaning that comparative analysis is to be used whenever it is needed, irrespective of the types of data or the stages of research.
- **Core variable**: refers to the concept/category that signals to the researcher its potential of being able to logically link together all the substantial codes.
- **Emergence of research question**: meaning that research questions are not derived from reviewing existing literature on the matter that interests the researcher, but from exploring the field in which the matter presents itself.
- **Memoing**: refers to the analysis that focuses on relationship establishment between and among the CGTM generated codes.
- **Open coding**: meaning that the analysis of data is remotely guided by the researcher’s interpretation of the research question – not preconceived codes or categories of any type. The terms “remotely” and “interpretation” are used here to distinguish from the practices of creating preconceived codes through operationalizing research questions. This can cause confusions because both types of coding (open and restrained) are both indeed guided by the research question. The key difference here is that open coding permits a greater chance for researchers to be inspired by data and restrained coding typically let go the data that do not speak directly to the preconceived codes.
- **Selective coding**: refers to the analysis that focuses on data sampled surrounding the emerging core variable.
- **Specification or property**: refers to the sub-categories established for a concept, which assist the breaking-down of meanings of the concept and/or the justifying of the establishment of the concept.
- **Substantive theory**: refers to the explanations developed for answering a substantive question, i.e., one that emerged in a specific context/field. A substantive theory is always open to further CGTM analyses.
- **Theoretical coding**: refers to the analysis that focuses on identifying or establishing fundamental logic relations between the core variable and substantive codes. The outcome of theoretical coding is the substantive theory.
- **Theoretical sampling**: refers to the technique of sampling that broadly speaking, possesses two characteristics: 1) alignment to the guidance of the emerged question(s) and 2) following of the lead of observations, results of comparisons, hypotheses etc.
generated in the process. It can be repeatedly applied until the discovered codes, i.e. conceptual categories, are considered saturated.

**Part II acronyms**
- CFD: Candidate for Deletion
- CNSS: Committee on National Security Systems
- CNSSI: Committee for National Security Systems Instruction
- CUI: Controlled Unclassified Information
- FISMA: Federal Information Security Modernization Act of 2014,
- FIPS: Federal Information Processing Standards
- NARA: National Archives and Records Administration
- NIST: National Institute of Standards and Technology
- NISTIRs: NIST Interagency Report
- OMB: Office of Management and Budget
- RMF: Risk Management Framework
- SP: Special Publications authored by NIST
- SAORM: Senior Agency Official for RM
- SDLC: System Development Life Cycle

**PART III core concepts developed**
- *Unsound legislative/regulatory conceptualization:* refers to the ambiguities exhibited by the conceptual relationships between the concepts of (federal) records, (federal) information, information resources, RM, information management, information security etc., which are core to the relevant US Federal Government laws and regulations.
- *Information shadow:* refers to the tendency and practices of using the term information commonly and pervasively without consulting the definition of (federal) records, and discussing the operation of organizational functions, including information security, without considering the managerial affordance of agency RM program. The extreme representation of the information shadow is the information ignorance where no traces of records officer, RM functions and electronic records can be found despite of their legislative status.
- *Archival shadow:* refers to the observation that, between NARA’s authorities of agency RM supervision and archival responsibility, the latter appears to be much more regarded, and this includes both NARA and agencies.
- *Truncated application of records definition:* refers to the phenomenon that despite the existence of an encompassing definition of records, practical uses display much narrowed applications.
- *Records* (invented outside the records community): such as the one invented by the US Federal Government information security, which exhibited fundamental differences with the one by the US Federal Records Act.
- *Record(s)* (proposed): any information that is any part of any operation of any entity.
Appendix 2. Coding example: coding FIPS and their associated SPs

<table>
<thead>
<tr>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>This publication establishes security categories for both information and information systems.</td>
</tr>
<tr>
<td>No record or records management</td>
</tr>
<tr>
<td>Information is categorized according to its information type.</td>
</tr>
<tr>
<td>These can be viewed as regrouping activity/program records from records classification system, where records are classified individually with a mark for their sensitivity</td>
</tr>
<tr>
<td>An information type is a specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor sensitive, security management) defined by an organization or, in some instances, by a specific law, Executive Order, directive, policy, or regulation.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>RM relevance</th>
<th>Categorization of Federal Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>security objective</td>
<td>confidentiality, integrity, and availability</td>
</tr>
<tr>
<td>potential impact definitions for each security objective</td>
<td>Table 1 summarizes</td>
</tr>
<tr>
<td>Security Categorization</td>
<td>The security category of an information type can be associated with both user information and system information and can be applicable to information in either electronic or non-electronic form.</td>
</tr>
<tr>
<td>Applied to Information Types</td>
<td>System information (e.g., network routing tables, password files, and cryptographic key management information) must be protected at a level commensurate with the most critical or sensitive user information being processed, stored, or transmitted by the information system to ensure confidentiality, integrity, and availability.</td>
</tr>
<tr>
<td></td>
<td>What does user information mean?</td>
</tr>
</tbody>
</table>

The generalized format for expressing the security category, SC, of an information type is:

\[
SC_{\text{information type}} = \{(\text{confidentiality, impact}), (\text{integrity, impact}), (\text{availability, impact})\},
\]

where the acceptable values for potential impact are LOW, MODERATE, HIGH, or NOT APPLICABLE
- \{(\text{confidentiality, impact})\}: the potential impact value of not applicable only applies to the security objective of confidentiality.

Security Categorization

Applied to Information Systems

Determining the security category of an information system requires slightly more analysis and must consider the security categories of all information types resident on the information system – this means:
- Not all information is categorized when it is not in an information system; then, this makes the definition of information system critically important, because we need to know where the information NOT in an information system is
- [Need to find out] What happens to categorized information type and information systems in terms of their subsequent management (e.g., maintenance, disposition)?

The generalized format for expressing the security category, SC, of an information system is:

\[
SC_{\text{information system}} = \{(\text{confidentiality, impact}), (\text{integrity, impact}), (\text{availability, impact})\},
\]

where the acceptable values for potential impact are LOW, MODERATE, or HIGH
- \{(\text{confidentiality, impact})\}: Note that the value of not applicable cannot be assigned to any security objective in the context of establishing a security category for an information system. This is in recognition that there is a low minimum potential impact (i.e., low water mark) on the loss of confidentiality, integrity, and availability for an information system due to the fundamental requirement to protect the system-level processing functions and information critical to the operation of the information system – again, the utmost importance of the definition of information system,

(continued)
... guidelines recommending the types of information and information systems to be included in each such category. The revision to Volume I contains the basic guidelines for mapping types of information and information systems to security categories. The appendices contained in Volume I include security categorization recommendations and rationale for mission-based and management and support information types.

- No author for either comes from NARA
- 3 Record (it won’t be convincing to count the numbers of information in the docs because the subject matter is about “information”. But how about information management and information resources management?)
- Central Records & Statistics Management
- Government Resource Management Functions and Information Types
- Information & Technology Management
- record retention
- The recommended information types provided in NIST SP 800-60 are established from the “business areas” and “lines of business” from OMB’s Business Reference Model (BRM) section of Federal Enterprise Architecture (FEA) Consolidated Reference Model Document Version 2.3, October 2007.
- Provisional security impact levels are the initial or conditional impact determinations made until all considerations are fully reviewed, analyzed, and accepted in the subsequent categorization steps by appropriate officials.
- Discuss information attributes that may result in variances from the provisional impact level assignment; and
- Describe how to establish a system security categorization based on the system’s use, connectivity, and aggregate information content.

The guideline and its appendices recommend a security categorization process; describe a methodology for identifying types of Federal information and information systems; suggest provisional security impact levels for common information types; establish the security categorization process; describe a methodology for identifying types of Federal information and information systems; and discuss information attributes that may result in variances from the provisional impact level assignment; and describe how to establish a system security categorization based on the system’s use, connectivity, and aggregate information content.

The SP 800-60 information types and associated security impact levels are based on the Office of Management and Budget (OMB) Federal Enterprise Architecture Program Management Office’s October 2007 FEA Consolidated Reference Model Document, Version 2.3

Security categorization starts with the identification of what information supports which government lines of business, as defined by the Federal Enterprise Architecture (FEA), and the result is strong linkage between missions, information, and information systems with cost-effective information security.

NIST Risk Management Framework also here, p. 7, and the process

The identification of information processed on an information system is essential to the proper selection of security controls and ensuring the confidentiality, integrity, and availability of the system and its information.

SP 800-60 V.2, Appendixes

Record and records management:

Central Records and Statistics Management involves the operations surrounding the management of official documents, statistics, and records for the entire Federal Government. This information type is intended to include information and information systems associated with the management of records and statistics for the Federal government as a whole, such as the records management performed by NARA or the statistics and data collection performed by the Bureau of the Census.

Note: Many agencies perform records and statistics management for a particular business function and as such should be mapped to the service support, management, or mission area associated with that business function. The central records and statistics management information type is intended for functions performed on behalf of the entire Federal government. The recommended security categorization for the central records and statistics management information type is as follows:

\[
\text{Security Category} = (\text{confidentiality}, \text{Moderate}), (\text{integrity}, \text{Low}), (\text{availability}, \text{Low})
\]

Special Factors Affecting Confidentiality Impact Determination: Unauthorized disclosure of some centrally managed records can pose a threat to human life or a loss of major assets.

(continued)
In such cases, the confidentiality impact is high.

Sensitive information includes information whose improper use could adversely affect the ability of the agency to accomplish its mission (i.e., not considered as records—information shadow), proprietary information, records about individuals that require protection under the Privacy Act, and information not releasable under the Freedom of Information Act for agencies that manage large income information involving records of the general public, the provisional confidentiality impact level can be expected to be at least moderate.

C.3.5.6 Record Retention Information Type

Records Retention involves the operations surrounding the management of the official documents and records for an agency. Subject to exception conditions described below, the recommended security categorization for the record retention information type is as follows:

Security Category = ((confidentiality, Low), (integrity, Low), (availability, Low))

C.3.5.7 Information Management Information Type

Information Management involves the coordination of information collection, storage, and dissemination, and destruction as well as managing the policies, guidelines, and standards regarding information management. This is logic (identified information type).

C.3.5 Information and Technology Management

C.3.5.1 System Development Information Type

C.3.5.2 Lifecycle/Change Management Information Type

C.3.5.3 System Maintenance Information Type

C.3.5.4 IT Infrastructure Maintenance Information Type

C.3.5.5 Information Security Information Type

C.3.5.6 Record Retention Information Type

C.3.5.7 Information Management Information Type

C.3.5.8 System and Network Monitoring Information Type

C.3.5.9 Information Sharing Information Type

2006 Minimum Security Controls for Federal Information Systems

FIPS Publication 199, Standards for Security Categorization of Federal Information and Information Systems, is the first of two mandatory security standards required by the FISMA legislation. FIPS Publication 200, the second of the mandatory security standards...

No RM

2 record:

- Audit and Accountability (AU): Organizations must: (i) create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and (ii) ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.

- The old legislative records definition

The focus here is... Information systems?

Yes, government by establishing minimum levels of due diligence for information security and facilitating a more consistent, comparable, and repeatable approach for selecting and specifying security controls for information systems that meet minimum security requirements.

The minimum security requirements cover seventeen security-related areas with regard to protecting the confidentiality, integrity, and availability of federal information systems and the information processed, stored, and transmitted by these systems.

Seventeen security-related areas:

(i) access control; (ii) awareness and training; (iii) audit and accountability; (iv) certification, accreditation, and security assessments; (v) configuration management; (vi) contingency planning; (vii) identification and authentication; (viii) incident response; (ix) maintenance; (x) media protection; (xi) physical and environmental protection; (xii) planning; (xiii) personnel security; (xiv) risk assessment; (xv) systems and services acquisition; (xvi) system and communications protection; and (xvii) system and information integrity

(continued)
Organizations must meet the minimum security requirements in this standard by selecting the appropriate security controls and assurance requirements as described in NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems. The process of selecting the appropriate security controls and assurance requirements ... is a multifaceted, risk-based activity ... Security categorization of federal information and information systems, as required by FIPS Publication 199, is the first step in the risk management process.

Security categorization must be accomplished as an enterprise-wide activity with the involvement of senior-level organizational officials including, but not limited to, chief information officers, senior agency information security officers, authorizing officials (a.k.a. accreditation authorities), information system owners, and information owners.

These definitions need to be double-checked:

**CHIEF INFORMATION OFFICER**
Agency official responsible for: (i) providing advice and other assistance to the head of the executive agency and other senior management personnel of the agency to ensure that information technology is acquired and information resources are managed in a manner that is consistent with laws, Executive Orders, directives, policies, regulations, and priorities established by the head of the agency; (ii) developing, maintaining, and facilitating the implementation of a sound and integrated information technology architecture for the agency; and (iii) promoting the effective and efficient design and operation of all major information resources management processes for the agency, including improvements to work processes of the agency. [44 U.S.C., Sec. 5125(b) – cannot find it]

**SENIOR AGENCY INFORMATION SECURITY OFFICER**
Official responsible for carrying out the Chief Information Officer responsibilities under FISMA and serving as the Chief Information Officer’s primary liaison to the agency’s authorizing officials, information system owners, and information system security officers. [44 U.S.C., Sec. 3544 - repealed]

**AUTHORIZED OFFICIAL**
Official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals. Synonymous with Accreditation Authority.

**INFORMATION SYSTEM OWNER**
Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system. [CNSS Instruction 4009 Adapted]

**INFORMATION OWNER**
Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal. [CNSS Instruction 4009]

Even if there was no Senior Records Officer at the time of drafting this standard, records manager should be mentioned here, i.e., even if not at the "senior-level" but at least “appropriate”.

To ensure a cost-effective, risk-based approach to achieving adequate security across the organization, security control baseline tailoring activities must be coordinated with and approved by appropriate organizational officials (e.g., chief information officers, senior agency information security officers, authorizing officials, or authorizing officials designated representatives).
<table>
<thead>
<tr>
<th>Glossary</th>
<th>No records management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit Record</td>
<td>212 records</td>
</tr>
<tr>
<td>An individual entry in an audit log related to an audited event.</td>
<td>o Audit records = 78</td>
</tr>
<tr>
<td>A chronological record of information system activities, including records of system accesses and operations performed in a given period.</td>
<td>o System of records = 23</td>
</tr>
<tr>
<td></td>
<td>o Access records = 15</td>
</tr>
<tr>
<td></td>
<td>o Training records = 5</td>
</tr>
<tr>
<td></td>
<td>o Records retention = 3</td>
</tr>
<tr>
<td></td>
<td>o Maintenance records = 3</td>
</tr>
<tr>
<td></td>
<td>o Payroll records = 3</td>
</tr>
<tr>
<td>51 record</td>
<td>o Audit record = 26</td>
</tr>
<tr>
<td></td>
<td>o Record retention = 10</td>
</tr>
<tr>
<td></td>
<td>▪ NARA = 8 all about record retention</td>
</tr>
<tr>
<td>8 recording; 5 recorded</td>
<td>A Definition for records, not citing the legal one, but as</td>
</tr>
<tr>
<td>agency, including improvements to work processes of the agency. [44 U.S.C., Sec. 5125(b) – cannot find it]</td>
<td></td>
</tr>
</tbody>
</table>

**SENIOR AGENCY INFORMATION SECURITY OFFICER**
- Official responsible for carrying out the Chief Information Officer responsibilities under FISMA and serving as the Chief Information Officer’s primary liaison to the agency’s authorizing officials, information system owners, and information system security officers. [44 U.S.C., Sec. 3544 - repealed]

**AUTHORIZING OFFICIAL**
- Official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals. Synonymous with Accreditation Authority.

**INFORMATION SYSTEM OWNER**
- Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system. [CNSS Instruction 4009 Adapted]

**INFORMATION OWNER**
- Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal. [CNSS Instruction 4009]

Even if there was no Senior Records Officer at the time of drafting this standard, records manager should be mentioned here, i.e., even if not at the “senior-level” but at least “appropriate”.

To ensure a cost-effective, risk-based approach to achieving adequate security across the organization, security control baseline tailoring activities must be coordinated with and approved by appropriate organizational officials (e.g., chief information officers, senior agency information security officers, authorizing officials, or authorizing officials designated representatives).
Records connotation of completed:

- "The recordings (automated and/or manual) of evidence of activities performed or results achieved (e.g., forms, reports, test results), which serve as a basis for verifying that the organization and the information system are performing as intended.
- "results achieved" implies the completion of the activity, yet "evidence of activities performed" does not necessarily so. Records generated IN the process of performing an activity is also evidence.

RM relevance:

- Organizations are required to adequately mitigate the risk arising from use of information and information systems in the execution of missions and business functions. A significant challenge for organizations is to determine the most cost-effective, appropriate set of security controls.
- There is no one correct set of security controls that addresses all organizational security concerns in all situations. Selecting the most appropriate set of security controls for a specific situation or information system to adequately mitigate risk is an important task.
- Organizations can demonstrate how to most effectively assure the confidentiality, integrity, and availability of organizational information and information systems in a manner that supports mission/business needs while demonstrating due diligence. Selecting, implementing, and maintaining an appropriate set of security controls to adequately protect the information systems employed by organizations.
- Requires strong collaboration with system owners to understand ongoing changes to missions/business functions, environments of operation, and how the systems are used.

Glossary:

1. Security Control [FIPS 199, Adapted]: A condition that results from the establishment and maintenance of protective measures that enable an enterprise to perform its mission or critical functions despite risks posed by threats to its use of information systems. Protective measures may involve a combination of deterrence, avoidance, prevention, detection, recovery, and correction that should form part of the enterprise’s risk management approach.
2. Security Capability: A combination of mutually-reinforcing security controls (i.e., safeguards and countermeasures) implemented by technical means (i.e., functionality in hardware, software, and firmware), physical means (i.e., physical devices and protective measures), and procedural means (i.e., procedures performed by individuals).

SECURITY CONTROLS: The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information. [FIPS 199]
• no records management
• records here is used in a more general sense, i.e., not limited to a specific type of records as in other documents, but the context is assessment (as evidence for assessment, this prohibits its moving to the front line of organization’s operation, where businesses/programs and information are highly regarded)
• Records = 1712
  o Audit records = 491
  o "or records" = 864 (documents or records)
  o Monitoring records = 18
  o access authorization records = 8
• but records are defined as “The recordings (automated and/or manual) of evidence of activities performed or results achieved (e.g., forms, reports, test results), which serve as a basis for verifying that the organization and the information system are performing as intended. Also used to refer to units of related data fields (i.e., groups of data fields that can be accessed by a program and that contain the complete set of information on particular items).”

### POTENTIAL ASSESSMENT METHODS AND OBJECTS:
Examine: [SELECT FROM: Access control policy and procedures; other relevant documents or records – this usage is constant in this doc].

### POTENTIAL ASSESSMENT METHODS AND OBJECTS:
Examine: [SELECT FROM: Access control policy; procedures addressing account management; information system design documentation; information system configuration settings and associated documentation; system-generated list of dynamic privilege management capabilities; information system audit records; other relevant documents or records].

### POTENTIAL ASSESSMENT METHODS AND OBJECTS:
Examine: [SELECT FROM: Access control policy; procedures addressing account management; information system design documentation; information system configuration settings and associated documentation; information system-generated list of privileged user accounts and associated role; records of actions taken when privileged role assignments are no longer appropriate; information system audit records; audit tracking and monitoring reports; information system monitoring records; other relevant documents or records].

• it also appears as the name of one type of documents, similar to procedures, policies, meeting minutes, plans, reports, etc.

---

**About the author**

Sherry Li Xie, MLIS (McGill University, Canada), MAS and PhD (University of British Columbia, Canada). Worked as librarian, archivist and records manager in universities and governments in Canada and is currently working as a Professor in School of Information Resource Management, Renmin University of China; Associate Director, Center for Electronic Records Management Research; Research Fellow, Key Laboratory of Data Engineering and Knowledge Engineering, Ministry of Education of China; and Adjunct Professor at the School of Library, Archival and Information Studies, University of British Columbia, Canada. Sherry Li Xie can be contacted at: sherrylx@outlook.com

---

For instructions on how to order reprints of this article, please visit our website: [www.emeraldgrouppublishing.com/licensing/reprints.htm](http://www.emeraldgrouppublishing.com/licensing/reprints.htm)

Or contact us for further details: [permissions@emeraldinsight.com](mailto:permissions@emeraldinsight.com)
Theory, regulation and practice in Swedish digital records appraisal

Elisabeth Klett

Mid Sweden University, Sundsvall, Sweden

Abstract

Purpose – Digital records appraisal and aspects of archival values in theory, regularization and practice are explored. This paper aims to reflect upon the appraisal process, responsibility and norms for value creation in a digitalized environment. The research question was how do appraisal theory, normative rules and appraisal practice meet the aims of values in digital archives?

Design/methodology/approach – The study triangulated appraisal theory, normative values and participants’ views about archival values in appraisal practice in a Swedish setting. Content analysis were used to explore normative documents and interviews. Appraisal theories of the Swedish Nils Nilsson and the Canadian Terry Cook were interpreted. The result was related to theories on public values, the nature of responsibility and relations between the state and citizens.

Findings – The results show influences between theory, norms and practice. Changes in norms and practice do not follow the development of digitalization. Responsibility is focused on tasks, which exposes risks of accountability control and knowledge of appraisal grounds. The paper concludes that access requirements and user needs may prompt change in appraisal processes. In the light of digitalization, “primary and secondary value” are merely a matter of use and usability in a time and space (continuum) perspective.

Research limitations/implications – This study is based in Sweden where extensive right of access to public records and default preservation are norm.

Originality/value – The result shows how allocated responsibilities impinge on a re-active digital appraisal process.

Keywords Digital archives, Archival norms, Archival responsibility, Records appraisal

Paper type Research paper

Introduction

The core of archival theory is about the creation, recreation and remediation of records and archives and about records being used in the course of these processes. For archival theory, the connection to practice is important through its roots in principles and its history of development, since the Manual of Muller, Feith and Fruin in 1898 (Muller et al., 1940; Ridener, 2009). Appraisal aims to create enduring value in archives. Archival appraisal embraces “theory, rationales, policies and procedures” for the selection of records of enduring value from records captured in organizations (Craig, 2015). The formation of archives is based on the principle of provenance (Nilsson, 1983), which means the creation and capture of records within the scope of organizational business interests. In a digitally transformed environment provenance becomes a conceptual context when organizations share information systems which affects internal and original order and the scope of an archive (Douglas, 2017; Hurley, 2005a).

How to scope, what to include in archives and how to appraise records is a recurring discussion connected to increased masses of records resulting from changes in technology (Ridener, 2009). During the past 20 years of the twentieth century until the present, the
development of information and communication technology (ICT) has raised a renewed discussion on the role of archives and methods for records appraisal (Eastwood, 2017; Foscarini, 2017; Kallberg, 2012; Klareld, 2015; Klareld and Gidlund, 2017). One problem identified is residual paper thinking among archivists in the digitally transformed environment, as if the prerequisites for control and authenticity, and for manifold access and usability were still more or less the same (Cook, 1994; Klareld and Gidlund, 2017; Runardotter et al., 2011, p. 74).

The public sector as a whole is struggling with digital transformation and e-government policies of efficiency, transparency, productivity, availability and high quality service (Persson and Goldkuhl, 2010). This challenges traditional conceptions of archives formation based on paper thinking with its tangible and stable format and appearance (Kallberg, 2013; Klareld and Gidlund, 2017; Runardotter et al., 2011). A change in responsibility for archives formation from archivists to IT professionals has followed digital transformation (Kallberg, 2013). Communication problems between the two professions are noted as a consequence (Klett, 2017; Runardotter, 2009). Digital transformation and changed responsibilities bring the matter of archival values and the creation of value in archives to the fore.

Traditionally the aims of records appraisal are to protect values and to define and delimit the archive (Nilsson, 1983); thus, the concept of value is central. In theory the value of records and archives is the fulfillment of needs substantiated through access (Klett, 2017; Menne-Haritz, 2001). The task is to develop conscious and logical grounds for digital records appraisal based on archival theory (Fredriksson, 2003, p. 23).

Records and archival appraisal are based on theory, rationales, policies and procedures (Craig, 2015). In this paper, these bases are interpreted as follows: theory identifies archival value, rationales are based on societal norms, regulations formalize norms, policies interpret and explain the regulations and guides to procedures. Finally, appraisal parameters support practice in effectuation of creating value in archives. Value in digital archives is the result of digital records appraisal which is comprised of assessment of both access and need, and across a spectrum of perspectives, such as time, business and society (McKemmish, 2005; International Organization for Standardization (ISO), 2016, 15489). The appraisal process results in an archive that contains records of both primary and secondary value (Schellenberg, 2003/1956). Primary value refers to business needs. Secondary value refers to any other use of records, by any user in the present or future time. In a digitally transformed environment requirements of access and needs may call for change in appraisal processes, of parameters for assessment and of structure in archives (Cook, 2011; Fredriksson, 2003). In practice, divided responsibilities for appraisal of primary and secondary values causes a black box of lost and unknown records, where scoping appraisal for primary value is decided by the creator and appraisal for secondary value and retention plans is decided by the archival authority. It also causes inconsistency in implementing rules of law, as various public agencies can decide differently when scoping the archive, despite similar types of records.

From this reasoning, three working agents can be identified as involved in records and archives appraisal: theory, regulation and practice. Knowledge about how aims of archival value are formulated and understood by the three working agents is a starting point for a process of change and adaption of records appraisal processes and value parameters in e-governance of the public sector.

This paper combines archival theory and empiricism (Fredriksson, 2003) and uses the Swedish example to empirically explore how the fulfillment of needs is interpreted by appraisal theorists, expressed in normative statements concerning appraisal that govern the public sector and again interpreted by professionals involved in records appraisal.
The research question is:

RQ1. How do appraisal theory, normative regulations and appraisal practice meet the aims of value in digital archives?

Background

In Sweden, preservation of official records is the default, connected to an extensive right to access official records (Sveriges Riksdag, 1949), which is unique for Sweden and Finland. Two main laws, the Freedom of Press Act and the Archives Act govern archives formation and management and records appraisal of the three autonomous public sectors in Sweden; the state, the municipalities and the county councils. There is no distinction in Sweden between archivists and records managers, although tasks may differ between an archival authority and a public agency (Kallberg, 2013, pp. 11-15). The view of appraisal is legalistic (Fredriksson, 2003) and any disposition has to be granted by an archival authority. The scope of the archive is set by identification of public records among all records created and captured or archived by a state, municipal and county council agency (Sveriges Riksdag, 1949). The Archival Act (Sveriges Riksdag, 1990) and the Freedom of the Press Act (Sveriges Riksdag, 1949) divide responsibilities for public sector archives formation and keeping between two parties – an archival authority and an archive holder, which is a public administration agency. The public agency, whether state or municipal, is responsible for delimiting the archive and thus scoping records appraisal. The archival authority has a prescriptive role in regulating archives formation, care and keeping and is also the keeper of records appraised for long-term preservation. Consequently records and archives appraisal is performed in a process of two main steps:

1. The public agency initiates and performs the appraisal inquiry.
2. The archival authority takes the final decision on retention periods and destruction of archival records.

The purpose of appraisal and retention decisions is to avoid burdening the public archive with records that are not relevant to understanding the character of the business of a public authority (Geijer et al., 2013). An archive, with a minor exception, is defined as the sum of public records. Archival values according to the Swedish Archives Act 3§ (Sveriges Riksdag, 1990) are:

- the right to access official records;
- information needs for the administration of justice and the administration; and
- research needs.

This paper takes the state and a municipality as examples of the public sector, both following the same main process and division of responsibilities given by rules of law. The first part of the two-step appraisal process lies in the agency’s procedures. Initiated by an emergent need to dispose of records, the scope of appraisal is decided upon, an inquiry into organizational business needs is performed, culminating in a proposal for the referral of a retention request. The resulting request for a retention and disposal decision is sent to the archival authority. The second part of the two-step appraisal process lies in the procedures
of the archival authority, investigating secondary values and taking into account societal needs. It concludes in a retention decision. The agency is obliged to act accordingly.

The Swedish National Archive’s policy “Preservation of the present” (authors translation) gives guidance on appraisal parameters to support appraisal inquiries and decision makers (Riksarkivet, 1995). Target groups of the policy are, besides the Swedish National Archives, primarily the local archival authorities of Swedish municipalities and county councils. In a pre-study report for a revised appraisal policy (Riksarkivet, 2012) the National Archives suggests that appraisal should be based on epistemological grounds. The report explains this as “empirics, rationality and context”, meaning records, core business and system, the last understood as contextual links and patterns.

Method
The method triangulated three working agents of archival value – theory, regularization and practice – to explore relations and influences of grounds for records appraisal. The result was related to theories of public values, the nature of responsibility and aspects of relations between the state and the citizens. The research techniques used were qualitative content analysis of a document survey and interviews. The data consisted of:

- **Agents of Theory**: the appraisal theories of Nilsson (1976, 1983) and Cook (2004).
- **Agents of Regulation**: the Swedish Archives Act (Sveriges Riksdag, 1990) and normative documents from the Swedish National Archives and Stockholm City Archives (Table 1).
- **Agents of Practice**: notes from 11 semi-structured interviews made with professionals from state and municipal sectors.

The two theorists are interesting and comparable because they both developed their theoretical approaches while working at their respective national archives and both have had impact in their respective country. The normative documents used, besides the Archives Act, were governing documents currently in force and digitally available from two Swedish archival institutions (Table I). The Swedish National Archives regulates the state administration that involves around 250,000 employees, while Stockholm City Archives regulates agencies within the municipal administration that involves around 40,000 employees.

<table>
<thead>
<tr>
<th>The Swedish National Archives</th>
<th>Stockholm City Archives</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Swedish Archives Act (Sveriges Riksdag, 1949)</td>
<td>The Swedish Archives Act (Sveriges Riksdag, 1949)</td>
</tr>
<tr>
<td>Guidance on Proposals for agency specific regulation (RA-MS) (Riksarkivet, 2014)</td>
<td>Guidelines to Archival ordinances (Stockholms Stadsarkiv, 2015b)</td>
</tr>
<tr>
<td>Policy 1995: Preservation of the present. (Riksarkivet, 1995)</td>
<td>To appraise and destroy (Stockholms Stadsarkiv, 2009)</td>
</tr>
<tr>
<td>Guidance on records appraisal (Riksarkivet, n.d.)</td>
<td>Handling digital information (Stockholms Stadsarkiv, 2016)</td>
</tr>
<tr>
<td></td>
<td>Archival requirements for IT-systems (Stockholms Stadsarkiv, 2011)</td>
</tr>
</tbody>
</table>

Table I. Normative documents analyzed
The interviews were undertaken in Summer-Autumn 2017. Questions were sent in advance to give time for preparation. The respondents, in positions with responsibility for regulation, appraisal decisions and supervision and involved in the effectuation of appraisal performance, were selected using snowball sampling (Williamson and Johanson, 2013, p. 344). In total, 9 archivists, one IT-officer and one administrative officer with appraisal tasks accepted the invitation which covered the desired range of responsibilities, with emphasis on archivists. The number of archivists with responsibility for appraisal policy and implementation in both organizations is relatively small and it was difficult to find stakeholders among IT professionals and administrators who were willing to participate.

Qualitative content analysis was used on the regulating and practice level data (Graneheim et al., 2017), using a deductive approach. Analysis strove to interpret meanings as they were expressed in text documents or in the notes taken during interviews (Graneheim et al., 2017; Hellspong, 2001). The choice of the triangulation method aimed to indicate how theory interacts with normative rules and regulations in the implementation of archival values by the people effectuating appraisal inquiries. This transfer of ideas includes the way in which the appraisal process is determined.

Ideas of archival value were explored by seeking answers to the following questions put to respondents. The same questions were used to guide textual content analysis of the documents (Hellspong, 2001):

- What is the purpose of appraisal?
- What are the grounds for retention and preservation decisions?
- What informational or archival values should be promoted in the steering documents?
- What are the main reasons for destroying or preserving records?
- What is the/your view on aspects like accessibility to and re-use of records information?
- What or who initiates the appraisal process?
- What are the main steps of the appraisal process?

Data analysis was done manually and included three steps:

1. extracting sentences that answered the questions;
2. sentences were rephrased to statements; and
3. statements were categorized into value domains.

The resulting five value domains, which were common to the three working agents, were used for comparative analysis within each agent and between the agents.

The result was examined from internal and external validity of values (Badersten, 2003/2004), which are presented in the analysis section. Finally the result was related to responsibility theory for aspects of the nature of responsibility taken by archival authorities; to normative theory for aspects of the relationship between the state and its citizens (Lundström, 1988); and to public value aspects (Beck Jørgensen and Bozeman, 2007). These aspects are presented in the discussion section.

**Result**

The result of the comparative content analysis indicates mutual influence between Agents of Theory and Agents of Regulation. Agents of Practice are influenced by Agents of
Regulation and have mutual influence with Agents of Theory. The Coordinated Appraisal theory (Nilsson, 1976) aims to show how power is exercised by public agencies through the intrinsic values in archives. The Macro Appraisal theory (Cook, 2004) aims to mirror societal power relations between public administration societal processes and citizens, by selection of Offices of Prime Interest (OPIs). Agents of regulation, in this case the Swedish Archival Act (Sveriges Riksdag, 1990) and two Swedish archival authorities, show close relationships: the rule of law formalizes the grounds of Swedish societal values; the common good by democracy and transparency. The hierarchy of steering documents in the two organizations studied mirrors the three values in the Archives Act and gives directions based on Nilsson’s Coordinated Appraisal, but are also influenced by thoughts of “impact in society”, later put forward in Macro Appraisal. The professionals that build and effectuate practice see records’ and archives’ usefulness as basic values, and limitations of budget as a restrictive force but as a facilitating factor for users by providing a better overview and structure. In the Swedish example, Coordinated Appraisal shows stronger and mutual influence between theory and norms than does Macro Appraisal which has a one-way influence on Agents of Regulation. Swedish practice and theory communicate with each other, and the influence of Macro Appraisal can be seen in practice. This means that the Canadian example influences Swedish regulating and guiding documents and thus practice but has had no influence at the legal level, being posterior. This is illustrated in Figure 1.

The triangulation shows influences at the general level on practice from both theory and norms. Theories of norms and value influence archival theory and normative values that are translated to archival values, which inform realization in practice. There are reciprocal relations between theory and norms and between theory and practice, but only a one-way influence from norms to practice (Figure 2).

Analysis
Analysis resulted in the identification of five value domains:

1. Aims of appraisal.
2. Basis for analysis.
3. Types of informational value.

![Diagram of Relationships between agents of theory, agents of regulation and agents of practice](Figure 1)
The agents of theory both strive for reflecting or showing power in society, but with different biases, either toward execution or toward relationships. The main difference is that Cook (2004) takes a societal focus including cultural norms. The appraisal process is performed from an outside and top-down view by the archival institution of organizational functions and structures. Responsibility seems to lie exclusively with the archival institution. The fulfillment of needs is limited to history and cultural heritage. Informational value in records is seen as unimportant and the whole of the public archives will be restricted by the impact parameter.

Nilsson on the other hand looks exclusively at the public sector archives: how the administration performed and ruled within its jurisdictions. Nilsson’s archive will emphasize the public sectors’ exercise of power. He protects the intrinsic values in archives. The theory is deeply anchored in western tradition from Jenkinson (1922) to Schellenberg (2003/1956). The appraisal process is performed from an outside view of the whole organizational archive.

The agents of regulation set limits and expectations. Both examples show the aims of archives as being to keep knowledge about the public sector for the future, keeping cost down as much as possible and to secure future understanding of the content in archives. The aims for appraisal are close to Nilsson: to keep knowledge about activities of governing functions rather than minimizing the amount of administrative records and aiming for cost reduction.

The agents of practice act upon the rules set out for them. The state focuses on cultural heritage, “the societal memory”, values in archives and knowledge, whereas the municipality adds accessibility, cultural expressions (for example, citizens’ language as documented in the complaint system), and future understanding to the list of values. The focus is on authoritative power and how it is executed. A separation between records management and archives management functions can be seen in the process, but archivists of the City’s agencies also act as external stakeholders thus providing a more holistic view of records value (Kallberg, 2013, pp. 17-18).

Value domain 1 shows that the intrinsic archival values in Coordinated Appraisal are transmitted from theory to normative to practice levels. Value terms used expose interesting differences in views on the archival mission; Nilsson uses “protect”, Cook “reflect”; agents of regularization use “secure” and “construct”, agents of practice “keep” and “identify”. This
### Value domains

<table>
<thead>
<tr>
<th>Aims for appraisal</th>
<th>Theory level Nilsson/Cook</th>
<th>Normative level State/Municipality</th>
<th>Practice level State/Municipality</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protect intrinsic archival values</td>
<td>Reflect societal values</td>
<td>Secure, comprehensive and justifying knowledge</td>
<td>Keep knowledge and secure value</td>
</tr>
<tr>
<td>The species of the archive – Administrative history and general value of the archive</td>
<td>Interactions creator – citizens – socio-economic processes</td>
<td>The principles codified in the Archival Act</td>
<td>Value creation, Stakeholders’ needs</td>
</tr>
<tr>
<td></td>
<td>Organizational functions and structures</td>
<td>The information needed for the administration of justice, the public administration, and research needs</td>
<td>National overview, Experience</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>A holistic assessment</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Experience Costs</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>National similitude</td>
</tr>
</tbody>
</table>

### Basis for analysis

<table>
<thead>
<tr>
<th>Types of informational value</th>
<th>Direct informational value</th>
<th>Archival value to identify OPI:s</th>
<th>Continuity, data quality, level of aggregation, uniqueness, functional context, business context, Authenticity, Range of impact</th>
<th>The process, the product, Reproducibility, Authenticity, Evidential value, Metadata</th>
</tr>
</thead>
<tbody>
<tr>
<td>Records relational web, The nature of search tools, Evidential value, Proximity value</td>
<td>Social context, Contemporary use, Provenance</td>
<td>---</td>
<td>Accessibility, Reusability of information, Pluralism</td>
<td>Accessibility, Reusability, Important events, Decisions of great consequence</td>
</tr>
<tr>
<td>Control, Insight, Rights protection, Risk for archives impoverishment</td>
<td>Ability to produce records valuable on a global level, “Hot spots”</td>
<td>Destruction normally granted when not against the three principles of the Archival Act</td>
<td>Technical aspects, Precision in metadata, Accessibility, Interdependencies, Economic values, Volumes, Authenticity, Originals are important for a time, after that scanned copies will suffice. Cost aspects of storage and migration/conversion, Search time for access, Linked systems</td>
<td>Mirror business, Events of controversial nature, Impact rate, The right to access, Cost aspects: – storage and maintenance – need and non-retrievability (after destruction)</td>
</tr>
</tbody>
</table>

### Types of informational value

<table>
<thead>
<tr>
<th>Direct informational value</th>
<th>Archival value to identify OPI:s</th>
<th>Continuity, data quality, level of aggregation, uniqueness, functional context, business context, Authenticity, Range of impact</th>
<th>The process, the product, Reproducibility, Authenticity, Evidential value, Metadata</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Influential factors

| Reasons for retention/destruction | Control, Insight, Rights protection, Risk for archives impoverishment | Ability to produce records valuable on a global level, “Hot spots” | Destruction normally granted when not against the three principles of the Archival Act | Technical aspects, Precision in metadata, Accessibility, Interdependencies, Economic values, Volumes, Authenticity, Originals are important for a time, after that scanned copies will suffice. Cost aspects of storage and migration/conversion, Search time for access, Linked systems |
|---------------------------------|-------------------------------------------------|-------------------------------------------------|-------------------------------------------------|
| | | | |

### Reasons for retention/destruction

<table>
<thead>
<tr>
<th>Control, Insight, Rights protection, Risk for archives impoverishment</th>
<th>Ability to produce records valuable on a global level, “Hot spots”</th>
<th>Destruction normally granted when not against the three principles of the Archival Act</th>
<th>Technical aspects, Precision in metadata, Accessibility, Interdependencies, Economic values, Volumes, Authenticity, Originals are important for a time, after that scanned copies will suffice. Cost aspects of storage and migration/conversion, Search time for access, Linked systems</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

Table II. Compiled results of the comparative analysis of the appraisal.

---

Table II. Compiled results of the comparative analysis.
exposes a difference between the state to “secure” and “keep”, contrasting with the municipality to “construct” and “identify” archival heritage. It indicates a mindset inclined toward postmodernism in the municipality. The terms used by the state are directly linked to Nilsson’s value term “Protect”. The terms used by the municipality are not directly linked to Cook’s value term but indicate distance, or a neutral stance toward the role of appraising archivist.

**Value domain 2: basis for analysis**

Agents of theory assume two divergent angles for analysis. Nilsson specifies intrinsic values as being the spices of the archive, but this is from an outside perspective, that is, from the archival institution view, and without respect to the archive holder. The general value of the archive is related to the administrative history of the governing instances (Nilsson, 1983). Cook specifies an interest in interaction between the socio-economic processes. The functions and structures of agencies are to be thoroughly examined by an archival authority to gain good understanding of the organization before doing the actual appraisal (Cook, 2004).

The agents of regulation use the Archival Act §3 for value assessment (Sveriges Riksdag, 1990). Other Acts are also included, mostly for required retention periods for less valuable records series. Information and records quality and secondary values are of interest. Primary business values are left in the hands of the archive holders, i.e. the administrative agencies.

Agents of practice tell us more about what they use for analysis. For example the high value of raw data and knowledge about how value in databases was created. The intention is also to take a holistic view both internally and nationwide. Experience and common practice are mentioned, for example “grounded in experience” and “develop a praxis built on opinion and reflection” (my translation). Cost aspects are taken into consideration for preservation, maintenance and storage, not for informational loss. Although there is awareness of the costs of redoing work due to lost records, this is normally not included in the cost calculation.

Value domain 2 shows no direct transmission from theory to normative level. The three principles of the Archival Act are the leading normative motives and thus the basis for appraisal, and no major difference is apparent between the state and the municipality. At practice level the principles are expressed differently. The municipality puts forward holistic assessment and national similitude, the state takes a national overview as account for value. Their holistic view and national overview seem to be influenced by Nilsson’s idea of coordinated appraisal and interest in administrative history, but may also be influenced by Cook’s idea of macro appraisal, from a top-down view.

**Value domain 3: types of informational value**

Agents of theory diverge in their view of the comprehensiveness of archives content. Nilsson identifies that direct value is in records content, facts atmosphere and views, and indirect value in the procedures that tell about work cultures and organization. Cook, on the other hand, aims at a specific outcome of archival value that is to identify Offices of Primary Interest. These are assessed by estimating social value, cultural heritage, economy, defense and international contacts. A consequence is that Cook is prepared to dispose of whole archives, while Nilsson seems to value a completeness of administration.

The agents of regulation emphasize quality, context, authenticity and accessibility as value in information. Quality of metadata is specified in policy documents as a value, especially for electronic records. Agents of practice seem to have been influenced by Cook,
mentioning impact rate, economy and cultural expressions such as how citizens’ express themselves in contact with public agencies. Informational value lies in enduring records series, quality and context, and uniqueness. The municipality includes cultural expressions as a type of informational value. The practitioners are also aware of value for users; in addition to accessibility, memory and evidence, they also foreground usability, that is, to be able to re-use archival records, not only for information.

Value domain 3 shows direct transmission from theory to practice of Nilsson’s direct informational value. At the theoretical level ideas of types of informational value are more or less converse. Nilsson looks at archival information for knowledge or other usable informational value that lies in archival records. Cook on the other hand rejects informational value, he uses the concept of archival value to identify the more interesting parts of public administration. At normative level there is little difference, probably an effect of the two organizations using the same source – the National Archives policy (Riksarkivet, 1995).

Value domain 4: influential factors

Differences between the two agents of theory are exposed by what each one asserts should be prime considerations in appraisal: their views on internal and external values. Nilsson looks at search tools – that is internal in the archive but with the future in mind. Cook looks at the social context, not records context and looks at contemporary use. Nilsson focuses on the informational values while Cook looks at provenance that is the archive holder/creator. The agents of regulation highlight impact as being influential. The agents of practice highlight access and reuse, and pluralism which may be influenced by current politics, where globalization and ethnic issues were hot topics at the time of the interviews.

Value domain 4 shows a more complex picture which broadens the grounds for appraisal and shows deviation from Nilsson’s path. The impact factor, promoted by Cook, appears as a state norm and is used by the municipality practitioners. The dominance of informational value in Nilsson’s thinking and Cook’s converse ideas of a societal overview is salient at the theoretical level in this domain. Here some interesting things appear: the impact factor, a prime value parameter of Cook’s appears in both the state normative documents and at the practice level of the municipality. This is interesting also as the content analysis of the normative level in the municipality gave no clear answer on influential factors.

Value domain 5: reasons for retention/destruction

The agents of theory diverge on aspects concerning the relationships between state and society and citizens. Nilsson promotes aspects that are value based in the common good of democracy and the value of archives for delivering highly cherished qualities: insight into how power is executed in public agencies. Cook, on the other hand, put forward value aspects based in democratic interactions in societal-historic processes showing power relationships. The top-down perspective he promotes does not seem to contain the smaller players in society, it is a bird’s eye perspective, were value is placed on impact and hot spots, interpreted as domains or events that echo their times. Agents of regulation focus on legislation, the Archival Act, and the importance of authenticity. The agents of practice are more specific, and identify several aspects as grounds for either keeping or destroying. These aspects are parameters for assessment.

Value domain 5 shows a return to general aspects of values assessed in appraisal investigations. This domain shows a developed practice, based on Nilsson’s aspects of informational value and influenced by Cook’s notions on impact. Technical aspects and economic realities are present, the latter not always for the good of use and usability.
Nilsson’s aspects are based in informational content of the archives. Cook broadens the view from the informational content to impact aspects of Organizations of Prime Interest, especially those of interest at a global level. The National Archives refers to the value principles of the Archival Act and the municipality looks narrowly at records quality. For the agents of practice, cardinal aspects are quality, usability and costs.

Discussion
This section sets out the Swedish example and the result of content analysis and triangulation of theory, regulation and practice in relation to the theories of norms, values and responsibility.

As is shown above, the whole responsibility for scoping and keeping the archive lie in the hands of the archive holders until disposal. The archival authority gives normative directions and guidance and decides on retention and destruction.

Normative directives and appraisal practice seem in a way pinioned by given definitions for official and archival record in legislation and the way responsibility is allocated. The result is gaps in coverage of appraisal scope. For example:

- **Rule 1**: The decision on what is a official/archival record is taken by the archive holders on at least two occasions; when access is required (Sveriges Riksdag, 1949, §14) and when scoping for appraisal and retention decisions. One respondent pointed out that the same kind of record can thus be public in one agency and not in another, affecting the value of the archive as this type of record may be of interest for business, the public or any other stakeholder for future interests; and

- **Rule 2**: Responsibilities divided between the archival authority and the archive holder (Sveriges Riksdag, 1990). The archive holder performs an appraisal inquiry and makes retention decisions which are proposed to the archival authority. The archival authority performs an appraisal inquiry for long-term value. The decision does not consider anything that is not in the proposal (Riksarkivet, 2014).

The problem seems to lie in the combination of these two rules. There are two ways of knowing what is included in the archive; one is when an enquiry for access is received; the other when a whole or a part of an archive crosses the threshold to a central archive or an archival institution. At disposal to an external archive, the account of what is delivered is at series level, and does not specify the boundaries of the scope, the records that were not appraised as official.

A question is, how and when should the scope of appraisal be set? Scoping is an important step in creating values in archives, for values of cultural heritage or other values such as knowledge development and economic growth as in the idea of open data (Group of Eight and G7, 2013). In reality records are already appraised before capture (McKemmish, 2005). The data show that in Sweden the problem is that this appraisal is done with strictly business focus or even intuitively by anyone handling business information in an organization, even in a public organization. Basic knowledge about appraisal and the standing of records should be a requirement for all employees managing records (International Organization for Standardization (ISO), 2016, 15489), but this is not always the case. In the end public archives are to be transferred to a national or central archive. What happened on the way, how decisions were taken on what to include or exclude as official and archival record depends on any case handler or other officer handling information and records and their knowledge and interest. This is also a question of accountability and transparency into public sector operations (Hurley, 2005b). In the digitally transformed office and business environment the technical and system
management officers also play their part in scoping the archive. This shows a gap in the inquiry process combined with a risk of lack of electronic appraisal competences and of public values.

The definition of an official record in Swedish legislation (Sveriges Riksdag, 1949, ch 2, 3§) focuses on case-related records created and received. Registers, diaries and databases are also official records. Work notes and memoranda are not official records except when adding facts to a case (Sveriges Riksdag, 1949, ch 2, 9§). The standing of official record is closely connected to citizens’ right of access. Status as an official record is tested when access is requested and when disposal is an issue. This means that in daily business there is no common awareness and knowledge among all employees and consultants about records status and subsequent implications, which conveys a gap in assigned responsibility.

Responsibility is divided into three categories; causal, sanction and task responsibility (Lundström, 1988). The question is whether responsibility is taken and what kind of responsibility is desirable. Table III gives an overview of the options:

<table>
<thead>
<tr>
<th>Responsibility theory</th>
<th>Looks at</th>
<th>Judges by</th>
<th>Conclusion</th>
</tr>
</thead>
<tbody>
<tr>
<td>Causal responsibility</td>
<td>Effect of action</td>
<td>Consequence</td>
<td>Not taken</td>
</tr>
<tr>
<td>Sanction responsibility</td>
<td>Effect of action</td>
<td>Normative system</td>
<td>Not taken</td>
</tr>
<tr>
<td>Task responsibility</td>
<td>Duty to act</td>
<td>Fulfillment</td>
<td>Taken</td>
</tr>
</tbody>
</table>

Normative theory provides aspects on obligations between the state and its citizens in democracies. Table IV summarizes normative theories (Lundström, 1988).

Among these three, Sweden as a welfare state is placed in the category of Theory of Resources. Where a state interferes in the life of its citizens, the right to timely access to usable public records independent of whether they are “current” or “historic” becomes an important archival value. Public values then come into focus.

Value domains connected to the public sector are divided into 7 categories with subsets (Jørgensen and Bozeman, 2007). This paper suggests that the working agents of appraisal and archival value can be connected to these categories and subsets of public values. The value categories that are promoted by the various working agents are shown in table V:

**Conclusions**

This paper explores electronic records appraisal and aspects of normative values in archives in theory, regulation and in practice. The paper also reflects upon responsibility for the result of records appraisal, the value in archives and whether views on appraisal can connect to normative theory and the relationship between state and citizen. The research question was:

<table>
<thead>
<tr>
<th>Theory</th>
<th>Role of the state</th>
<th>Commodities</th>
<th>Individuals</th>
</tr>
</thead>
<tbody>
<tr>
<td>Theory of rights</td>
<td>Passive, neutral and fair</td>
<td>Transfer to citizens</td>
<td>Strong rights</td>
</tr>
<tr>
<td>Theory of resources</td>
<td>Interfering</td>
<td>Apportions to citizens</td>
<td>Rights and obligations</td>
</tr>
<tr>
<td>Utilitarian theories</td>
<td>The end justifies the means</td>
<td>Rich → Poor</td>
<td>Not important</td>
</tr>
</tbody>
</table>

"Swedish digital records appraisal"
RQ1. How do appraisal theory, normative regulations and appraisal practice meet the aim of values in digital archives?

The research question indicates a flow from theory to regularization to interpretation and effectuation by practice. The result indicates that such a flow is bi-directional between theory and regulation and theory and practice, but one way from regulation to practice (Figure 1). Changes in norms and mindsets, in this case consequences of digital transformation, do not necessarily follow from the development of ICT. Agents of practice in the Swedish example show awareness of appraisal problems related to digital records, as shown in the analysis.

One conclusion is that in the Swedish context there is little interest in interaction with society. The activities of administration are what is preserved, and the underlying norms are democratic values of the common good, as rights to access and to use official records in archives. The view of archives as part of cultural heritage seems to be limited to official authority archives. The influence from Nilsson and the Swedish National Archives policy is apparent. The norms of the 1980s, that laid ground for the Archives Act, dominate records and archives appraisal.

Divided responsibility as in the Swedish example exposes two kinds of risk; (i) Accountability control on grounds other than bureaucratic and legal requirement is low (Hurley, 2005b). (ii) Knowledge of records and archives appraisal grounds, parameters and values may be set aside due to lack of archival competences in business operations. These [archival] competences are normally not asked for until the moment of redundancy and need of disposal. The Swedish example shows how societal norms formalized in rules and regulations bind appraisal performance to paper thinking by positioning the appraisal inquiry at the threshold of the archival institution. This leaves prevalent archival discourse and effects of digital transformation aside, even when it is apparent that digital transformation purports archival values in possibilities for usability and data processing.
Some conclusions drawn are as follows:

- At present, the Nilssonian theory and norms of the 1980s dominate but are influenced at practice level by the Macro Appraisal theory of Cook. An example is adoption of a sector view in sector analysis in state retention decisions and to some extent the use of impact factor as a parameter for appraisal (Riksarkivet, 2012).
- The cost of storage and preservation (Fredriksson, 2003) continues to be a dominant factor, but costs of loss of information due to destruction are also mentioned.
- Appraisal is restricted to redundant records due to the default preservation rule which entails a black box of lost and unknown records.
- An active appraisal process starting at records capture (Upward, 2005) should replace the re-active process in the digitally transformed environment.

The high-level archival values stated in the Archives Act are grounded in societal norms of democracy and transparency and citizens' needs. The problems lie in:

- divided responsibility;
- the main two-step process; and
- a re-active selection model (McKemmish et al., 2005, pp. 175-177) applied at the threshold of the archival institution, resulting in the “black box” mentioned above.

Responsibility is taken for appraisal performance according to allocated tasks. Responsibility is not taken for follow-up of appraisal results, whether or not the value requirements specified in rules and regulations are fulfilled by the archives, after appraisal and disposal (Table IV). Causal responsibility should be desirable and diminish the problem of the “black box” by knowledge-based professional appraisal beginning at records capture combined with structured follow-up activities, which may be automated.

Archival value and informational value in records reciprocally build value, as value in records builds value in archives and the archival context strengthens the value of records. In the same way Nilsson and Cook show that archival value is strengthened by the context in a network of archives. Value is identified through records appraisal thus creating value in archives (Brothman, 1991). Assessment is performed by the use of value parameters, cultural norms, scientific paradigms and practice. These change over time. By definition the value of records and archives is:

- The fulfillment of needs, substantiated through access (Klett, 2017; Menne-Haritz, 2001).

Needs are not predictable for the appraisal team in any way other than through knowledge of past and current use of archives. In view of the findings of this research this paper suggests adding the following to the definition above:

- The basic concepts of archival values are memory, relations, benefits and usability.

“Primary and secondary value” (Schellenberg, 2003/1956) have been thought of as a concept, but in the light of digital transformation are merely a matter of use and usability in a time and space (continuum) perspective. Use and usability require authenticity, access and the means to process or elaborate archival records.

Further research on electronic records appraisal is needed and several interesting possibilities arise from the problems identified in the conclusions. For example, whether the value in archives is as is intended, or whether the appraisal parameters are functional for the actual value found in archives. Is the question of responsibility vital for the appraisal result? This paper suggests pilot projects to support appraisal
decisions, built into systems of business intelligence. Various professions should be involved, cooperating in a structured way at system level, setting and supporting business procedures in appraisal knowledge.

References


Group of Eight and G7 (2013), “Open data charter”.


Further reading


Corresponding author
Elisabeth Klett can be contacted at: elisabeth.klett@miun.se

For instructions on how to order reprints of this article, please visit our website: www.emeraldgrouppublishing.com/licensing/reprints.htm Or contact us for further details: permissions@emeraldinsight.com
An integrated framework to elevate information governance to a national level in South Africa

Paul Anthony Mullon
COR Concepts, Centurion, South Africa, and
Mpho Ngoepe
University of South Africa, Pretoria, South Africa

Abstract

Purpose – As an emerging discipline, information governance (IG) presents a number of challenges to organisations and countries. For example, IG has not yet been clearly defined and current proponents present the concepts as records management, information management, enterprise content management, privacy (data protection), freedom of information, corporate governance, information risk, information security and e-discovery, to mention just a few areas. At an organisational level, initiatives focus on one of these aspects, often conflicting with the other elements, and are initiated because of some immediate business challenge, such as the introduction of the Protection of Personal Information Act (data protection or privacy legislation) in South Africa. This is compounded by the fact that the country creates many fragmented policies and pieces of legislation on the same IG aspects which are conducted in a disjointed manner. This study aims to present an integrated IG framework at the country level, comprising key success factors, required instruments (policy and legislation), principles and a proposed list of elements or disciplines, which should be managed in a cohesive manner.

Design/methodology/approach – This study adopted the Information Governance Initiative’s pinwheel facets of IG to design an integrated framework of elevating IG to country level. The pinwheel helped to identify different facets of information disciplines and the responsible oversight mechanism for implementation in South Africa. The study relied on data obtained through content analysis of policy documents, legislative frameworks, and literature review regarding the identified facets of IG in South Africa.

Findings – The study established that only some aspects/domains/facets of IG are legislated and driven by policy in South Africa. These domains are at different levels of maturity and different stakeholder groups are responsible for each domain; for instance, the National Archives of South Africa is responsible for records management and the State Information Technology Agency is responsible for information technology, while the newly established Information Regulator is responsible for freedom of information and data privacy. There is generally no over-arching structure responsible for overall IG in South Africa as the elements are fragmented in various oversight mechanisms and institutions. As a result, domains compete for limited resources and often lead to “knee-jerk” responses to legislative, legal or risk drivers.

Research limitations/implications – It is concluded that if IG is not regulated and modelled at a country level, it is highly unlikely to filter down to organisations. Implementing IG at country level will go a long way in helping to filter it down to an organisation level.

Originality/value – The study is useful by presenting a framework to ensure that IG is implemented at the country level with a single coordinating body established for oversight mechanisms such as the Information Regulator (which currently has a narrow scope of privacy and freedom of information, although with limited resources).

Keywords Information technology, Records management, South Africa, Freedom of information, Information governance

Paper type Conceptual paper
1. Introduction

This study stems from the development of an integrated information governance (IG) model for organisations, which was initiated because of a perceived lack of consistent understanding of IG across various industry sectors in South Africa. While there is no standard definition for IG per se, there is also no clear model for managing all aspects of IG at the country level. There is no evidence at all of IG having been described at the country level, in any country. Franks (2013, 2015), Hagmann (2013) and Gartner (2018) mostly define IG at an organisational level. As an emerging discipline, IG presents a number of challenges to organisations and countries. For example, IG has not yet been clearly defined and current proponents present the concepts as records management, information management, enterprise content management, privacy (data protection), freedom of information, corporate governance, information risk, information security and e-discovery, to mention just a few areas, at the organisational level (Franks, 2015). The IG approach and focus of the various proponents stem almost entirely from the current mindset and historical expertise of various organisations. Furthermore, the responsibility of IG at the country level, especially in South Africa, is not clear (Mullon, 2017). In South Africa, as described in the King III report, IG has mostly been limited to information technology governance.

The concept of IG is still new but is gaining popularity all over the globe (Hagmann, 2013). Indeed, IG has emerged globally in recent years in various guises, such as records management, freedom of information, e-discovery and information privacy. It encompasses all data activities. Early references to IG appeared in the late 1990s, focusing primarily on health-care information in the UK. Since the mid-2000s, it has been used to describe various disciplines and has been used by the vendor community as a catch-all for information-related services. As a result, it lacks a clear definition and is used to mean many different things. For example, Franks (2015) defines IG as an integrated strategic approach to managing, processing, controlling, maintaining and retrieving information as evidence of all transactions of the organisation. This definition takes its lead from records management, where records are regarded as evidence of the activities of the organisation. Gartner (2018) contents that the concept includes the processes, roles, policies, standards and metrics that ensure the effective use of information to enable an organisation to achieve its goals. In both the definitions, the focus is on an organisation. Changes in corporate governance, new information-related global legislation and regulations and the rapid increase in the amount of information in use in organisations have led to the need to clearly define a framework for IG, with a consistent definition, appropriate inclusion of affected disciplines and an approach to implementation. According to Hagmann (2013), in the absence of a framework, the danger is that organisations just rebrand existing records and information programme into an IG programme. Although a bit ambitious, this calls for elevation of IG to the country level, covering both the public and private sectors. For example, in South Africa, private sector organisations are required to comply with various pieces of legislation, depending on the nature of their business. There is no single law which imposes records retention requirements on all private sector organisations. Even in the public sector, where the National Archives and Records Service of South Africa (NARSSA) Act govern records management, it does not impose retention periods, but rather point to other disparate pieces of legislation.

While working with stakeholders from the public sector, it became apparent to the authors of this article that no single organisation in South Africa has an overarching responsibility for IG at the country level. This was especially evident in 2018 as the country sought to develop regulations for the newly promulgated Protection of Personal Information Act (Act No. 4 of 2013). This Act is administered by the Information Regulator (Regulator),
which is part of the Department of Justice in South Africa (Information Regulator, 2018). The Regulator is also responsible for freedom of information, which in South Africa is governed by the Promotion of Access to Information Act (Act No. 2 of 2000). It is worth noting that previously, freedom of information legislation was the responsibility of the South African Human Rights Commission until 2016 (Mojapelo, 2017; Mojapelo and Ngoepe, 2017). The proliferation of technology has further fragmented the elements of IG as the State Information Technology Agency (SITA) in South Africa is responsible for IT governance. All these functions of IG are interrelated, but executed in silos by different organisations. As a result, there is no mechanism of dealing with duplication of functions and intellectual efforts. This study adopted the Information Governance Initiative (IGI) model as a guide to propose a framework for IG that can be applied at the country level, which in turn can be implemented at the organisational level. In this regard, the focus of the study is to identify the various interpretations of IG in use in South Africa and the various existing frameworks that can be used to encompass all related disciplines. The article recognises that issues such as information privacy, freedom of information, IT governance and records management are all important and any one of them could be a catalyst for an IG implementation. It is further recognised that organisations have departments or functions specifically designed to govern and manage these disciplines, often in a silo and with little regard for other related IG disciplines. For example, Mojapelo (2017) and Ngoepe and Van der Walt (2009) report that in some government agencies, access to information is managed by the legal departments, while in others, it is either IT or records management departments. This may be due to the absence of a national framework to guide the implementation at the organisational level. The silo of business information and processes has long been a hindrance to the management of an organisation’s data, and it continues to be a primary barrier to progress in the implementation of IG policies that successfully maximise the value of data and minimise risk (Information Governance Initiative, 2018).

The underlying assumption is that countries are also faced with an IG requirement, which generally translates into laws, regulations and other governance instruments which provide for an element of each IG discipline. Furthermore, administration, monitoring and governance of the discipline fall within the mandate of a specific government entity. In the same way that organisations struggle to implement IG in a cohesive manner because of the “silo” nature of the organisational functions responsible for each discipline, it is expected that the same will apply at the country level. As a result, IG implementations are potentially incomplete and comprise fragmented initiatives leading to often overlapping, conflicting or duplicate initiatives (Mullon, 2017). For example, in the Limpopo Province in South Africa, while the premier’s office is responsible for transversal records management throughout the province, the Limpopo Provincial Archives is also responsible for regulating records management activities in provincial departments and municipalities. There is a clear duplication of functions and effort in this regard. The same applies at the national level where SITA sometimes implements electronic records management without the involvement of the NARSSA, which has a statutory regulatory role regarding records management in governmental bodies (Ngoepe, 2015). Although mitigated through a memorandum of agreement between NARSSA and the Auditor-General of South Africa (AGSA), the situation could have played itself out where the AGSA audits records management in governmental bodies, a function which is the responsibility of NARSSA.

Unless government adopts a cohesive, unified approach to IG at the country level, it is probable that organisations will struggle to implement IG in a unified manner, as each function will be faced with reporting and compliance obligations to a multitude of different government oversight regulatory bodies. This is the case in South Africa, and this study
hoped to identify the responsibilities of each IG element and propose the national framework. For the purpose of this study, IG is the set of multi-disciplinary structures, including oversight mechanisms, policies, procedures, processes, standards and controls available at the country level, to manage information on all media in such a way that organisations can customise to support their immediate and future regulatory, legal, risk, environmental and operational requirements.

2. Models for information governance used in South Africa

A few models and frameworks have emerged from various organisations and initiatives, all focusing on IG from different perspectives. As IG is maturing, various models are changing their direction while retaining their core area of expertise. As the concepts emerge, the definition changes and matures. For example, according to Smallwood (2014):

IG is a sort of super discipline that has emerged as a result of new and tightened legislation governing businesses, external threats such as hacking and data breaches, and the recognition that multiple overlapping disciplines were needed to address today’s information management challenges in an increasingly regulated and litigated business environment.

Without providing a specific definition, the concepts in Smallwood’s description provide insight into how IG ties directly to legislation and other governance requirements. As Smallwood (2014, p. 462) expands further:

IG is a subset of corporate governance and includes key concepts from records management, content management, IT and data governance, information security, data privacy, risk management, litigation readiness, regulatory compliance, long-term digital preservation and even business intelligence.

Perhaps this expansion explains why in South Africa, the corporate governance framework (King Report) initially listed IT governance (as compared to IG) as an umbrella term; hence, Ngoepe (2012) recommends that the proper concept to be used is IG. In this way, it will encompass all other elements of IG rather than curtail it to IT perspective only.

Finally, Smallwood (2014) ties IG once again to legislation, as it includes the set of policies, processes and controls to manage information in compliance with external regulatory requirements and internal governance frameworks. This inclusion of oversight mechanisms emphasises the need to elevate IG to national level. A number of frameworks have been developed for implementation at the organisational level and some are applied by some institutions in South Africa. The following have been identified:

- **COR Concepts information governance framework**: The IG framework was developed by Mullon (2017), and this framework is mainly implemented in various organisations where he consulted on IG in southern Africa, including, the Reserve Bank of South Africa and the eSwatini Revenue Authority. Mullon’s framework includes three essential pillars, namely, instruments (policy and legislative framework), infrastructure (technology) and interest (people, change management and accountability).

- **Corporate governance using the King IV Report**: The corporate governance framework in South Africa is the King IV Report, which emphasises the need for information and technology governance, but does not provide detailed guidance (Institute of Directors in Southern Africa, 2009). The previous King reports (I, II and III) placed much emphasis on IT governance as if the concept embraces the wider IG (Ngoepe, 2012). As Ngoepe and Ngulube (2013) would attest, IT does not constitute IG, but it is an enabler and a component within IG.
• **Association of Information and Image Management (2018):** It provides a certification for IG but does not provide a single framework or model. They focus primarily on enterprise content management, but they have subsequently expanded to include other elements of IG.

• **ARMA principles and information governance maturity model:** This model focuses primarily on records management and has been adapted and aligned to the Electronic Discovery Reference Model (EDRM) e-discovery IG framework.

• **ARMA information governance body of knowledge:** ARMA International (2018) defines IG as a “strategic, cross-disciplinary framework composed of standards, processes, roles, and metrics that hold organizations and individuals accountable for the proper handling of information assets”. The framework helps organisations achieve business objectives, facilitates compliance with external requirements and minimises the risk posed by sub-standard information handling practices.

• **IT governance models, with Cobit5 as an initial reference point:** The focus of this model is on IT governance, with awareness of the need to govern information as a core element. Cobit5 does not purport to be an IG framework but is included, as there is often confusion between IT governance and IG as also reflected in the first three corporate governance reports (the King reports) (Ngoepe and Ngulube, 2013). According to Chauke (2018), the Department of Transport in South Africa used Cobit5 in implementing its IT governance.

• **IBM information governance maturity model:** IBM defines IG as “the disciplines, technologies, and solutions that are used to manage information within an enterprise in support of business and legal requirements. Information governance encompasses a broad set of subjects covering information quality, information protection, and information lifecycle management.” IBM has had a long-standing interest in data governance, and established the Data Governance Council in 2004. Of particular interest is that IBM changed this to IG in 2010, recognising that “information governance is a business concern, and not just a data concern”. The IBM Data Governance Forum has since evolved to become the Compliance, Governance and Oversight Council (GGOC), which has a far broader focus than data governance. The CGOC has adopted the EDRM information governance reference model (IGRM) as a basis.

• **Data Management Association International and Data Management Body of Knowledge framework for data governance:** While Data Management Association International (DAMA) in its widely acknowledged Guide to the Data Management Body of Knowledge (DAMA-DMBOK2) uses the terms “data governance” rather than “information governance”, in its preamble and definitions, the Association uses the terms data and information interchangeably. In the DAMA framework, what is described as data governance is described as IG elsewhere.

• **Electronic Discovery Reference Model:** The IGRM emerged from a need in the e-discovery community to have a framework for information management (EDRM, 2018). The primary focus is on e-discovery and, in doing so, it includes a heavy focus on the need to identify, capture and govern all information. The EDRM’s IGRM is widely used and has been adopted by both ARMA (where it has been aligned with the Generally Accepted Recordkeeping Principles) and the CGOC (Franks, 2015).
Within this emerging IG discipline, the IGA pinwheel infographic reflected in Figure 1 identifies the various potential facets of IG. The pinwheel clearly demonstrates the coordinating role of IG. It represents the promise of IG to finally put an end to the disjointed approach to information management that is witnessed in so many organisations, an approach that leads to poor governance outcomes and a failure to extract value from information (Information Governance Initiative, 2018; Ngoepe and Ngulube, 2013). This pinwheel was adopted in this study and helped to understand and identify the organisational disciplines and functions that should be represented in IG. The identified IG facets then informed the identification of stakeholders responsible for each element and the development of a national framework. The pinwheel offers great value as it identifies the elements/facets/disciplines which potentially comprise IG at the organisational level and, for this study, at the country level.

Figure 1.
The various facets of IG

3. The role of standards in information governance

The importance of standards in IG has been raised by Lomas (2010) when arguing that:

\[ \ldots \] embedding the international information security standard such as ISO 27001 in conjunction with the records management standard ISO 15489, will deliver a holistic information governance strategy that is responsive to change.

Indeed, most focus areas or disciplines within IG are addressed by at least one international standard or framework. The list reflected in Table I would be too comprehensive for this paper, but some key standards are listed as they highlight the fact that the disciplines are addressed in isolation. It must be noted that this is not designed to be a complete list, and the authors recognise that many industry bodies have developed other standards which are widely recognised and used by their respective communities. Furthermore, these standards are each developed under different technical committees, each with their own focus and area of specialisation. A process and framework for liaisons and stakeholder inclusion is integral to the development of standards; however, the risk always exists that a standard will take a direction to the detriment of some stakeholder requirements.

In South Africa, various governmental bodies have adopted international standards and use them either as guidelines or include them in their policy frameworks. For example, the NARSSA draws heavily on ISO records management standards in the development of policy. As is the case in many countries, the NARSSA Act does not apply to the private sector; hence, records management standards are used for guidance, although there is no legislation dictating that private organisations should use any particular standard. This is the case for almost all legislations having an IG component.

4. Methodology

This study adopted IGIs pinwheel facets of IG to design an integrated framework of elevating IG to the national level. The pinwheel helped to identify different facets of information disciplines and the responsible oversight mechanism for implementation in South Africa. The study relied on data obtained through content analysis of policy documents, legislative frameworks and literature review regarding the identified facets of IG in South Africa. The disciplines identified by the IGI have been used as a starting point

<table>
<thead>
<tr>
<th>Discipline</th>
<th>International standards</th>
</tr>
</thead>
<tbody>
<tr>
<td>Records management</td>
<td>ISO 15489:2016 Records management</td>
</tr>
<tr>
<td></td>
<td>ISO 30300 Family: Management system standard for records</td>
</tr>
<tr>
<td>Information security</td>
<td>ISO/IEC 27001: Information security management system</td>
</tr>
<tr>
<td>Corporate governance</td>
<td>ISO 19600:2014 Compliance management systems – Guidelines</td>
</tr>
<tr>
<td></td>
<td>ISO/AWI 37000 Guidance for the governance of organisations (under development)</td>
</tr>
<tr>
<td>Privacy</td>
<td>ISO/IEC 29100 Privacy framework</td>
</tr>
<tr>
<td></td>
<td>ISO 27018 Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII Processors</td>
</tr>
<tr>
<td>Freedom of information</td>
<td>Few specific standards for FOI, but many related standards can be applied</td>
</tr>
<tr>
<td>IT governance</td>
<td>ISO/IEC 38500:2008</td>
</tr>
</tbody>
</table>

Table I. List of standards and frameworks for IG
as this is a comprehensive list of potential disciplines which could be considered in a
country-wide IG framework and ultimately implemented in organisations. These disciplines
are listed and are used to determine whether they are catered for in the South African
country governance framework. The analysis was done thematically as guided by the facets
of the IGIs pinwheel. This also helped to identify the facets, related legislation and
stakeholders.

5. Facets of information governance and responsible stakeholders in South
Africa
There are a number of South African Government entities responsible for implementing
various aspects of IG. Different public organisations are accountable for different aspects of
IG, as identified in Figure 1. However, there is no coordinating entity to ensure alignment.
Furthermore, there is a duplication of effort or conflict between the various resulting laws.
For example, while public records can be accessed only after a period of 20 years in terms of
the NARSSA Act, the Promotion of Access to Information Act makes provision for access of
records without stipulating the age of a record. Table II provides a summary list of public
entities responsible for IG facets in South Africa.

<table>
<thead>
<tr>
<th>Organisation or accountable entity</th>
<th>Legislative mandate</th>
<th>Applicable legislation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minister of Telecommunications and Postal Services</td>
<td>Facilitation and regulation of e-Government services and electronic communications and transactions with public and private bodies, institutions and citizens</td>
<td>Electronic Communication and Transaction (ECT) Act of 2002</td>
</tr>
<tr>
<td>Minister of Public Service and Administration (MPSA)</td>
<td>Mandated to foster good governance and sound administration in the public service Establish norms and standards related to, amongst other, information management and electronic government in the public service</td>
<td>The Public Service Act of 1994</td>
</tr>
<tr>
<td>Minister of Public Services and Administration</td>
<td>Sets out regulations for e-Government Requires all departments to manage information technology (IT) effectively and efficiently, taking into consideration that IT must improve the delivery of public services, the productivity of the department and the cost-efficiency of the department</td>
<td>Public Service Regulations of 2001</td>
</tr>
<tr>
<td>Minister of Public Services and Administration</td>
<td>Information security whereby the MPSA is required to issue a handbook called the Minimum Information Security Standards (MISS). All persons working with public service information resources will be required to comply with the MISS The final area deals with interoperability whereby the MPSA in consultation with the Government</td>
<td>Minimum Information Security Standard (MISS) of 1996</td>
</tr>
</tbody>
</table>

Table II.
List of public entities in South Africa responsible for different IG facets (continued)
<table>
<thead>
<tr>
<th>Organisation or accountable entity</th>
<th>Legislative mandate</th>
<th>Applicable legislation</th>
</tr>
</thead>
<tbody>
<tr>
<td>SITA</td>
<td>Mandated to provide IT, information systems and related services to, or on behalf of, participating departments and in regard to these services, act as an agent of the South African Government with the Minister of Telecommunications and Postal services as the sole shareholder representing the government SITA Act requires the Agency to set standards for the interoperability of information systems and standards for a comprehensive information systems security environment for departments</td>
<td>SITA Act of 1998</td>
</tr>
<tr>
<td>National Planning Commission (NPC)</td>
<td>The strategic framework to form the basis of future government planning Although, the NDP 2030 does not mention e-government as a key enabler to the implementation thereof, it is important that the key elements of the NDP 2030 are taken into consideration in the development of the e-government strategy to ensure that the long-term objectives of the e-government strategy are aligned to those of the country</td>
<td>National Development Plan</td>
</tr>
<tr>
<td>Information regulator (Part of Department of Justice)</td>
<td>Development and implementation of privacy legislation</td>
<td>The Protection of Personal Information (POPI) Act of 2013</td>
</tr>
<tr>
<td>Human Rights Commission</td>
<td>Development and implementation of Freedom of Information Legislation. NOTE: This will fall under the auspices of the information regulator in future</td>
<td>Promotion of Access to Information Act</td>
</tr>
<tr>
<td>Not yet assigned</td>
<td>Freedom of Information implications</td>
<td>Protection of State Information Act (Bill)</td>
</tr>
<tr>
<td>Cabinet</td>
<td>National Integrated ICT Policy White Paper by cabinet in October 2016</td>
<td>N</td>
</tr>
<tr>
<td>N/A</td>
<td>The Information Society and Development (ISAD) Plan of 2007</td>
<td>NARSSA Act of 1996 and its regulations</td>
</tr>
<tr>
<td>Department of Arts and Culture (DAC)</td>
<td>Records and archives management for government – via the NARSSA, a unit within the DAC</td>
<td>Public Audit Act of 2004</td>
</tr>
<tr>
<td>Auditor General of South Africa</td>
<td>Supreme audit institution within South Africa. Looks at strategic government objectives, programmes and initiatives and responds to identified risks</td>
<td></td>
</tr>
<tr>
<td>National Treasury</td>
<td>Allocation of budget and responsible for public finance management</td>
<td>Framework for managing programme performance information</td>
</tr>
<tr>
<td>Statistics South Africa</td>
<td>Collect statistical data in South Africa</td>
<td>South African statistics quality assurance framework</td>
</tr>
<tr>
<td>The Presidency</td>
<td>Monitoring and evaluation system. Aims to provide for oversight. Monitoring involves collecting, analysing and reporting data on inputs, activities, outputs, outcomes and impacts as well as external factors, in a way that supports effective management</td>
<td>Policy framework for the government-wide monitoring and evaluation system</td>
</tr>
</tbody>
</table>

Table II.
It is apparent from the list in Table II that different entities are tasked with different aspects of IG and there is no single coordinating or oversight entity. For example, the NARSSA is responsible for regulating records management in governmental bodies. In a study by Ngoepe and Keakopa (2011), it was established that the records management function, which is one facet of IG, would have more weight if it is placed either under the oversight of the AGSA or the Office of the President, as opposed to the NARSSA. In the South African e-government strategy, a number of challenges are identified, which are closely related to IG challenges (Department of Telecommunications and Postal Services, 2017), such as:

Lack of synchronisation in approaches to digital transformation adopted by different government departments.

Duplication of processes, databases, large-scale system incompatibilities and inefficiencies as major e-Government hindrances.

Fragmentation of e-government initiatives within government has been identified as one of major challenges. e-government programme has not been directed and managed in a collaborative manner which leads to lack of accountability and responsibility due to the overlapping roles between government departments.

There is no dedicated budget allocation for the specific implementation of e-government in South Africa. A number of initiatives are still run under separate budgets.

Currently, there are still a number of government departments which make use of diverse applications, platforms, software and databases. Most of existing ICT systems were not designed to share information across departments. Cross departmental information sharing is essential to the success of e-government, thus there is a need for government to standardise the interchange requirements for the delivery and management of data.

While IG would have different implications for different sectors, the key elements of the framework remain intact. Governance elements remain the same across sectors, while the nature of the information to be managed will change. With regard to other industries, for example, the health-care sector has long been a global proponent of IG. The health-care sector defined IG in the late 1990s (Donaldson and Walker, 2004). In this regard, many references to IG refer to health-care records as IG. The banking industry has also been identified as a candidate for an IG framework (De Abreu Faria et al., 2013) in which key aspects of IG are noted as:

Information Governance is an emergent concept […] developing and implementing an Information Governance Framework (IGF) is accepted as a natural course of action, though there is no one-size-fits-all solution […] IGF is composed of multiple dimensions.

The dimensions identified align with many of the IG facets included in the IGI facets. However, in the public sector in South Africa, there is no evidence of any government IG framework, although most governments have clearly defined records management and information security frameworks.

6. Proposed national framework for information governance
As reflected in the proposed national framework for IG in Figure 2, the government entities identified have been mapped to the IGI facets to see which organisations are responsible for different facets of IG. The analysis clearly shows that there are multiple entities involved.
The identified IG domains include corporate governance, records management, IT governance, data privacy, knowledge management, master data management, information security and information risk.

As the facets of IG in South Africa are fragmented, a top-down approach to implementation is recommended as opposed to the current one, which does not yield any positive results. Implementation should start at the government level with legislative instruments, support infrastructure and mandate with the president as ultimately accountable. Then it can be cascaded down to the departmental level (ministerial) with a cabinet minister as the accounting officer. Once cascaded down to the organisational level, an IG business unit can be developed to be responsible for organisation-wide implementation. Currently, at most government entities in South Africa, this role is played by the Chief Information Officer who tends to focus more on IT than other facets of IG (Ngoepe and Ngulube, 2013). The key success factors, as identified by Mullon (2017) and Franks (2015), would be executive buy-in, alignment to corporate goals, integrated approach, change management and stakeholder inclusion. In this regard, information is regarded as a business asset.

7. Conclusion and recommendations
As stated in the discussion, IG is a high-level function with different facets that involve stakeholders across the government, each with its own expertise and mandate. There is generally no overarching structure responsible for the overall IG in South Africa as the elements are fragmented in various oversight mechanisms. The negative consequences of fragmentation or silo thinking include duplication of effort and missed opportunities for synergies. As a result, domains compete for limited resources and are “knee-jerk” responses to legislative, legal or risk drivers. As IG is not regulated and modelled at the country level, it is highly unlikely to filter down to organisations. Implementing IG at the country level will go a long way in helping to filter it down to the organisation level.
The study has presented a framework to ensure that IG is implemented at the country level with a single coordinating body established for oversight mechanism. Finally, this study suggests the development of a country think tank on IG, as well as a centralised and coordinated governance structure. The think tank is to investigate the feasibility of establishment of a single coordinating entity for IG at a country level. For example, the information regulator can be assigned a broader scope as opposed to the current narrow scope of privacy and freedom of information, although with limited resources. A further study for assessing IG implementation at organisational level is recommended, as the elements of IG are not grouped together; for example, there are no IG divisions but chief information officers are mostly IT focused and IT driven. Without a proper IG framework at the country level, organisations are open to risks at various stages. It is concluded that failure to transform this pattern would pose a risk to digital transformation as the IG elements would continue to be fragmented.

References


Further reading


About the authors
Paul Anthony Mullon is a PhD Candidate at the University of South Africa in information governance (IG). He is the Founder of a consulting company COR Concepts, which specialises in IG. He is currently serving in the national committee of the South African Society of Archivists (SASA). Mr Mullon was the Chairperson of SASA from 2015 to 2017. He has implemented a number of IG projects in southern Africa. Mr Mullon is involved in a number of committees in South Africa. He is currently the Convener of the working committee for TC171 at the South African Bureau of Standards for the generation of national standards. He is currently serving in Gauteng Provincial Archives Council, which advises the member of the executive committee on issues relating to archives and records management in the province.
Mpho Ngoepe is a Professor in the Department of Information Science at the University of South Africa (Unisa). Prior to his current position at Unisa, Professor Ngoepe has worked for the United Nations Children’s Fund, Auditor-General South Africa and the National Archives of South Africa. He is serving in the national committee of the SASA (2009-2019) and the board of Eastern and Southern Regional Branch of the International Council on Archives (2009-2019) as an Editor of the journals. He also serves on the advisory council of the National Archives of South Africa in his capacity as the Chairperson of Gauteng Provincial Archives. He is the Director of the African team for the multi-national, interdisciplinary research project exploring issues concerning digital records called the International Research on Permanent Authentic Records in Electronic Systems (InterPARES Trust) (2013-2018). Mpho Ngoepe is the corresponding author and can be contacted at: ngoepms@unisa.ac.za

For instructions on how to order reprints of this article, please visit our website: www.emeraldgrouppublishing.com/licensing/reprints.htm
Or contact us for further details: permissions@emeraldinsight.com
Leadership and political will for implementation of the access to information (ATI) Act (2016) in Kenya

Victor Kabata and Francis Garaba
University of Kwa-Zulu Natal, Pietermaritzburg, South Africa

Abstract

Purpose – The purpose of this paper is to demonstrate the importance of leadership and political will towards successful implementation of an access to information (ATI) legislation.

Design/methodology/approach – The paper adopted a mixed methods approach with a bias towards a quantitative survey, complemented by a qualitative follow-up and triangulation during data collection. A complement of theoretical models underpinned the paper, thus enhancing understanding of the multifaceted phenomenon of ATI.

Findings – The paper revealed that the state has demonstrated leadership and political will for ATI by developing government-wide records management manual for public entities; developing an ATI implementation action plan and availing resources for ATI. However, there is need to review laws that perpetuate secrecy; formulate regulations to operationalize the Act and allocate adequate finances for ATI activities.

Research limitations/implications – The paper focused on assessing the extent of leadership and political will on the executive arm of the government excluding the Judiciary and the legislature.

Practical implications – The paper proposes an ATI implementation roadmap, which can be adopted by other countries with comparable contexts.

Social implications – The proposed action plan if adopted will result in an informed citizenry that understands and leverages ATI to claim their socio-economic rights.

Originality/value – The paper provides empirical evidence on some aspects of leadership such as the ministries with ATI policy; level of engagement of policy-makers in ATI matters and the availability of resources for ATI. Further, the paper adopted a multidisciplinary approach by including the concept of ‘meaningful engagement’ whose theoretical foundation is in law to the concept of access to information.

Keywords Regulation, Records management, Legislation, Freedom of information

Paper type Research paper

Background and context

World over, access to information is regarded as a fundamental right that is recognized in international conventions, national constitutions and national laws. Further, access to information laws are anchored on the democratic notion that public bodies hold information, not for their own interests but for public good (Stiglitz, 2002). Consequently, public bodies are expected to provide information to citizens. This information enables the public to meaning-fully participate in public policy formulation and decision-making. ATI laws therefore reinforce the democratic premise that government is meant to serve the people (Odote, 2015).

In the developed world, access to information can be traced back to 1766 when Sweden became the first nation to recognize the right to information by enacting a law allowing the...
press to obtain and publish information held by the state. Other nations followed suit such as Finland in 1951 and the USA in 1966. The period between the fall of the Soviet Union in 1991 and the attack on the World Trade Centre and Pentagon in 2001 was christened as the golden period of openness. Indeed, in that decade alone, 26 countries legislated guarantees for the right of access to government information (Darch and Underwood, 2010). By 2017, 115 out of 195 countries in the world had enshrined the right to free access to information in law and 59 per cent of countries had legal frameworks establishing the right and procedures for public to request and receive government held information.

In Africa, According to the Africa Freedom of Information Centre (AFIC) Report 2017, only 21 out the 54 countries have constitutional, legal and policy guarantees for public access to information. Kenya has recently enacted the Access to Information Act 2016. While passage of the ATI law is a useful step towards enhancing transparency and accountability in the conduct of public affairs, enforcement and implementation of the ATI laws around the world has been challenging particularly in countries with a weak rule of law and poorly capacitated institutions (Neuman and Calland, 2007). One of the factors that influences implementation of ATI laws is aspect of leadership and political will. This study sought to establish the extent of leadership and political will for the implementation of the ATI regime in Kenya.

Theoretical framework
This paper is concerned with assessing the extent of leadership and political will for implementation of the ATI Act 2016 in public bodies in Kenya. This assessment is underpinned by a complement of models and concept. This theoretical triangulation enhances the understanding of the phenomenon of access to information and increases the validity of the findings. Specifically, the main model underpinning this study is the UK, Department of Constitutional Affairs (DCA), Model Action Plan (MAP) (UK, DCA, MAP, 2003) for the implementation of the Freedom of Information Act 2000. The model outlines five areas that are key to implementation of an ATI legislation. These are leadership and policy; training and awareness; information and records management; customers and stakeholders and systems and procedures. This paper will limit itself to the aspect of leadership and policy.

Although the UK, DCA, MAP 2003 provides a framework of the actions that public entities need to undertake to demonstrate leadership and political will for implementation of the ATI legislation, it does not provide a mechanism for assessing the extent of leadership and political will for ATI implementation. To address this concern, this study brought on board the Carter Centre’s, access to information, Implementation Assessment Tool (IAT). The IAT framework consists of functions and elements that assesses the capacity of public entities to perform the three main access to information functions, namely receiving and responding to requests, proactive disclosure of information and records management (Carter Centre, 2014a). These elements are: leadership, rules, systems, resources and monitoring (Carter Centre, 2014b). This paper will limit itself two aspects, that is, leadership and resources.

Although the two aforementioned models adequately address the aspect of leadership and policy which is the subject of this paper, they do not factor in the aspect of political will. To address this concern, this study incorporated the concept of ‘meaningful engagement.’

According to Chenwi and Tissington (2010), ‘meaningful engagement’ takes place when communities and government talk and listen to each other, and try to understand each other’s perspectives towards achieving a particular goal. It is a ‘neutral’ space where people and the state can discuss and shape options and solutions to contentious issues.
Indeed, ‘meaningful engagement’ was first properly defined by the South African Constitutional Court (2008) in the *Olivia Road case*, which dealt with the right to have access to adequate housing for those facing eviction from the rundown buildings in the intercity of Johannesburg (Chenwi and Tissington, 2010). In this case, the court directed the parties to litigation to engage in meaningful dialogue with each other and come up with an amicable and mutually acceptable solution (Orago, 2013).

Accordingly, meaningful engagement seeks to cultivate a culture of dialogue between the state and the citizenry and recognizes access to information as a building block for engagement (Arko-Cobbar and Olivier, 2016). In essence, concept submits that government’s willingness (political will) to provide information to citizens creates a conducive environment for public dialogue between the state and the citizens. Meaningful engagement is, therefore, relevant to this study, as it advocates the need for the government to willingly (political will) provide information to citizens to facilitate dialogue.

The relevance of the concept of meaningful engagement to this study is further underscored by the fact that it has been used in other studies on access to information. For example, Arko-Cobbar and Olivier (2016) used the concept to demonstrate the causal linkage between access to information (ATI) and social economic rights. The authors argued that meaningful engagement facilitates realization of access to information (ATI) and social economic rights (SERs) (Arko-Cobbar and Olivier, 2016).

Further, ‘meaningful engagement’ is relevant particularly when ATI is perceived as a ‘power’ right that has the potential to change relations between different actors providing an opportunity for less powerful actors to engage meaningfully with more powerful actors in their deliberation over political choices that will impact on the former (Calland, 2013).

The relevance of the concept of meaningful engagement to this study is further underscored by the fact that it is anchored on the principles of public participation in governance and decision-making which are predicated on the availability of information and are entrenched in the Constitution of Kenya (2010) (Orago, 2013).

**Literature review**

**Leadership and policy**

ATI implementation entails institutional, legal and cultural changes within the public service. Specifically, effective implementation of an ATI regime requires setting up formal institutions to oversee and enforce the law; enacting laws and policies that promote openness and embedding a paradigm shift from a bureaucratic culture of secrecy to openness. These changes can only be achieved with a solid, focused and sustained political leadership. Some of the actions that demonstrate leadership for ATI include: policy commitment by leaders towards ATI implementation; existence of ‘information champions’ at senior level to drive the ATI agenda and existence of infrastructure (info-structure) that supports implementation of the ATI law.

In the developed world in countries where ATI implementation was guided by a plan of action, the implementation process was coherent, structured and consistent across the public service. For example, in the UK, the government developed the Model Action plan 2003 that guided public entities in implementation of the UK Freedom of Information Act 2000. Although the plan was not mandatory for public entities, it provided a framework for effective implementation of the Act.

Further, the UK government demonstrated leadership for ATI by coming up with a policy that directed all public agencies to nominate senior officers to act as FOI champions and push through its implementation in their respective organizations [United Kingdom (UK) House of Commons, Constitutional affairs Committee first report (2004/2005)].
However, in countries where ATI implementation is not guided by a plan of action, implementation efforts have tended to be disjointed. For example, in South Africa, a report submitted to the African Peer Review Mechanism (APRM) on the progress of the implementation of the South Africa’s Promotion of Access to Information Act (PAIA) 2000 revealed that South Africa lacked an action plan for PAIA implementation. Worse still, there was no dedicated budgetary allocation for ATI programs. As a result, access to information continues to be a challenge in South Africa (Kisoon, 2010).

Under the aspect of leadership, this paper sought to establish two broad issues. First, whether public entities in Kenya had formulated policies necessary for implementation of the ATI Act 2016. Secondly, whether the leadership required to drive these policies was present in public entities in Kenya. The specific questions that this paper seeks to answer under this theme are:

- Is there a formal institutional architecture for ATI?
- Does the Ministry/department’s strategic plan incorporate the aspect of ATI?
- Is there an ATI and records management policy in government ministries/departments?
- Is there an ATI action plan in government ministries/departments?
- Are policy makers in ministries/departments involved in ATI matters?
- Is there top management support for ATI implementation?
- Are resources (physical, personnel and financial) available to facilitate implementation of the ATI legislation?

**Political will**

According to Brinkerhoff (2010), political will refers to the commitment by political leaders and bureaucrats to undertake actions to achieve a set of objectives and to sustain the costs of those actions over time. Undoubtedly, political will is a key ingredient to successful implementation of ATI legislation. Indeed, there is broad consensus among ATI scholars that successful implementation of ATI legislation requires strong political will (Dokeniya, 2013; Neuman and Calland, 2007; Mutula, 2006).

In the developing world, political will for ATI varies in different countries. For instance, in the UK, political will for implementation of the Freedom of Information (FOI) Act 2000 was very pronounced. In particular, preparation for the implementation of the FOI Act 2000 was spearheaded from the highest political level with the Department of Constitutional Affairs (DCA) (Ministry of Justice) being responsible for the operationalization of the Act. Similarly, India and Mexico demonstrated political will for ATI by setting up designated departments within government as focal points for ATI implementation (Dokeniya, 2013).

On the contrary, in Romania, the law 544 on access to public information lacks a provision for an independent oversight body. Instead, a general secretariat within government is mandated to undertake the oversight role. Worse still, the secretariat is underfunded. This arrangement demonstrates lack of political will and has stifled implementation of the law (Dokeniya, 2013). But it is not only in Romania where political will for ATI was lacking, in the larger Eastern Europe, civil society played a key role advocating for the right to information which had been stifled by the authoritarian communist regime (FOIAnet, 2013).

In Africa, because of weak governance systems in many countries, there is limited political will for ATI implementation. In Uganda, for example, the Access to Information
Act (ATIA) 2005 has not provided for an independent oversight body. Instead, an executive oversight body was established but staffed with partisan individuals and without meaningful budget allocated for its operations. As a result, there is an implementation gap and suspicion in the system with citizens, the media and NGOs resorting to private connections to access public information (Dokeniya, 2013).

Similarly, in South Africa, Dimba (2009) noted that there was no sense of political leadership on the compliance with and implementation of South Africa’s Promotion of Access to Information Act (PAIA) 2000. Indeed, Dimba (2009) noted that between the year 2000 and 2003 hardly any money was allocated for official public awareness campaigns on ATI. Furthermore, Kison (2010) noted that although the South African Human Rights Commission (SAHRC) is mandated by South Africa’s PAIA 2000 to oversee and enforce the Act, it is ill-funded thus undermining its effectiveness.

Notably, to counter the limited political will for ATI in Sub-Saharan Africa, civil society activism for ATI is pronounced in countries such as Uganda, Kenya, Botswana and Mozambique. Indeed, civil society organizations initiated and drafted ATI Bills in these countries. Currently, civil society activism for ATI has gained visibility in Africa particularly with the formation of the African Freedom of Information Centre, a Pan-African civil society organization that brings together civil society groups. However, the restrictive environment for civil society operation in many African countries continues to be a challenge (FOIA.net, 2013).

In Kenya, lack of political will was very much pronounced during the decade-long process of enactment of the ATI Act 2016. Indeed, only one out of the four ATI drafts bills that were presented to parliament for debate were government sponsored indicating government’s unwillingness to facilitate access to information (Article 19-Eastern Africa, 2015). Although ultimately, parliament passed the ATI bill 2016, it is worth noting that the enactment of the ATI Act 2016 was largely a civil society-driven process culminating into a private members bill in August 2016. Further, enactment of the ATI Act was largely driven by the need to adhere to constitutional timelines. Specifically, the Constitution of Kenya 2010 had stipulated that the ATI Act had to be passed within five years of the promulgation of the constitution.

Against this background, any meaningful discussion regarding effective implementation of the ATI Act 2016 in Kenya has to factor in the aspect of political will. Brinkerhoff (2010) submits that it is difficult to accurately and objectively assess political will, as it entails ‘intent’ and ‘motivation’ which are intangible and are prone to manipulation and misrepresentation. However, Malena (2009) argues that there are certain indicators that demonstrate government willingness to support a given agenda. These are:

- efforts by the state to initiate or actively support ATI legislation implementation;
- efforts made by the state to introduce legal and regulatory reforms to facilitate institutionalization of an ATI regime;
- efforts made by the state to create platforms and administrative mechanisms that facilitate citizen access to government information;
- efforts made by the state to allocate adequate resources for ATI implementation; and
- efforts made by the state to mobilize stakeholders in support of implementation of an ATI regime (Malena, 2009).

This paper sought to establish whether the aforementioned indicators of political will for ATI implementation were present in Kenya. However, it is important to mention that as far
as implementation of ATI is concerned, the concepts of leadership and political will are intertwined. Indeed, most of the indicators of political will are the same factors that demonstrate leadership for ATI implementation. As such, these two aspects were discussed under the same sub-themes.

Research methods and research site
The study adopted the survey research design using mixed methods approach. Notably, the purpose of the current study is descriptive and explanatory meaning that the study sought to report on the extent of leadership and political will for the implementation of the ATI legislation and where necessary provide explanations (Neuman, 2014). In this case, adoption of a mixed methods approach enabled the researcher to achieve this purpose. First, this was done through a quantitative survey that addressed questions of (what and how many) and second through qualitative interviews and documents review that provided explanation of the first quantitative results. Indeed, Ngulube et al. (2015) observed that mixed methods research provides the possibility for researchers to obtain a comprehensive picture of a phenomenon under investigation and achieve their research purpose effectively.

In essence, the researcher was guided by a quantitative dominant strand that was complemented by a qualitative follow up and triangulation during data collection. In particular, mixing occurred during data collection particularly when the researcher was collecting the second set of data. In this case, the researcher connected the two strands by using the results of the first quantitative strand to build to the collection of the qualitative data. In essence, the quantitative results shaped the collection of qualitative data by guiding the researcher in refining the qualitative data collection protocols and selecting participants that were best fit to clarify the unclear quantitative results (Creswell, 2007, p. 67).

Primary data was collected using questionnaires, interview schedule and an observation checklist. Secondary data was gathered through document review. Specifically, literature in books, journal articles, conference proceedings, policy documents, legislations and reports was reviewed. The first quantitative phase of the study entailed administering of questionnaires to Public Communication Officers who are involved in handling of ATI requests. Questionnaires were also administered to records managers in government ministries to collect their views on leadership and policy for records management. Subsequently, semi-structured interviews were administered to Directors of Administration and key informants such as Director of Public Communication; Director, National Archives and the Ombudsman. The interviews assisted in clarifying and explaining the initial quantitative survey. An observation checklist was used to verify data obtained from the questionnaire by taking note of the available ATI and records management policy documents, ATI infrastructure among other aspects in government ministries.

The survey was conducted in the 22 Ministries that make up the public sector in Kenya. A census approach was adopted where all the units of analysis were studied. The target population was 193 purposively sampled respondents who were distributed as follows; 42 Directors of Administration, 22 heads of records, 84 registry clerks, 42 Public Communication Officers, Key informants such as The Director National Archives, The Director of Public Communication, the Director of Administration and the Ombudsman were purposively selected, as they were considered information rich and key in ensuring the objectives of the study were fulfilled.

The staff establishment of every ministry as well as the list of all ministries acted as the sampling frame (Kenya, 2016, executive order). Before the actual data collection, three ministries were surveyed to pre-test the questionnaires and the observation checklist to ensure their reliability and validity. Quantitative data was analyzed using Statistical
Findings and discussion

Existence of formal institutional architecture for ATI

According to Martini and Transparency International (2014), a formal institutional architecture is important for effective implementation of an ATI law and allows citizens to easily access information. The institutional architecture includes the establishment of oversight bodies and other agencies within the public administration that support the proactive and reactive disclosure of information.

In Kenya, leadership and political will for ATI implementation was first demonstrated by the allocation ATI functions to the Commission on Administrative Justice (CAJ) as stipulated in the ATI Act 2016. The Commission is an independent body headed by the Ombudsman and is spearheading the implementation of the ATI Act 2016. Specifically, the Commission is charged with the responsibility of overseeing and enforcing the Act; facilitating public education awareness on ATI; auditing public entities compliance with the Act; liaising with other public entities to promote the right to access to information; hearing and determining complaints and reviewing decisions arising from violations of the right to information among other functions (Kenya, 2016, ATI Act).

Further, international access to information best practices dictate that nations that wish to effectively implement ATI laws should establish ATI implementation units in each public entity. These ATI units assist in coordination of ATI activities in specific agencies. In Kenya, the findings of the present study revealed that the government and in particular the Ministry of Information and Communication Technology was yet to guide other ministries in setting up ATI implementation units. As a result, ATI activities in the ministries were uncoordinated, thus compromising effective implementation of the Act. The absence of ATI implementation units signifies poor leadership by the Ministry of Information and Communication Technology in terms of prioritizing the ATI agenda.

Pronouncements in support of ATI by public officials and in government policy documents

The UK, DCA, MAP 2003 and the Carter Centre’s, access to information, Implementation Assessment Tool (IAT) that underpin this study submit that one way public entities can demonstrate leadership and commitment to implement ATI law is through pronouncements in support of openness in government policy documents and plans. The study revealed that a sample of 18 out of 26 (69.2 per cent) respondents indicated that their ministries had incorporated the aspect of ATI in their strategic plans. In support of this finding, one of the Directors of Administration noted:

Our Ministry’s strategic plan recognises ATI in line with Article 35 of the Constitution of Kenya 2010. In fact, we are in the process of reviewing our strategic plan and the aspect of ATI will feature prominently.

Similarly, an analysis of government documents revealed that the government has clearly stated its commitment to openness through pronouncements made in national strategic plans. For example, Kenya’s economic blueprint ‘Vision 2030’ recognizes the importance of information access and provision for the realization of the vision. Specifically, the Vision states that Kenya endeavors to create an accountable system that is open, transparent and one that permits free flow of information (Kenya, 2007, Vision 2030).

The commitment of Kenya’s leadership to openness is also demonstrated by the fact that the country is a member of the Open Government Partnership (OGP) forum. This
partnership consists of a community of 70 countries where governments, civil society and
the private sector engage in actions that enhance openness and accountability in public
affairs. In 2016, the Kenyan government demonstrated its political will for openness by
renewing its commitment to Open Government Partnership by submitting its second
national action plan within the framework of OGP. The plan outlined eight smart
commitments that focused on legislative openness, beneficial ownership, access to
information and records management, extractive sector transparency, budget transparency,
open contracting, anti-corruption and climate resilience (Kyalo and Singoei, 2016).

Political will for ATI was also demonstrated recently in June 2018 when the President
issued an executive order directing all public entities to publish details of procurement of
government goods and services.

Existence of an ATI and records management policy in government ministries/departments
Effective implementation and sustainability of an ATI regime is dependent on the existence
of an enabling policy framework. This view is reinforced by the Carter Centre’s, access to
information, Implementation Assessment Tool (IAT) and the UK, DCA, MAP 2003 which
recommend that public entities intending to implement ATI laws should have an ATI
policy. Specifically, the policy should provide for among other things; establishment of an
access to information implementation unit; appointment of ‘information champions’ and a
project team in each public entity to spearhead ATI implementation.

Although initially a sample of 14 out of 26 (53.8 per cent) of the respondents reported that
their ministries had an ATI policy, they could not produce copies of the policy when
challenged to do so. As such, it is right to argue that ministries/departments lacked policies
for implementation of the ATI Act 2016. The lack of ATI policies was attributed to delay by
the Ministry of Information Communication and Technology in formulating a government-
wide ATI policy for adoption by other ministries. In support of this finding, the Director of
Administration at the Ministry of Information and Communication Technology noted, “Our
Ministry is in the process of formulating a national ATI policy”.

Indeed, the absence of an ATI policy framework at national level has created a chaotic and
inconsistent information regime where public entities disseminate public information
haphazardly. The delay in formulation of the ATI policy, two years after the enactment of
the ATI Act 2016, signifies lack of leadership and commitment towards openness.

Further, 14 out of 26 (53.8 per cent) of the respondents indicated that senior of-
ficers in their ministries were not involved in the creation, review and adoption of ATI policy. Worse
still, in the ministries where senior officials were involved in ATI policy matters; the study
revealed that their level of engagement of was minimal. Seemingly, in the absence of a
government-wide ATI policy, policy-makers in ministries were unaware of their ATI duties,
hence the minimal level of engagement.

According to Mutula and Wamukoya (2009), there exists an inextricable link between
access to information legislation and sound records management. Indeed, the success of an
access law rests firmly on the ability of governments to create and maintain records and
citizens’ ability to seek out and obtain reliable, trustworthy and accurate government
records (Millar, 2003, p. 1). In view of this, this study sought to establish the extent of
leadership in management of records in government ministries. The study revealed weak
leadership in terms of records management in the public sector. In particular, the study
revealed that the existing national records management policy has been in draft format
since 2009. Consequently, there is no elaborate policy framework to guide individual
ministries in developing agency-specific records management policies. This finding was
reinforced by the revelation that more than half of the ministries lacked records
management policies. The absence of agency-specific records management policies undermines sound creation, access and retrieval of records. This impedes effective implementation of the access law.

However, on a positive note, the study established that more than half of the ministries had developed agency-specific records management manuals. This finding was reinforced by the presence of a government-wide record manual that outlined procedures for managing records across the public sector and guided ministries in developing agency specific records manuals.

**Existence of an ATI action plan in government ministries/departments**

The UK, DCA, MAP 2003 that underpinned this study recommends that public entities should formulate ATI action plans that identify important milestones towards effective preparation for ATI implementation and set out dates for their achievement. The study revealed that all ministries lacked written ATI action plans. The absence of ATI action plan means ATI activities in ministries were uncoordinated and devoid of sound leadership. It would appear that in the absence of a national ATI policy, ministries were unaware of their ATI responsibilities as well as the activities associated with ATI implementation. The absence of ATI action plan indicates lack of leadership by policy makers in ministries in driving the ATI agenda.

However, at national level, the study revealed that the Ombudsman has demonstrated leadership by developing a national action plan for implementation of the ATI Act 2016. The plan outlines among other things; the activities to be undertaken to promote the implementation of the ATI Act 2016; the timelines within which these activities will be undertaken and the agencies involved. It is expected that ministries/departments will use this action plan as a guide to develop agency-specific action plans.

The Ombudsman has also demonstrated leadership by developing an ATI performance management framework that assesses public entities compliance with the requirements of the ATI Act 2016. One of the requirements of the performance management framework is that public entities should submit an approved annual implementation plan detailing the initiatives they are taking towards implementing ATI Act 2016.

**Top management support in ATI implementation**

The clearest signal of political will for ATI implementation is unequivocal commitment and support by top management towards openness. The study revealed that a sample of 16 out of 26 (61.5 per cent) respondents indicated that their ministries top managers supported ATI. Although managers offered support as indicated by the findings, this support was limited to advice on the handling of difficult requests and was only offered during emergencies. Accordingly, the fact that top managers were only consulted during emergencies suggests weak leadership for ATI implementation. Indeed, global best practices on ATI implementation demand that top management should support the whole process of ATI implementation.

**Availability of resources physical resources to facilitate implementation of the ATI legislation**

The Carter Centre’s Implementation Assessment Tool (IAT) that provided the mechanism for undertaking this study recommends that public entities should have resources (physical, human and financial) for receiving and responding to ATI requests as well as for proactive disclosure. The responsibility of ensuring that the requisite resources for ATI implementation are available lies with the leader of a public entity.
Table I below illustrates the availability of equipment for ATI implementation in government ministries.

Table I above indicates that a sample of 17 out of 26 (65.4 per cent) respondents reported that their ministries had regular access to necessary equipment for ATI implementation.

Further, the study revealed that computers with internet capacity, photocopier machines and scanners respectively were the most readily available equipment for ATI implementation in government ministries.

Table II below illustrates the specific equipment available in government ministries.

The availability of ATI equipment is attributed to the fact that the Kenyan government has increasingly embraced e-government to improve service delivery. Indeed, Ambira (2016)’s study noted that utilization of e-government in Kenya had grown significantly and more ministries were adopting e-government services. The availability of physical equipment demonstrates a leadership that is committed and willing to implement the ATI Act 2016.

Notably, following the inclusion of ATI as a performance target in the performance management guidelines in July 2017, public entities are expected to report on the establishment of ATI infrastructure. Specifically, public entities are expected to submit a report to the Ombudsman providing details of their institutional website as well as ATI links and portals.

**Availability of physical and virtual space**

The leadership of a public entity is expected to provide physical space where citizens requesting information can be assisted. Likewise, public entities are also expected to have virtual spaces where citizens can access information online.

The study revealed that a sample of 15 out of 26 (57.7 per cent) respondents indicated that their ministries had physical space for receiving and responding to requests. However, observation by the researcher revealed that none of the ministries had clearly marked and designated offices for ATI. Instead, the first point of contact for receiving ATI requests was the customer care desk. The absence of dedicated space for handling ATI requests signified

<table>
<thead>
<tr>
<th>Public officers responsible for ATI functions and duties with regular access to necessary equipment (n = 26)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequency (%)</td>
</tr>
<tr>
<td>Yes</td>
</tr>
<tr>
<td>Has access but not regular</td>
</tr>
<tr>
<td>Has no access</td>
</tr>
<tr>
<td>Total</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Specific physical equipment available for ATI function (n = 26)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequency (%)</td>
</tr>
<tr>
<td>Computers with internet</td>
</tr>
<tr>
<td>Scanners</td>
</tr>
<tr>
<td>Photocopy machines</td>
</tr>
<tr>
<td>Airtime</td>
</tr>
<tr>
<td>Camera</td>
</tr>
<tr>
<td>Photography and vide</td>
</tr>
<tr>
<td>Video camera</td>
</tr>
</tbody>
</table>
weak leadership that was yet to make far-reaching preparations towards implementation of ATI Act 2016.

In terms of availability of virtual space, the study revealed that all ministries have websites where information relating to the operations of the ministry is uploaded. Indeed, the Information and Communication Technology Authority (ICTA), an ICT regulatory body in the public sector, compels all ministries to have websites. Additionally, the ICTA has developed technical standards that have to be adhered to by ministries in developing their websites. Accordingly, all the government websites have a search and enquiry feature that allows citizens to make an ATI enquiry and search for information. Indeed, arguably, the government through ICTA has provided the necessary leadership in terms of enabling citizens’ access to information online.

On the availability of space for proactive disclosure, a sample of 15 out of 26 (57.7 per cent) of the respondents reported that their ministries lacked physical space for proactive disclosure. Indeed, observation by the researcher revealed that the government has concentrated its proactive disclosure efforts in print and electronic media. The failure by the leadership to avail adequate physical space for proactive disclosure means that citizens with no access to the internet are disadvantaged in terms of accessing information.

Deployment of specific staff to handle ATI requests
A leadership that is committed to effective implementation of the ATI legislation will deploy expert staff to undertake ATI activities. The study revealed that ministries were yet to deploy specific staff to handle ATI requests. Instead, ATI duties were added to the existing responsibilities of Public Communication officers (PCOs). Although the Act designates the Principal Secretary (PS) in the Ministry as the access to information officer, in most cases these officers are overwhelmed by administrative duties thus forcing them to delegate the ATI responsibility to Public Communications Officers. However, ATI requests that relate to sensitive information are still forwarded to the Principal Secretary as the designated officer under the law.

While assigning ATI duties to PCOs may seem convenient, it is only a short-term solution. It is expected that as citizen’s awareness of ATI Act grows, the demand for information will increase. Accordingly, PCOs will be under pressure to deliver on their main mandate as well as to undertake ATI duties. This pursuit of multiple objectives may result in lack of focus and uncoordinated leadership, thus compromising effective implementation of the ATI Act 2016.

Further, a sample of 14 out of 18 (77.8 per cent) of the respondents revealed that the PCOs deployed to handle ATI requests were inadequate. This finding was confirmed by the Director of Public Communication who noted, “Our staff capacity is inadequate owing to natural attrition and failure to replace the departed staff due to government moratorium on fresh recruitment”.

The failure to commit sufficient staff to undertake ATI activities indicates a weak leadership that has only taken short-term measures towards ATI implementation.

Appointment of officer to undertake proactive disclosure
The study revealed that respondents had varying views regarding the appointment of officers to undertake proactive disclosure.

Table III below indicates that a sample of 12 out of 26 (46.2 per cent) of the respondents indicated that in their ministries specific officers had been formally tasked to undertake proactive disclosure. This finding was confirmed by one of the Director of Administration
who noted, “Proactive disclosure duties are undertaken by staff in the publicity department”. Formal tasking of staff compels them to take their responsibilities seriously since they know they will be held to account. This enhances sound leadership for ATI.

On the other hand, Table III below indicates that a sample of 3 out of 26 (11.5 per cent) of the respondents reported that staff undertaking proactive disclosure were informally tasked. This finding contradicts the requirements of the Carter Center’s IAT tool that recommends that staff undertaking proactive disclosure duties be formally appointed. It would appear that this finding is alluding to staff undertaking proactive disclosure in the course of their regular duties. For example, ICT officers update government websites and in so doing provide updated information though they are not formally tasked to do so.

Finally, Table III above indicates that a sample of 11 out of 26 (42.3 per cent) of the respondents reported that there was no specific tasking for officers undertaking proactive disclosure in their ministries. The absence of formal tasking for proactive disclosure means there is uncoordinated approach towards proactive disclosure. This undermines effective implementation of ATI.

Funds allocated for ATI activities
Another aspect of leadership relates to commitment of sufficient funds for ATI implementation. This entails having a dedicated budget for ATI activities at agency level as well as allocating adequate funds to the oversight body.

The study revealed that ministries lacked dedicated budget for ATI activities. In support of this finding, the Ombudsman noted, “Most public entities have not set aside resources for ATI as they consider it burdensome and have relegated it to the periphery”. Seemingly, although the government had made pronouncements in support of ATI in its policy documents, these pronouncements are not accompanied by necessary resources thus indicating lack of political will towards implementation of ATI. Brinkerhoff (2010) noted that dedicated public spending is a tangible expression of prioritised political intent.

Similarly, the study revealed that the Commission on Administrative Justice (CAJ) lacked adequate funds to oversee and enforce implementation of the ATI Act 2016. The Ombudsman explained that that part of the challenge in implementing the ATI Act 2016 was attributed to government’s budget cycles. Specifically, the fact that the Act came into force in the first quarter of the financial year long after the government budget had been prepared. This meant that the commission had to wait for next financial year to present its budget for ATI implementation. Although, the National Treasury has approved the Commission’s current 2018/2019 budget, the Ombudsman explained, “We have to commit the funds immediately lest they fall prey to budgetary cuts as is common practice”.

In the absence of adequate funding from the exchequer, the Commission has demonstrated leadership by lobbying donors to support ATI programs.

Table III.

<table>
<thead>
<tr>
<th>One or more public official tasked/appointed responsible for proactive disclosure functions and duties (n = 26)</th>
<th>Frequency</th>
<th>(%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Formally tasked</td>
<td>12</td>
<td>46.2</td>
</tr>
<tr>
<td>Informally tasked</td>
<td>3</td>
<td>11.5</td>
</tr>
<tr>
<td>No specific tasking</td>
<td>11</td>
<td>42.3</td>
</tr>
<tr>
<td>Total</td>
<td>26</td>
<td>100</td>
</tr>
</tbody>
</table>
Efforts made by the state to introduce legal and regulatory reforms to facilitate institutionalization of an ATI regime

The concept of meaningful engagement that underpins this study submits that for there to be meaningful dialogue between the state and the citizenry, there has to be a conducive environment and in particular a supportive legal and regulatory framework. Indeed, effective implementation of ATI legislation is anchored on the existence of a supportive legal and regulatory framework.

The study revealed that the government was yet to create a fully conducive legal and regulatory framework to facilitate implementation of the ATI Act 2016. This is demonstrated by the absence of regulations to operationalize the ATI Act 2016 and the presence of laws that perpetuate secrecy in Kenya’s statutes. Some of the laws that undermine access to information include the Official Secrets Act, the Preservation of Public Security Act, the National Assembly Powers and Privileges Act among others. The failure by the Ministry of ICT to formulate regulations two years after enactment of the Act demonstrates poor leadership and lack of political will to operationalize the Act.

Although Kenya has ratified international laws and covenants committing itself to international best practices on access to information, the study revealed a lack of political will in adherence to the requirements of international and regional instruments that protect the right to information. For example, Kenya is yet to submit one report to the African Charter on Human and People’s Rights (ACHPR). Further, Kenya has only ratified four out of the six African treaties that recognize the right to information. Specifically, Kenya is yet to ratify the African Union Convention on Preventing and Combating Corruption as well as the African Charter on Democracy Elections and Governance (AFIC, 2017).

However, the executive has demonstrated considerable political will particularly towards proactive disclosure. For instance, in June 2018, the president issued an executive order directing all government institutions to begin publishing full details of tenders and awards on the 15th of every month beginning July 2018. Specifically, public entities are required to publish information on goods and services purchased, contract prices, and the particulars of the suppliers including owners, directors and beneficial ownership of the companies (Kenya, 2018, Executive Order No. 2).

Moreover, the Ombudsman has also demonstrated leadership by drafting instructions guiding public entities on the implementation of the ATI Act 2016. The instructions require public entities to among other things:

- proactively disclose information in their custody;
- publish the name or names of Information Access officers;
- process the applications for access to information held by them within the set timelines at a reasonable cost;
- keep and maintain accurate, authentic and credible records;
- computerize their records and information management systems within three years since the commencement of the Act on or before September 21st, 2019; and
- submit a report to the Commission on implementation of the Act by June 30th every year or at any time required by the Commission (Commission of Administrative Justice, Circular 2018).

Further, the Ombudsman has developed several policy guidelines aimed at facilitating implementation of the ATI Act 2016. These include a hand book to guide public entities on the implementation of the ATI law, a guideline on proactive disclosure for public entities as well as a simplified version of the ATI Act 2016 to ease citizens understanding of the Act.
The formulation of guidelines for use by public entities ensures there is a coordinated and standardized approach towards ATI implementation across the public sector.

In terms of records management, the study revealed that the state had demonstrated political will by initiating the process of review of the Public Archives and Documentation Service Act to align it with the ATI Act 2016. Specifically, the Director, Kenya National Archives revealed, “We are in the process of amending the Archives legislation to align it with provisions of the ATI Act”. In particular, he noted, “The Act has been gazetted by parliament for amendment and the public have been invited to submit their views as required by the Constitution of Kenya 2010”.

Although considerable efforts have been made in formulating guidelines to facilitate the implementation of the ATI Act, the delay in reviewing laws that are inimical to openness demonstrates lack of political will towards ensuring citizens access to information.

Efforts made by the state to create platforms and administrative mechanisms that facilitate citizen access to government information

The ‘concept of meaningful engagement’ that underpinned this study submits that the state should undertake measures that promote sharing of information with the citizenry. One way of demonstrating political will for ATI implementation is creating platforms that facilitate engagement and consultation between the state and citizens. The study revealed that the government had undertaken several administrative measures that enhanced citizen access to information. Key among them is the establishment of platforms where government information is shared. These platforms include:

- MyGOvt, a weekly newspaper that disseminates information on government achievements, job opportunities in the public sector and available tenders for supply of goods and services in the public sector.
- Social media platforms such as #gokdelivers and #gokinteracts. These platforms disseminate information on government achievements and facilitate interaction between the state and the citizenry.
- An e-citizen portal that allows citizens to access a range of services such as; application for identity card and passport, renewal of driving license, filing of tax returns among other services.
- The public–private partnership disclosure web portal. The portal provides information on key commercial contracts between the government and private investors.

Efforts made by the state to mobilize stakeholders in support of implementation of an ATI regime

Political will for ATI is also manifested by the extent to which government agencies consult, engage and mobilize stakeholders on matters pertaining to implementation of the ATI Act 2016. Although the Ombudsman had made efforts to mobilize ATI stakeholders particularly through convening the ATI stakeholder’s conference, the same cannot be said of the executive. Although the Ministry of Information and Communication Technology is in the process of formulating an ATI policy, there was no evidence to indicate that there was stakeholder engagement in the process thus raising concern whether there was genuine political will.

However, the study established that the government had set up a committee to spearhead the formulation of Data Protection law. This committee is comprised of stakeholders in the
field of information management. The committee has prepared a draft Data Protection Bill 2018 that is currently being debated by parliament.

**Conclusion and recommendations**
The study has revealed that the level leadership and political will for ATI implementation was not at its optimum. To address the situation, the study makes two key recommendations. First, the need for ATI implementation efforts to be anchored on an elaborate legal and regulatory framework. In particular, the government should fast-track formulation of ATI policy and attendant regulations to breathe life to the ATI implementation process. Second, the government should prioritize ATI funding by committing sufficient funds towards the ATI agenda. Overall, the study has demonstrated that implementation of an ATI law is undeniably and unavoidably a political process. Accordingly, the study proposes an ATI implementation roadmap that captures both leadership and political will as key components of an ATI implementation process. This action plan if adopted would facilitate effective implementation of the ATI Act, thus facilitating access to information by citizens. Undeniably, this will positively impact on the society, as an informed citizenry is able to understand and claim their socio-economic rights as well as participate in governance and decision-making, thus resulting in political and socio-economic empowerment.

**References**


Further reading


About the authors
Victor Kabata is a Doctoral student at the University of Kwa Zulu-Natal, Information Studies Programme. This article is revised from a chapter of his thesis titled “Preparedness of public bodies for the implementation of the ATI Act 2016 in Kenya,” under the guidance of Dr Francis Garaba. Victor Kabata is the corresponding author and can be contacted at: kabataukzn@gmail.com

Dr Francis Garaba is a Senior Lecturer at the University of Kwa Zulu-Natal, Information Studies Programme. His main research interest is records and archives management.

For instructions on how to order reprints of this article, please visit our website: www.emeraldgrouppublishing.com/licensing/reprints.htm
Or contact us for further details: permissions@emeraldinsight.com
The impact of new public management through outsourcing on the management of government information

The case of Sweden

Proscovia Svärd

Department of Information Science, University of South Africa, Pretoria, South Africa and Södertörn University College, School of History and Contemporary Studies, Stockholm Sweden

Abstract

Purpose – Using a case study method, the article investigates the impact New Public Management (NPM), through outsourcing has had on the management of government information at the Swedish Transport Agency. In April 2015 the Agency outsourced its IT-operations to IBM company. Some of the IBM subcontractors had not been cleared by the Swedish Security Service. This exposed the Agency’s information to risk. By outsourcing the IT operations, the General Director of the Agency deviated from the laws governing government information such as the Swedish Security Protection Act, the Personal Data Act and the Publicity and Secrecy Act.

Design/methodology/approach – The researcher has applied a case study method as the investigation focuses on a phenomenon in a real-life setting. The case study method entails the use of past studies, which facilitates the exploration and understanding of a complex issue. The phenomenon under investigation is NPM’s impact, through outsourcing, on the management of public information at the Swedish Transportation Agency.

Findings – Outsourcing should be foregone by well-formulated contracts that should put into consideration the management of government information and the involvement of all stakeholders such as records managers/archivists, IT personnel, heads of departments, lawyers and business analysts. Outsourcing risks to compromise the two tenets of democracy that is, accountability and transparency which are central to Swedish public administrations’ operations.

Research limitations/implications – The study is limited by the fact that it only presents the views of the archivists. This was, however, purposely done because their voice was missing during the discussions that followed after the data breach scandal had become public knowledge. Additionally, archivists are supposed to play a major role in the management of government information at Swedish institutions. Further research that will involve different categories of employees might give a deeper and better understanding of the impact that NPM, through outsourcing, is having on the management of government information and what implications this might have on issues of trust, transparency and accountability.

Practical implications – The study demonstrates the need for well-formulated outsourcing contracts that will include information management clauses. It is of crucial importance in a democratic society that access to government information is not compromised as institutions endeavor to achieve efficiency and high-quality service delivery.

Social implications – It is government information that gives citizens knowledge about the various processes of government institutions. It is therefore of paramount importance that government information is not left in the hands of unauthorized companies that are involved in the outsourcing activity but should be securely managed and guarded, as the opposite might pose privacy and national security challenges and hence undermine the trust that citizens have in government institutions.
Originality/value – The search that the author conducted confirmed paucity in research that discusses issues related to NPM, outsourcing and the management of government information. This paper is therefore a contribution to the discourse from an archives and information management perspective.

Keywords Outsourcing, New public management, Transparency, Accountability, Government information

Paper type Research paper

Introduction
This article investigates the impact that New Public Management (NPM) through outsourcing has had on the management of government information at the Swedish Transport Agency. It demonstrates the need for well-formulated outsourcing contracts that should properly spell out responsibilities for the management of government information and involve all stakeholders such as: records managers/archivists, IT personnel, heads of departments, lawyers and business analysts. Government administrations are operating in a world of constant technological change and disruptive innovation. This development has brought along great opportunities but also challenges. Organizational environments are more unpredictable and insecure today (OECD, 2017), and this has forced organizations to deploy new management styles to achieve efficiency and flexibility in a world of constant change. The globalization and the pluralization of service provision has required government institutions to collaborate with external partners to meet the citizens’ demands. Globalization and market liberalization increased the criticism toward the old style of management of public administrations and have led to the adoption of private sector practices to the public sector. This resulted in a shift from administration to management and hence, the NPM style. Furthermore, public administrations were not only to be regarded as implementers of rules and laws but organizations that can meaningfully use governments resources to deliver high-quality service (UNDP and Global Centre for Service Public Excellence, 2015).

Therefore, globalization, the free movement of capital, people and competition are the driving forces behind the streamlining of organizational business activities and the focus on core business activities to deliver satisfactory services (Baltic Quality, 2012). Since 1980s, the European Governments have embraced NPM in the quest for efficient institutions and have outsourced government functions to private organizations (Van de Walle and Hammerschmid, 2011). NPM is considered a model that can increase trust in government institutions. It is the introduction of private sector practices into the public sector, strengthening the prerogatives of managers, measuring performance, increasing competitive pressures and cutting costs. Outsourcing is a strategy within NPM and is about the contracting out of a service traditionally delivered by a government organization to a private organization. While it is seen as a means to cut costs and to create efficiencies, it has also been blamed for exacerbating unemployment and is considered a threat to data security, and hence the warning that it should be prudently applied to certain sectors (Tholons, 2010).

In the 1980s, the declining citizens’ trust was identified as the driving force of the changes that government institutions underwent (OECD, 2017). Even today, the public sector is working hard to distance itself from inefficiency, non-transparency and being expensive and is working hard to put the citizens, sometimes referred to as customers, at the centre of its business activities (Svärd, 2014). It continues to implement reforms with the objective of inclusive growth, the delivery of high-quality service to the citizens amidst budgetary constraints (OECD, 2017). Like large organizations, government administrations...
need cost savings and operational efficiencies during the execution of their functions. This is what is driving outsourcing within the public sector (Hood, 1995; Van de Walle and Hammerschmid, 2011). For example, IT outsourcing in Sweden has steadily been growing and is considered the largest in the Nordic region and third largest in Europe. The reasons behind outsourcing include lack of domestic skills, high costs of in-house solutions and the need to refocus on core competencies (Baltic Quality, 2012). Many governments such as the USA, UK, Australia, Japan and Singapore are investing massive amounts of money in outsourcing. Organizations engage in outsourcing with the intent to lower labor intensity and to increase efficiency. Swedish Government institutions are also involved in the outsourcing of some of their functions (UNDP and Global Centre for Service Public Excellence, 2015).

In 2015, it was revealed by Dagens Nyheter, one of the Swedish newspapers, that the Swedish Transport Agency had outsourced government information without prior security clearance of some of the IBM sub-contractors in Eastern Europe by the Swedish Security Service. This led to the breach of the legal framework that governs government information (Swedish Radio, 2018). In the digital age where information is the driver of all government processes and can threaten national security, its effective management is of paramount importance (Ceeney, 2008). Sweden is internationally known for being a transparent country and its Public Access Act is 250 years old (Bohlin, 2010). It further promotes open data initiatives and its institutions are encouraged to proactively publish government data for public access. Swedish public information is further governed by the Archival Law, which dictates the way information generated by public institutions should be managed. Despite the transparency nature of Swedish administrations even though the scandal took place in 2015, it did not become public knowledge until the beginning of 2017. This study investigates the impact NPM through outsourcing has had on the management of government information at the Swedish Transport Agency. It offers an introduction, a method used to examine the case, a literature review, a discussion, conclusion and recommendations.

**The research problem**

Governments have globally undertaken reforms to create more efficient administrations that at a low cost are meant to deliver high-quality services to the citizens. Therefore, in the name of efficiency and cost-savings, government functions are being outsourced within the realm of NPM. This impacts the management of public information, which in today’s environment could violate the personal integrity of the citizens negatively and could also be a threat to national security (Ceeney, 2009). The Swedish National Transport Agency outsourced its information to IBM with sub-contractors in Eastern Europe who had not received security clearance by the Swedish Security Service. Additionally, the General Director of the Agency deviated from the legal framework that governs the management of government information. Information is central to efficient service delivery, and where it is inefficiently managed, public trust and service delivery are affected. Outsourcing should be foregone by well-formulated contracts that will put into consideration the management of government information and the involvement of all stakeholders such as records managers/archivists, IT personnel, heads of departments, lawyers and business analysts (Svärd, 2011; Eriksson, 2014). Outsourcing risks to counteract the two tenets of democracy of accountability and transparency upon which Swedish public administrations operate.

**The method**

The researcher has applied a case study method as the investigation focuses on a phenomenon in a real-life setting (Yazan, 2015). The case study method entails the use of
past studies, which facilitates an exploration and understanding of a complex issue (Zainal, 2007). The phenomenon under investigation is NPM’s impact through outsourcing on the management of public information at the Swedish Transportation Agency. Yin (2009) stated that the case study method enables a researcher to use multiple sources of evidence, and Pickard (2007) argued that a case study should have well-defined boundaries. The case study method therefore enables a researcher to investigate a bounded phenomenon in detail without seeking to generalize the findings. For this study, the researcher carried out a literature review of scientific articles that are relevant to the phenomenon being studied, and other documentary evidence such as newspaper articles, Google Scholar, ScienceDirect and SöderScholar databases have been consulted and search words such as NPM, outsourcing, government organizations and government information were used to access articles relevant to the study. The rubrics under which the literature review is presented were identified in conjunction with the reading that the researcher identified as relevant to the study. The study also draws on the data that the researcher gathered using a group interview with the archivists that oversaw the management of information at the Agency. The archivists were chosen because of their role in the management of information at Swedish administrations and because when the IT and data breach scandal unfolded, their voices were not heard. The discussions that followed in the public sphere focused on information systems and not the information that is maintained in the systems. One of the interviewed archivists had a background in cultural studies and the second one was a historian. They both had a university degree and 40 university points in archives and information science. The archivists will be referred to as A and B. The interview took 1 h 46 min and was recorded and transcribed. It generated data of about 18 single-spaced pages with responses that were deep enough to give an understanding of the issue being researched. It is only data that demonstrate the impact of NPM on the management of government information, which is presented in this paper.

The literature review
The next section presents research that the author identified as relevant to the study. The author does not claim to cover all the work that has been done so far on NPM but cites the studies that give the reader a brief background of NPM and bare relevance to information management in public institutions. The search in the different databases such as Google Scholar, SöderScholar, ScienceDirect and Emerald proved that a very little research has dealt with NPM’s impact on the management of government information.

New public management
Van de Walle and Hammerschmid (2011) carried out an overview of academic evaluation and impact studies of the entire NPM style reform programs and argued that despite the fact that it has been implemented in the European public sector for a period of 30 years, there were very few empirical evaluations of its effects. They distinguished between two sets of NPM style changes and reforms; one that is of specific managerial innovations within public organizations and another that constitutes changes to the role of government and citizens. They concluded that a lot of academic work has focused on the first NPM style, while the second style was only a critical discourse with limited empirical studies. They suggested that evaluations should not only look at specific managerial and operational reforms but also the wider effect that NPM reforms have on the role of the state and on the position of the citizen-client. When Hood (1991) investigated NPM, he concluded that it was the most striking international trend in public administration. He identified elements that constituted NPM as follows:
a shift toward greater disaggregation of public organizations into separately managed corporatized units for each public sector product;

a shift toward greater competition between both public sector organizations and private sector organizations;

a move toward greater use of management practices broadly drawn from the private corporate sector;

a move toward greater stress on discipline and parsimony in resources use and active search for less costly ways to deliver services;

a move toward hands-on management;

a move toward explicit and measurable standards of performance; and

attempts to control public organizations in a more “homeostatic” style according to pre-set output measures (Hood, 1995).

O’Flynn (2007) examined the emergency of NPM approach and contrasted it with a public value paradigm. Her intent was to provide a conceptual discussion of difference in approach and to highlight some practical implications for both the public sector management and managers. She postulated that the post-bureaucratic paradigm of public management reflected reforms that meant a break away from the traditional model of public administration, which was based on Weber’s (1946) bureaucracy, Wilson’s (1887) policy administration divide and Taylor’s (1911) scientific management model of how work was organized. NPM was a reaction to the weaknesses that were identified in the traditional bureaucratic paradigm of public administration. Some of the common practices adopted within the realm of NPM include corporate planning based on central goals, comprehensive program budgeting, management improvement programs, contract employment for managers, central auditing and performance monitoring of individuals. She concluded that the weaknesses in NPM have led to a paradigmatic change in the way the state is looked upon, its purpose, function and management.

Pegnato (2011), who looked at the US federal outsourcing, stated that the proponents of outsourcing were of the view that competition between government employees and the contractors should lead to more efficient government and hence, huge savings for the taxpayers. Outsourcing enabled government to access the latest technologies through its contractors, and that officials were relieved of administrative burdens and could concentrate on core missions and strategic activities. Additionally, goods and services that were not available in the public sector could be found in the private sector. It further enabled federal agencies to avoid certain constraints such as the removal of a poorly performing contractor compared to a removal of a civil servant. However, Mulgan (2015), whose research aimed to establish the current state of evidence on transparency of the performance of outsourced government services, argued that outsourcing does not necessarily reduce government spending. He contended that transparency is needed to ensure that contractors do not hide problems and to allow public scrutiny. Transparency promotes efficiency and government performance. The empirical evidence for the cost savings has therefore been challenged, and there are concerns that outsourcing poses threats to the democratic values of transparency and accountability. As the focus of this article is the impact that NPM through outsourcing has had on the management of government information at the Swedish Transport Agency, the next section presents literature on the theme.
Information management and outsourcing

Leming (2015) argued that despite the fact that information is regarded as an important asset, it rarely appears in the definition of asset management. He asserted that information management should be a central function subject to controls and should have resources for its management in the same manner as other functions do. He further asserted that records management, information security, business continuity and data management disciplines should collaborate and coordinate to ensure that the confidentiality, integrity, availability and disposition of data and content are well managed throughout the information continuum. The information management function should have a defined network of local champions and experts to work for its integration in all the business activities. He argued that this was critical to information asset management and risk mitigation. The current environment which involves outsourcing of government information clearly requires collaboration of the different stakeholders to mitigate risks as public organizations are operating in a constantly changing and challenging environment. This is an environment with digital processes and data, staff changes, new ways of working, office relocations, the Freedom of Information Act, open data initiatives, the management of sensitive and confidential information and sometimes outdated processes (Iron Mountain, 2015).

Muid (1994) argued that though NPM reforms and informatization were presenting opportunities for the re-engineering of government business activities, more awareness and debate were needed to understand the implications the two trends have had on the stewardship of government information. He was of the view that public service reforms that led to both fragmentation and the contract culture impacted the development and implementation of information systems. He highlighted issues such as the privacy of the individual, the protection of public interest and the fact that public officials should be competent in the management and use of information that they hold in trust. Mulgan (2015) argued that public sector information is recognized as a common resource, and hence, the transparency of information about expenditure and performance of contracts for government-funded services ensures that government funds are well spent.

Klareld (2016) explored the consequences of an outsourcing policy on the management of information generated at the Swedish Transport Administration. Using interviews, she focused on the issues that were identified by the employees of the administration as important during the outsourcing act. The issues included information governance and ownership; roles and responsibilities in records management; the business systems in which records are created and managed; the legal requirements of public agencies; knowledge transfer about records management requirements; and defining organizational boundaries. She concluded that outsourcing poses challenges, and therefore, existing practices need to be revisited if the Agency was to meet with its business needs and citizens’ expectations and to comply with the legal framework that governs government information.

One of the conclusions the author drew from her PhD research on the management of information amidst e-government development was that, despite the stringent legal framework that governs government information in Swedish local administrations, some knowledge about how effective information management should be achieved and the deployment of information systems, there were still challenges in the management of government information. This conclusion could be applied to the state agencies. The author worked at a state agency and saw how difficult it was to implement effective information management and to secure top management support that was needed to align information management requirements with the business processes (Svärd, 2011). In one of the studies that were part of the author’s licentiate research, a respondent argued that even though they were soon to outsource part of their health service process to a private sector, the
management showed very little interest in how the records and the metadata catalogue issues were to be solved. Yet, this concerned about 3,000 employees. Additionally, the results from this research also showed that The Archival Law that regulates the management of government information in Swedish administrations in a majority of cases was only known by archivists and that the training of officers in records management was very minimal (Svård, 2011).

It is stated in a guideline published by the Public Record Office Victoria (Public Record Office Victoria, 2010) that as the requirement of the legislation governing government information does not extend to outsourced organizations, it is important that adequate records management planning is undertaken before outsourcing any government service. Contracting managers should include records management clauses when drafting outsourcing contracts. The clauses are meant to ensure the following:

- The ownership of records developed and maintained by outsourced organizations is clear;
- All records are appropriately created, maintained and controlled in accordance with agency requirements
- Accurate information is stored within the records;
- Access to records is appropriately regulated and controlled;
- Records are appropriately stored;
- Records are only disposed of in accordance with contractual requirements; and
- Sub-contracts with any third parties mirror the agency's records management requirements.

Lack of inclusion of records management clauses in outsourcing contracts is likely to expose an agency to risks such as:

- the inability of the agency to meet their legislative obligations (e.g. the provision of records under the Privacy and Data Protection Act 2014 or Health Records Act 2001);
- poor decision-making because of incomplete or inaccurate information;
- loss of personal information/personal history of members of the community;
- unsatisfactory service provision to clients;
- exposure to public and regulator criticism for the failure to adequately manage public records;
- loss of public accountability and transparency;
- loss of the State’s history; and
- increased legal liability.

Scholl (2006) carried out a study entitled “Electronic government, information management capacity organizational capabilities and the sourcing” and established that e-government sourcing mixes impact governments’ information management and organization capabilities. He highlighted the need to understand e-government related sourcing and its integration with traditional public management information systems. According to an overview of Swedish outsourcing done by Lindqvist (2018), all outsourcing of business must adhere to the provisions of Directive 95/46/EC on data protection, and from May 2018, it should be made in accordance with the new Regulation (EU) 679/2016 General Data Protection Regulation (GDPR).
The literature reviewed above confirms that there are advantages with NPM, but there is still lack of empirical evidence on the wider effect that NPM reforms have on the role of the state and on the position of the citizen-client, and the advantages of outsourcing are challenged too. NPM is meant to create more efficient public administrations but more research needs to be undertaken to analyze in broader terms its impact on the management of public administrations. The literature review further demonstrates the need for well-formulated outsourcing contracts that should ensure that government information is efficiently and securely managed not to compromise the two tenets of democracy, which are accountability and transparency and additionally national security. The section that follows presents the research findings.

**The research findings**

This section presents the Swedish Transport Agency, the information management environment, a chronology of events prior to the IT and data breach scandal and the findings based on the group interview the author carried out with two archivists that work at the Agency.

*The Swedish Transport Agency*

The Swedish Transport Agency has the overall responsibility for the Swedish transport infrastructure and draws regulations that govern it. It further ensures that the society at large follows the regulations. It is a member of the European Car and Driving License Information System (EUCARIS). This is a continent-wide collaboration of national agencies with a mission to facilitate data exchanges on vehicle registration, driving licenses, traffic and parking violations and accompanying personal data. EUCARIS uses a closed and encrypted EU network for the cross-border transfer of data between individual states. The partners in the EUCARIS collaboration must ensure the secure storage and legitimate use of the transferred data. Compliance with EU data protection regulations is a condition of EUCARIS’s membership. As such, it is an important institution (ITS International, 2017).

The organizational chart shows what constitutes the transport infrastructure activities, driving licenses, civil aviation and maritime, vehicle information, road and rail and strategic development and management and the departments that support the activities (Figure 1).

*The data breach scandal*

In April 2015, the Swedish Transport Agency contracted IBM to manage its IT operations. IBM had personnel from its sub-contractors in the Czech Republic, Romania, Croatia and Serbia. These IBM sub-contractors had not been cleared by the Swedish Security Service (SAPO). When the General Director of the Agency outsourced the IT operations to IBM, she deviated from the laws governing government information, which included; the Security Act, the Personal Data Act, the Publicity and Privacy Act and the authority’s own guidelines for information security requirements. On November 25, 2015, the Agency’s IT security unit and the Swedish Security Service warned the Agency and urged it to stop the contract in vain (Nilsson and Nilsson, 2017). The Agency outsourced the maintenance of its firewalls, networks and databases with information about all vehicles in Sweden, information on police and military vehicles, people with protected identities, the routes of armoured vehicles which transport large sums of money, information about the weight capacity of roads and bridges, personal details of fighter pilots, police force members, members of the Swedish military (the most secret unit), information on people in Sweden’s witness protection program, information on criminal suspects and encrypted communications system used by Swedish authorities (Krug, 2017; Warwick, 2017) (Table I).
Figure 1. 
Organizational chart for the Swedish transport agency


Table I. 
Chronology of events that led to the IT scandal at the Swedish Transport Agency

<table>
<thead>
<tr>
<th>Date</th>
<th>Happening</th>
</tr>
</thead>
<tbody>
<tr>
<td>April 2015</td>
<td>The transport agency signed an agreement with IBM Sweden to operate the authority’s IT system (outsourcing). The agreement meant that IBM Sweden was responsible for the hardware, networking and the functioning of applications. The agreement is valid until October 31, 2020 with the possibility of extension. In connection with the outsourcing, during the first half of 2015, the Director General, Maria Ågren decided to deviate from the Security Act, the Personal Data Act, the Publicity and Privacy Act as well as the authority’s own guidelines for information security requirements.</td>
</tr>
<tr>
<td>Latter part of 2015</td>
<td>In the latter part of 2015, SAPO carried out an oversight of the authority’s security protection. The SAPO finished its work on the June 16, 2017.</td>
</tr>
<tr>
<td>January 2016</td>
<td>Prosecutors initiated a preliminary investigation based on the SAPO report.</td>
</tr>
<tr>
<td>January 18, 2017</td>
<td>Maria Ågren resigned from the post of Director General of the Transport Agency.</td>
</tr>
<tr>
<td>January 26, 2017</td>
<td>Maria Ågren received a criminal injunction, which imposes daily fines because of negligence with confidentiality, but without intent.</td>
</tr>
<tr>
<td>August 3, 2017</td>
<td>The transport agency was asked by the government to map what information had been handled by people who had not received security clearance and to assess what measures may be needed to adequately handle the protection of the information in the future. The investigation that was presented on January 23, 2018, showed that the information had been made available to the supplier’s staff and had not been safeguarded according to the Swedish law, but there were no indications that it had ended up in the wrong hands. The government also decided to appoint an independent investigator to investigate the events that led to the outsourcing of sensitive and confidential information in a manner contrary to Swedish legislation.</td>
</tr>
</tbody>
</table>

Source: The Swedish Transport Agency’s website: www.transportstyrelsen.se/sv/Om-transportstyrelsen/fragor-och-svar/, Translated into English by the author
The Swedish Transport Agency Information Management Environment

According to the data collected from the group interview, the organization does not have a pronounced information governance Model but there are, however well-developed routines and guidelines that facilitate the management of information. Knowledge and skills in information management among the employees vary depending on whether people have worked in the public sector. The employees who have worked in the public sector understand why the information they generate needs to be managed according to the legal framework that governs it, while those from the private sector do not. The archivists rely on the National Archives guidelines for the management of electronic information. The Agency had an electronic archive (e-archive), which was a result of a project pursued between 2010 and 2011. The e-archive had a lot of technical problems, and therefore after several internal discussions and investigations, it was shut down in 2013. In 2014, the Agency got involved in the development of an e-archive solution that is currently taking place at the State Service Center (Statens Servicecenter). This development is supposed to result in an e-archive solution for state agencies. The State Service Center is a state owned organization that is charged with the responsibility to promote efficient administration within the state administration.

The State Service Center provides administrative services and consultancy support in accounting, salary management and human resources and is currently working on the development of e-archiving services for government agencies. The Swedish Transport Agency currently has one of its staff members who is an archivist as a participant in the development of a requirement specification for a well functioning e-archive. Since the Agency is not among the pilot agencies, it is still waiting and hoping to be among the first agencies to buy the e-archive solution. The e-archive solution is expected to facilitate the management of the Agency’s information in a co-ordinated manner. Government agencies are expected to buy the e-archive solution from the centre and to use it to archive their information resources. The solution that the State Service Center is to sell to the government agencies will lead the information to what is referred to as a middle archive. This is where all the information from the state agencies will converge but under each respective agency before it is transferred to the National Archive. This will be an effort to create a unified repository for all the state agencies and will serve as some sort of a state cloud. Traditionally, when information was transferred to the National Archives, the entire responsibility for its management was handed over to it by the depositing agency. However, with the State Service Center’s solution, the responsibility for the deposited information will still be with the depositing agency.

Respondent A informed that the same legal framework governing government information will apply to the middle archive. The administration and development work will be shared among all the state agencies to leverage economies of scale and also because developing an e-archive is too expensive for a single agency. This will further facilitate the management of the knowledge that will be accumulated during the development phase as it will be managed in one place, that is, at the center. Respondent B informed that the Agency has a variety of case management systems and databases, and that most information is still maintained in the legacy systems. How all this information will be transferred to the e-archive when it is finally implemented is still a challenge that the Agency will deal with once the e-archive solution has been implemented. The integration of the systems has been identified as a necessity, but without an e-archive, it is difficult to motivate the employees to start planning for the delivery of information to it. Both archivists confirmed that to a certain extent they know what to do to export the metadata from the legacy systems, but they still do not know what tools they will have to apply, and that it is still a difficult situation.
Outsourcing of the Agency’s information
The respondents confirmed that when the outsourcing took place, they were not consulted because it was regarded as an IT issue. When I asked why they never actively tried to involve themselves, they informed that they sent a fellow archivist to engage with the people who were involved in the outsourcing, but he was never given time to ask questions. The timeframe within which the outsourcing took place was very tight. The information they had about the scandal was what was being reported in the media as the data breach scandal unfolded. Respondent B confirmed that based on what was being reported, he could relate to some of the questions he had been indirectly asked at the Agency by those involved in the outsourcing. The Agency uses the National Archive’s specific and general regulations regarding the management of government information and the information systems, but they are not followed by the IT unit as it is assumed that they only concern the archivists. The IT personnel do not read the guidelines and have very little understanding as to why the archivists and the National Archives must involve themselves in their work. Respondent B further confirmed that they try to interest the IT personnel to follow the National Archives’ guidelines, but it is not an easy task.

Respondent A clarified that this is an effect of NPM because in the IT unit, most of the people who have been recruited are from the private sector. Some of these people have never worked in the public sector and therefore do not fully understand the requirements put on them. Respondent A confirmed that there is a cultural shock when the archivists come with their demands where people only have private sector work experience. Additionally, the IT personnel have a higher status in the organization compared to the archivists trained in the management of government information, and they do not as such collaborate with the archivists where information systems are concerned. My follow-up of the reporting that was being done in different media showed that the focus was on the information systems and not the information that they contained.

The impact of new public management on the management of information
Respondent B expressed that there has been a lot of focus on efficiency, cutting costs, encouragement to think about how efficiently processes could be carried out and whether the time spent on each process could be measured. Respondent A complained that new business models are presented all the time, which makes their integration, implementation and follow-up difficult. He further argued that a lot of focus is put on the hard values that are easier to measure and that the soft values are disappearing. By the soft values, the respondent meant the employees’ attitudes toward their work such as devoting extra time to see to it that a process is well executed or undertaking courses to improve their knowledge. Respondent A contended that when the focus is on the hard values such as measuring performance and quarterly reports, the humane aspect of work disappears. This respondent argued that he found it hard, for example, within the information management realm to establish how he can measure performance when it comes to the delivery of information to the archives and appraisal investigations because sometimes these processes can take up to a year to conclude.

Respondent B informed that administrative positions have been reduced, which means that the remaining administrative personnel have heavy workloads and hence must prioritize their work. Where new documentation plans must be created, it is sometimes difficult to find an employee who is willing to do it because they are so few. All these cause stress to the employees. Documentation plans in Swedish administrations document all types of records/information that is generated by each department within the organization, the formats in which the information is captured and the form of preservation or when the
information is to be disposed of. He argued that the appraising of government information should not be arbitrarily pursued and should be based on the guidelines from the National Archives. He confirmed that some of the bosses who never include the cost of information management in their budgets, when they discover how much it will cost to preserve the information, wonder if the information should not be appraised. Respondent B lamented that this was absurd as these bosses display lack of understanding of the need to preserve historical information where old documents are concerned and the citizens’ right to access public documents through the Public Access Act, which also allows public scrutiny and promotes transparency and accountability.

Responding to the question as to whether the Agency had a department charged with the management of its information, Respondent B confirmed that they have due to re-organisations belonged to different units but now belong to a unit called strategic management, which also deals with overall questions that are directed to the Agency. Both respondents expressed the need to find allies outside their unit such as; with the IT department and the business people. They informed that they need to find allies they can convince about the value of structured and systematic information management and the need to comply with the regulations. They, however, confirmed that there are people at the Agency who understand the importance of managing information efficiently and who consider the archivists as contributors to the information management puzzle as they have skills that they lack. These included people such as IT developers and IT architects (people who are not programmers). The relationship that existed between the archivists and their allies to work toward achieving effective information management is not formal and therefore, when such people left the organization, the relationship was also terminated and they had to look for new allies, which is a time-consuming process.

Respondent A argued that the employees needed to understand what a public record is and to reflect over the information they generated if they are to handle it correctly. All employees who worked at the Agency needed to understand the legal framework that governs government information. Both archivists confirmed that some of the employees are very good at managing public records and some are not. Respondent A postulated that the employees daily made decisions that affected the quality of the information. The employees were given a 20 min introductory Web-based course in the management of government information and it was the bosses who were responsible for ensuring that the newly recruited employees followed the course. The archivists used to offer the course in person as this is a large organization and the exercise used to take a lot of time, it was reduced to 20 minutes. They argued that since some of the Agency’s employees are from the private sector where information is not governed by the same stringent legal framework, dedication to the management of information varies. Therefore, not all bosses are interested in information management issues and this is not properly followed up.

Responding to the question as to how the scandal has impacted the management of information, Respondent B confirmed that before the scandal, people did not care much about the kind of information or content they handled, but now everything is super-secret. Suddenly, they cannot almost handle information, and nobody really knows what information they have in custody. Respondent B informed that there was fear in the organization to make mistakes, and lack of knowledge about what is public or not created further insecurities. Information that was supposed to be public was being classified as Level 3, because it might contain personal data. Respondent B informed that the Levels 1, 2 and 3 are those prescribed in The ISO standard 27000 called Management System for Information Security. This was likely to compromise access to government information and transparency and accountability of the Agency.
Respondent A, however, argued that with the implementation of the GDPR, which was implemented by May 2018, a lot of discussions were being pursued at the Agency and future contracts will have to include the management of information. She confirmed that it was not only the archivists who were advocating the effective management of personal data but the Agency’s lawyers too. As public documents contain personal data, she hoped that this would slowly raise awareness and enable the employees to understand the need to effectively manage public records. Despite the shared shortcomings, Respondent B confirmed that their unit was quite active and that they were involved in many projects that were about requirement specification of information systems. They worked with open data, the implementation of GDPR and collaborated with those who work with information security. A management system was in the process of being developed, and they had collaborated with the lady in charge to see to it that information governance issues are put into consideration. They currently had a mission to develop better management and support routines for information governance and were constantly trying to find new ways of improving the information management landscape.

Respondent A confirmed that the positive side of the NPM thinking is the fact that he thought about the way he carries out his work and constantly asked if it was the best way. This created both internal and external value.

Discussion
This study set out to investigate the impact that NPM through outsourcing has had on the management of government information at a Swedish Transport Agency. In the quest for efficient government administrations and high-quality service delivery, a new management style referred to as NPM has been embraced by government administrations. It is about the emulation of private sector practices. Outsourcing, which is a strategy within NPM, is being used by government institutions to cut costs and to create efficiencies. This is not a new trend as literature reveals that it has been going on for a period of over 30 years within Europe. However, the literature reviewed confirmed that more research on the advantages delivered by outsourcing of government functions is needed (Van de Walle and Hammerschmid, 2011). Though the proponents of outsourcing claim that it delivers efficiencies, the empirical data mostly highlighted the negative impact outsourcing has had on the management of government information. The list of the negatives included re-organizations, which interrupts the continuity of processes and the capture of knowledge and routines; the trimming of an organization, which in the studied case left very few administrative personnel and led to stressed employees overwhelmed by work; the prioritization of work, which meant that some work was overlooked such as in the case of the development of the Agency’s document management plans; constantly changing business models were are hard to implement, incorporate and follow-up; the prioritization of the hard values as referred to by one of the respondents which killed the humane side of work, i.e. engagement and the desire to further develop one’s skills; and compromising the most important tenets of democracy upon which public administrations are built, i.e. transparency and democracy.

Information is a strategic resource and should be effectively managed to achieve efficient processes. As argued in the reviewed literature, clauses outlining responsibilities for its management should be included in the outsourcing contracts. Additionally, the literature warned that precaution should be taken to outsource certain functions of government. Even though all employees in an organization created and handled information, the understanding of its management varied. The IT personnel did not collaborate with the archivists to promote efficient information management. They further enjoyed a more
prestigious position at the Agency than the archivists. The unclear distribution of responsibilities between the archivists and IT personnel confused the heads of departments who perceived information management to be the remit of the IT personnel and left the archivists out when outsourcing deals were being made, yet their expertise could have mitigated the risk the exposure of the Agency’s information caused.

Even though government information is governed by a stringent legal framework, most government employees seem to think that information management issues are the remit of the archivists. Organizations should have a department and resources devoted to information management. The Swedish Transport Agency’s organizational chart does not reflect this. As discussed by Leming (2015), information management should be of concern to all employees and organizations should use expertise from various disciplines if information is to be effectively and securely managed. The Swedish National Archives is responsible for the overall management of government information and issues general and specific guidelines to facilitate the management of information at the various agencies, but in this case, the guidelines were not embraced by the IT department. This further confirmed my own research observation that despite the legal framework, some knowledge as to how effective information should be achieved and information systems, information management still poses challenges in Swedish government administrations. Lack of an e-archives is still a challenge to the efficient and secure management of government information (Svärd, 2011). Hopefully, the efforts that are being made through the State Service Center will help government agencies to better manage and coordinate their information resources in some sort of state “cloud.” The findings confirmed that lack of collaboration between the IT personnel, and the archivists compromised the effective management of information.

Furthermore, very little time was devoted to the training of government employees in information management. A person who has never worked in a government institution to be given a 20 min Web-based course demonstrated the lack of understanding of the complexity of the information management landscape that also required an understanding of the legal framework that governed government information. Information management is not about information systems as they are only tools used to facilitate its management. The employees need to understand why government information must be managed. When the IT and data breach scandal happened, the focus was on IT and very little discussion was pursued regarding the information the systems contained and information security.

The complex nature of the information landscape requires collaboration among all stakeholders who should be involved in the drafting of the outsourcing contracts to formulate the necessary clauses that should safeguard government information. Information today is not only there to create efficiencies but also, as demonstrated by the scandal at the Swedish Transport Agency, can put an entire nation at risk. Therefore, information management issues should be taken seriously.

Conclusion
The study sought to investigate the impact that NPM through outsourcing has had on the management of government at a Swedish Transport Agency. The study has had limitations as it was only one category of employees that were interviewed. Further research with a broader focus is therefore needed to capture the views of all employees to enable a broader understanding of the challenges posed by NPM. The study has highlighted the negative effects caused by outsourcing and the need to include information management clauses in the contracts for outsourcing government functions. Government information is the basis upon which transparency and accountability are based, and therefore, its effective and
secure management is of crucial importance to the trust that citizens have in government institutions. The information landscape has become complex, and outsourcing complicates it further as it creates a blend of public and private practices. People who have worked in public administrations might have a better understanding of the routines and guidelines that govern the management of information but those from the private sector might not. This makes the training of all government employees in the management of government information of crucial importance as the quest for efficiency continues. The in-house expertise that should constitute people from different disciplines should be consulted to avoid data breaches. I struggled to find literature that discusses the impact that NPM through outsourcing has had on the management of government information. Hopefully, this article will be a contribution toward this gap.

**Recommendations**

- Outsourcing contracts should include clauses that will ensure that the contracted companies take care of government information according to the legal framework that governs it.
- Outsourcing should be done in consultation with all the stakeholders that might be affected by it.
- Collaboration among employees is key to the effective and secure management of information. The IT personnel, information security personnel, business people and information specialists and management should all be involved.
- Information security should be prioritized as information does not only prevent business efficiencies but also can cause security threats. This means that top management should take more responsibility for the efficient management of information.
- Investments should be made in the training of all government employees in information management and the legal framework that governs it. It should not just be the concern of archivists.
- The implementation of an e-archive solution is crucial to the efficient management of information, its security and service delivery.

**References**


Ceeney, N. (2009), “Information management – headache or opportunity? The challenges that the recent focus on information management is presenting to senior leaders in the public sector”, *Public Policy and Administration*, Vol. 24 No. 3, pp. 339-347.


Appendix. Interview guide

New Public Management as a concept.

- What is your understanding of the concept of “New Public Management”?
- How has it been embraced in your organization?
- What impact has it had on the overall function of your organization?
- What are the advantages and disadvantages of New Public Management?

The Management of Government Information.

- Does the organization have an Information Department that focuses on the management of information?
- What Information Governance Model does your organization have?
- What impact has New Public Management had on the management of information in your organization?
- Is the Information Management Department consulted when information regarding the institution is going to be outsourced?
- Does the organization follow the legal framework governing government information?
- Are the employees given training in information management?
- Do the employees understand the legal framework governing government information for example the Archival Law and the Public Records Act?
- What impact has the scandal had on the information governance model of your institution?
Your Role As an Archivist.

- How is your role understood in the organization?
- How is your expertise used in matters regarding outsourcing of the information that your organisation produces?
- What are the challenges related to your role?
- Do you have Top Management Support in your work as Archivist?
- How are you working to make yourself relevant in discussions regarding the outsourcing of government information?
- What do you think should have been done to avoid the scandal?
- Are the people managing information trained? Do they have the right skills?

Corresponding author
Proscovia Svärd can be contacted at: Proscovia.Svard@sh.se
Open government data: critical information management perspectives

Elizabeth Shepherd, Jenny Bunn, Andrew Flinn and Elizabeth Lomas

Department of Information Studies, University College London, London, UK

Anna Sexton

The National Archives, London, UK, and

Sara Brimble, Katherine Chorley, Emma Harrison, James Lowry and Jessica Page

Department of Information Studies, University College London, London, UK

Abstract

Purpose – Open government data and access to public sector information is commonplace, yet little attention has focussed on the essential roles and responsibilities in practice of the information and records management professionals, who enable public authorities to deliver open data to citizens. This paper aims to consider the perspectives of open government and information practitioners in England on the procedural and policy implications of open data across local public authorities.

Design/methodology/approach – Using four case studies from different parts of the public sector in England (local government, higher education, National Health Service and hospital trust), the research involved master’s level students in the data collection and analysis, alongside academics, thus enhancing the learning experience of students.

Findings – There was little consistency in the location of responsibility for open government data policy, the range of job roles involved or the organisational structures, policy and guidance in place to deliver this function. While this may reflect the organisational differences and professional concerns, it makes it difficult to share best practice. Central government policy encourages public bodies to make their data available for re-use. However, local practice is very variable and perhaps understandably responds more to local organisational strategic and resource priorities. The research found a lack of common metadata standards for open data, different choices about which data to open, problems of data redundancy, inconsistency and data integrity and a wide variety of views on the corporate and public benefits of open data.

Research limitations/implications – The research is limited to England and to non-national public bodies and only draws data from a small number of case studies.

Originality/value – The research contributes to the debate about emerging issues around the complexities of open government data and its public benefits, contributing to the discussions around technology-enabled approaches to citizen engagement and governance. It offers new insights into the interaction between open data and public policy objectives, drawing on the experience of local public sectors in England.

Keywords Information management, England, Open government, Open government data, Public records management

Paper type Research paper

Funding: This work was supported by the Canadian Social Sciences and Humanities Research Council (SSHRC), Trust in Digital Records in an Increasingly Networked Society (InterPARES Trust), grant number 895-2013-1004. UCL is one of the European partners in the InterPARES Trust (IPT), a multi-national, interdisciplinary research project (www.interparestrust.org/).
Introduction

Open government data and access to public sector information in the UK and across the world is in transformation, and yet little attention has focussed on the essential roles and responsibilities in practice of the information and records management professionals who enable public authorities to deliver open government data to citizens. This article presents the research findings from UCL, one of the European partners in the InterPARES Trust (IPT), a multi-national interdisciplinary research project exploring digital records (www.interparestrust.org/). The article considers the perspectives of open government and information practitioners working in localities in England, set into an international academic research frame. It draws on practice experience across different types of local public authorities of the procedural and policy implications of open government data. It seeks to surface the significant but often-overlooked links between the effective management of information and the delivery of open government data.

Since 2013, UCL has run several linked projects that studied the role of the information and records management discipline in the context of new obligations on public sector bodies towards open government data (i.e. the proactive release of data by public sector organisations for re-use by third parties in the public benefit) and greater access to data for citizens. The research aims to develop a picture of implementation and compliance in the field outside central (national) government by using four case studies from different parts of the public sector in England. The lens through which it studied open government data was the professional discipline of information and records management as these professionals have a critical but under-recognised and, hence, often under-resourced role in the practical operation of open government data. It frames the findings from practice with a literature review drawing on academic research into the intersection between open government data and information management internationally. It concludes with implications for policy and practice.

In the policy context, public authorities are responding to the European General Data Protection Regulation (GDPR), which further constrains the requirements for managing and sharing personal data. Regulatory agencies including the UK Information Commissioner’s Office (ICO, 2017b) propose additional administrative data duties such as, the “duty to document”. In addition, citizens demand greater accountability and transparency in public processes. In this shifting climate, it is critical that open government data policy is better understood and framed holistically. Although related to freedom of information, access to public information and records management, as suggested by Janssen et al. (2012) and Zuiderwijk and Janssen (2014), open government data has distinct characteristics that merit investigation. For example, the relationships between open government data, public records, freedom of information, linked data and the role of information managers and data scientists are complex, overlapping and not fully understood, as set out by Luna-Reyes et al. (2014) and Shepherd (2015, 2017). As government functions are increasingly delivered by commercial and third sector bodies in partnership with the public sector, issues of data provenance, guarantees of data standards and ownership need exploration. The secondary use of open government data is a significant resource to policymakers and for academic researchers, especially if data sets can be linked, as Safarov et al. (2017), and Sexton et al. (2017), explore.

Research methods

The foundation of the research was a literature review in two phases, on open government data broadly and then focussing more closely on the related privacy issues. The primary
data about open government data in practice were collected in four linked case studies over a period of three years (2014-2016) in four different local public sector settings: a local government authority, National Health Service (NHS) England, a hospital trust and a university.

**Literature review**

The first stage of the literature review identified key literature about open government data and the record keeper’s role. The second stage of the literature review focussed more specifically on the implications for information management of moves to extend open government data and access to public sector information, including medical records and patient data, in the context of data protection and privacy regulations in the UK and EU. It analysed legislation, policy documents and research literature on the re-use of public sector information, data protection and use of medical records and patient data. The focus was predominately England but also looked outward to legislation and policy in the devolved nations of the UK, as well as internationally.

**Case studies**

The research method adopted was a qualitative, instrumental case study, extended to four cases, each with some similarities and some differences, following Stake’s (1994) typology. He identifies three main types of case studies (intrinsic, instrumental and collective), although all have the characteristics of setting out the historical and contextual background, information about the respondents and the nature of the case. Through the collective case study, the researchers aimed to provide insight into an overall research aim, to investigate the impact of open government data requirements in local public authorities in England through the lens of the practice of information and records management. Each case studied how open data were managed within one public authority, explored the reality of practice and where the roles and responsibilities lie. These case studies enable comparative work, analyzing the open government data policy setting and how it interacts with information management roles. The research explored the role of the information and records manager in practice in an open government environment, given that it is a critical actor in the delivery of open government data to citizens (Thurston, 2012).

The geographical scope was England, bounded by the specific legislative and government policy requirements: firstly, a local government authority in the South East of England responsible for providing services to 1.5 million residents, directly or with commercial and third sector bodies, including transportation, schooling, social care, housing, environment, planning, libraries and culture; secondly, NHS England, which leads the NHS, nationally, regionally and locally by setting strategy and priorities and implementing policies, distributing £100bn annually, commissioning contracts for health services and contributing to public debates on health care (given the unique size and role of this body, it was not possible to anonymise this organisation); thirdly, an NHS hospital trust which delivers clinical services to a large urban population, as in-patients and in the community from several hospital sites. This case is published by Chorley (2017). The fourth case study was a multi-faculty university employing about 1,800 staff, undertaking research, higher education teaching of 20,000 students and knowledge exchange, funded by public and private funds. These four organisational settings had significant differences from each other in terms of size (number of employees and budget), organisational priorities and culture, leadership, government policy context for core service functions and client groups. See Table I for brief details.
In each case, the specific research objectives were:

- to identify the governing legislative and regulatory open government and open data frameworks;
- to investigate existing organisational practices and job roles in delivering open government data and complying with public obligations; and
- to develop better understanding of the critical information management issues, policies and guidance, relating to open government data.

The research process was the same for each case. UCL research ethical approval and data protection registration was obtained for the IPT project overall, 2013-2018. Consent required the anonymisation of interview participants and the organisations, except for NHS England, retaining contextual data, including job titles and organisational type.

Data collection
Research data were collected through a series of 15 individual semi-structured interviews (40-60 min in duration) with information, records, data, governance and other professionals. The interviews were organised on a series of common themes drawn from the literature and designed to explore the research objectives. For example, see the summary of semi-structured interview questions as follows:

1. **Interviewee’s role:**
   - Please explain your role and the responsibilities of your department?

2. **Guidance and Regulations:**
   - What OGD obligations and regulations are imposed by central government?

<table>
<thead>
<tr>
<th>Four IPT case studies</th>
<th>Date of data collection</th>
<th>Research assistant</th>
<th>No. of interviews/job roles of interviewees</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Local government</td>
<td>June-July 2014</td>
<td>Jessica Page</td>
<td>4 interviewees: Information access officer, Business intelligence officer, Records manager, Information governance officer</td>
</tr>
<tr>
<td>2. NHS England</td>
<td>June-July 2015</td>
<td>Emma Harrison</td>
<td>4 interviewees: Senior advisor, The National Archives, Senior data sharing specialist, Head of data policy, Senior information governance advisor</td>
</tr>
<tr>
<td>3. Hospital trust</td>
<td>June-July 2016</td>
<td>Katherine Chorley</td>
<td>3 interviewees: Information governance manager, Corporate records manager, Assistant records manager</td>
</tr>
</tbody>
</table>

Table I. Overview of case studies
What OGD guidance is available?
What internal and external policies are used for publishing OGD?
Is five-star scheme used?
Has OGD impacted on FOIA requests?
What metadata schema is used for OGD?

(3) Implementation:
What are your responsibilities for OGD?
What challenges are there OGD?
How is authenticity, reliability and accuracy of OGD guaranteed?

(4) Roles and Responsibilities:
Who is responsible for OGD?
Which departments publish OGD? What kind of data?

(5) Record-keeping of open government data:
How do OGD and RM systems interact?
What functional classification is used for OGD?
Is OGD linked to other data? How?
What OGD publication formats?
How to ensure accessibility of OGD?
What OGD Policy training?

(6) Users of open government data:
Which groups use OGD?
How does OGD encourage public participation?

(7) End questions:
What are future plans for OGD?

Data collection focussed around guidance and regulations, implementation approaches, roles and responsibilities, record-keeping and users of open government data. We did not specifically seek data about individual data sets but rather the policy and operational context in which they might be made open. Interviews were usually audio recorded and then selectively transcribed.

Documentation supplied by interviewees, including internal policies and procedures, organisation charts and manuals, was also analysed. Data coding and analysis was carried out using the pre-coordinate themes which framed the data collection (i.e. role, responsibilities and job context; governing regulations, institutional policies and guidance for information governance, open data, information and records management, freedom of information and data protection; institutional practices for open government data, information and records management, staff awareness and training; future developments) and extended by the findings of the data collection. An initial summary report of data was shared on the IPT project intranet (https://interparestrust.org/).

Literature review
The literature review framed the research by drawing on academic research into open government data. The literature also helped to establish the themes which were explored in the data collection.
Novais et al. (2013) provided a literature review of open government data studies from 2007 to 2012, in which they indicated the need to broaden the geographic coverage of open government data research and to improve the quality criteria for assessing open government data, including to ensure the trustworthiness of data (Ceolin et al., 2014; Léveillé and Timms, 2015). Novais et al. (2013) suggested that the term open government data began to appear in 2007, following the publication of the original eight open data principles, which stated that open data should be complete, primary not aggregated, timely, accessible, machine-processable, non-discriminatory, non-proprietary and license-free (https://public.resource.org/8_principles.html). These principles framed much of the subsequent discussion, but many technical, managerial, organisational and cultural barriers remain in delivering open data. Kitchin (2014) surveyed the data landscape, including big and open data, and in Chapter 3, he considered the consequences and difficulties of moving from traditional closed data access to more open data access. He provided a clear historical account of the open data movement, discussed further below.

Work on models and methods for evaluating open government data and benchmarking includes Kalampokis et al.’s (2011) stage model of open government data and the Open Data Institute (2015). They built on models proposed to assess the progress of e-government to incorporate open government data more fully by outlining two dimensions (organisational and technological complexity and added value for data consumers) and four stages (aggregation of government data, integration of government data, integration of government data with non-government formal data and integration of government and non-government data with social data). The model should improve benchmarking and the construction of roadmaps for open government data. The information and records management community began to engage with open government data in early 2010s, encouraged by the development of records management guidance in the Open Government Guide (2015), an online resource developed by international civil society organisations to support governments in developing commitments for Open Government Partnership (OGP, www.opengovpartnership.org/) national action plans and by growing professional awareness of the importance of the management of the underlying data to the effective delivery of open government data to citizens. The UK and USA Governments were among the eight founding countries of the OGP in 2011 committed to fostering “a global culture of open government that empowers and delivers for citizens, and advances the ideals of open and participatory 21st century government”, based on access to information, citizen engagement, fiscal transparency and income and asset disclosure (Herrero, 2015). The influence of OGP action plans on practice and on research was considerable. For example, the UK Government (2016) national action plan for 2016-2018 developed in collaboration with civil society organisations included commitments to engage with data users about their needs and to gain their views on priority areas for the development of the open data agenda and to develop <gov.uk>, the website for government publications, to make it more open and accountable.

Privacy and data protection are often seen as problematic in an open data context, inhibiting the public good in sharing data. While sharing data may lie at the heart of the open government data agenda, from a privacy perspective, the right to limit the sharing of identifiable personal information is cast as a fundamental human right. A number of overlapping legal measures exist to protect privacy, including privacy rights, which guarantee freedom from interference; data protection, which controls the processing of personal data; and duties of confidentiality, which protect against unauthorized or unreasonable breaches of confidence (Nuffield Council on Bioethics, 2015). There is recognition that personal privacy is not always in the public interest if it impedes other
fundamental human rights and interests. For example, there is a public good in the use of medical records and patient data to support advances in medical, health and scientific research. However, there is also a public good in respecting and protecting privacy, maintaining confidentiality and limiting the use of medical records and identifiable patient data. Balancing these public goods (the public good in enabling research and the public good in protecting data) is increasingly challenging given the rapidly evolving mechanisms open to researchers and others to reuse and link data (Caldicott, 2013).

Research results and discussion

This section presents and discusses the main practice findings, illustrated by quotations from the interviews, referenced by case study and interview (e.g. 1:1) as in Table I.

Who is responsible for open government data in public authorities?

Our first question sought to understand where responsibility for open government data sat organisationally and the professional groups and units that led on the issue. We were particularly looking for evidence that records and information managers were explicitly involved and their information skills acknowledged as relevant to open data. As might be expected, given that the four case study organisations had very different core mandates and significant differences in size and structure, there was little consistency in the location of responsibility for open government data policy, the range of job roles involved or the organisational structures in place to deliver this function. That each case study took such radically different approaches to delivering the same open data function was perhaps unexpected. As this was a fairly new area of work, the local authority had established an open data working group in its business intelligence team to develop policy, including governance and law, information governance, information access and records management. An operational team for information transparency had responsibility for data protection, freedom of information, data sharing, data security and environmental information but open data was not yet part of its functions. The authority sought to “make the data we are creating as an authority, as part of our daily business, available for more general use” (interview 1:3) and equated open government data with “transparency […] being able to give data to the public when they ask for it and being open about it […] being open about what we spend our money on” (interview 1:1). This authority seemed to have well-established teams to deliver existing information functions, and the cross-functional working group was making progress in defining and identifying the policy aspects of open data as a preliminary step towards making the new function part of an operational team.

In the NHS hospital trust, responsibility for open data was not yet established and no job titles referenced that role directly. As in many health settings, the overarching function was information governance, following the Caldicott (2013) principles for handling patient information across the National Health Service (2016). A traditional line management structure for information governance sat within the directorate of corporate affairs. Information governance and internal corporate records functions were fairly traditionally conceived as having a primarily corporate focus, rather than external obligations for openness and transparency, although with responsibility for freedom of information requests. One interviewee anticipated that when the hospital trust formally adopted an open data function, there would be a separation between policy and operations:

I would expect to see it coming to Corporate Affairs and the stuff that’s around releasing data, IG and FOI would probably come our way, but some of the stuff probably more about policies, about how the Trust runs itself would probably sit with the Trust Secretary. (3:1)
But in practical terms, existing staff would “just do it as we go along” (3:1). Another interviewee thought that open government and open data were not yet high priorities for the hospital trust (3:2). This position is somewhat at odds with the picture given by NHS England, guided by its obligations under the Health and Social Care Act 2012. At the time of the case study in 2015, NHS England had a policy unit to develop policies around information standards, open data and patient care data which sought to be a center of expertise, acting as a “think tank for NHS England” and learning actively “from the best across the UK and internationally” (2:3). NHS Digital collects, manages and publishes health and care data under the direction of NHS England and the Department of Health (2:4). The case study hospital trust noted that it reported large amounts of data to NHS England; much of the hospital’s open data is effectively published by a third party. However, the responsibility for open government data is not always completely clear in large and complex public services. Sometimes it is not clear how variants of data sets relate to each other, or who should publish which ones.

In the university case study, there was evidence of a very active approach to business intelligence, data assurance and responsive provision of personal data and corporate information, partly driven by the requirement to provide data to the Higher Education Statistics Authority (HESA) as a condition of grant funding. One interviewee from the strategy and planning unit admitted, however, “I’m not that familiar with the open data stuff”, which she saw as an external issue about access to data for academic research rather than a corporate issue (4:1). The university records manager’s role had expanded rapidly from managing corporate records and information to include information assets, audit and compliance and information governance. To deal with this changing environment:

We set up an Information Governance Group, [...] more involved in information security and information assurance. What we’ve had to do is to bring together representation from across the HEI including security, IT, academics, our Research Information Manager who handles research data management (4:2).

The case studies suggested that proactive individuals could make progress in encouraging a public authority to develop policy and practice in open government data by bringing a group of interested officers together in a focussed, short-term way, such as on a policy working group, with the longer-term aim of embedding the new function in an existing unit. The corporate environment could help or hinder such initiatives.

No one professional group routinely took on open government data functions: it depended more on the interests of individual staff taking advantage of corporate opportunities rather than yet forming part of formal role descriptions. Job titles included directors of governance and law, information governance specialists, information access officers, data sharing specialists, corporate communications officers, business intelligence officers, heads of data policy, freedom of information and data protection officers and corporate information and records managers. Post holders had backgrounds in law, ICT, information and cybersecurity, informatics, education, social sciences and media and communications, as well as records management. The research reflected a shift in some organisations to information governance as the overarching corporate function for open government data. Information and records managers often have the skills needed to manage and deliver open data, but in practice, their employing organisations did not always exploit these skills for public benefit.
What policy and guidance on open government data exists in public authorities?

Part of the explanation for the variation of approaches to the management of open government data discussed in the previous section might be found in the varied policy and guidance context. All of our case studies were subject to Freedom of Information Act (FOIA) 2000, and the Data Protection Act (DPA) 1998, replaced by the GDPR and DPA in 2018. Although there is no open government data legislation, there is central government policy directed at public bodies encouraging them to make their data available for re-use, including the Open Data White Paper and Open Public Services White Paper (UK Government, 2011, 2012). The OGP promotes the open government agenda through action plans: the UK issued its third action plan including open data commitments in 2016. The requirement to publish certain data to fulfill the government’s transparency agenda at <https://data.gov.uk/> facilitates central agencies in publishing data.

However, considerable local and sectoral variation in policy can be found in our four case studies. Some sectors are much more highly regulated, in particular in two of our case studies in the health sector. NHS England, including NHS Digital, has a responsibility for improving the quality of health and care data and publishes a number of national guidance and policy documents. NHS Records Management Code of Practice for Health and Social Care forms part of NHS Digital’s guidance and policies on information governance, including the Information Governance Toolkit (National Health Service, 2006, 2016). Several of our interviewees commented on the lack of connection between records management and information governance in the NHS, even though these policies ought to support each other. Records management was described as “not visible or vocal enough to be involved in open government data” (2:3). Information governance, by contrast, was well developed and although, the IG Toolkit was “not directly mandated by legislation but it is […] done without question” (2:1). “The idea of patient confidentiality is one that has been at the heart of doctor-patient relationship since time immemorial” (2:4) and data confidentiality is integral to information governance in the NHS. In the NHS, “the more open you get, the more nervous people get” (2:3) and “already there are large numbers of people who do not want their identifiable data used for anything other than their direct care” (2:4), not least in the wake of failed data sharing initiatives such as care data (Presser et al., 2015; McLeod and Childs, 2018), and concerns over data sharing with commercial companies such as Google DeepMind (ICO, 2017a). Much of the data held in the NHS is patient data and identifiable personal data cannot ever be open, such data will only be published if “aggregated and anonymised” (2:4).

The national open data and transparency agendas of NHS England are not always reflected at a local level. Barriers to proactive publication of data, as one interviewee remarked, “the culture is more around publishing as little as possible”, “partly the culture, partly a lack of awareness and also partly […] the technical capability” (3:2). For policy areas not governed by legislation, such as open government data, there was a considerable delay between policy-making at the national level and the filtering down of policy and associated practice to the local level.

By contrast, the local authority case study approach to open government data was longer established, although in practice only a few specific data sets were routinely made open. The Local Government Transparency Code (2015), together with guidance from the Local Government Association, provided a framework, which was overseen locally by elected councillors. One interviewee (1:2) commented on the tension between, on the one hand, central government policy to publish as much data as possible and rules requiring publication of certain local financial data with, on the other hand, allowing the authority to
decide which data was of interest to local public audiences and prioritise their resources to select and process that data for publication.

Problems with delivering open government data in practice were also identified, especially an assumption that data and information are held in well-established electronic systems. Local authorities were expected to meet at least level three of the “5 Star” scheme when publishing data (a simple indicator of the openness of a data set, such as its format and metadata, see <http://5stardata.info/>). In our case study, the local authority records management systems were still predominately based around paper-based records, while emails, HR and financial data were held in separate digital systems. Many different formats were used for the creation and business use of data sets, yet most of the data required re-formatting, additional metadata and re-presentation to make it openly accessible. For the authority to meet the requirements for opening up data and assure data reliability and quality of the data drawn from records systems, major changes in the way data and records were managed and accessed might be needed.

While open government data remains unlegislated, it is largely at the discretion of individual organisations whether they proactively publish data sets, what they publish and indeed for what purpose. The university case study interviewees were mindful of its statutory obligations to provide data to HESA and to comply with data protection and freedom of information but to go beyond that to publish large swathes of data, which might have reputational risks and would cost scarce resources, was not a current priority. As opening up data consumes resources, the corporate, individual and public benefits needed to be balanced.

If more data are to be made open, then choices have to be made by the creating organisation about which data to open. At present, these choices are neither transparent, nor are the reasons for them explained in public. Open data is generally not contextualised and users just see individual datasets: a proper understanding of open data might also require knowledge of which data was not opened.

Open government data as a policy-driven activity is subject to localised pressures. Resources, technical capabilities and strategic and local policy priorities tended to drive the choices about which data to open. Secondary data use is therefore highly dependent on local pathways, and citizens and researchers are faced with highly variable open datasets from place to place, making re-use problematic and unpredictable. The case studies suggested that consistent policies are lacking between different sectors, different organisations and indeed between different teams and units within one organisation, leading to inconsistency and a lack of transparency. While a single common mandated approach would not necessarily serve the needs of diverse organisations and their clients, such a wide range and the lack of even a common set of principles leads to confusion about open data priorities. Under UK FOIA (2000), The National Archives (2009) published a Code of Practice on Records Management providing core common requirements to support freedom of information, which individual organisations could adopt in a way suited to their own structure and mandate: no similar guidance exists for best practice in open government data provision.

*Publishing data is not enough: what else is required?*

As Dawes (2010) stated, publishing data is not enough, it needs to exist within a technical infrastructure and information context that renders it meaningful and usable to the public. The interviewees reported that as data were not created with public access in mind, a considerable amount of work was needed to ensure that data was re-usable, including perhaps requiring staff to change their working practices to use open data formats for
business as usual (1:2). They were also concerned about problems of data redundancy, inconsistency and data integrity. One records manager (1:3) explained her responsibility for guaranteeing protective markings on records containing confidential or personal data and for ensuring the protection of personal data and privacy of individuals before data is made open. The Open Data policy in this case study gave heads of service the responsibility to ensure that data published is as accurate and usable as possible but the practicalities of implementing data checking processes systematically across the authority to ensure this were considerable, according to our interviewees (1:2, 1:4). Another interviewee (3:1) said that there was a need to rebut the misconception that publishing data would be easy and straightforward and commented “I’m sure the politicians do just think it’s the click of a button, but it’s not.”

Complete and accurate metadata sets are needed to establish the connection of the dataset to its creating context and to assist with interpretation but available metadata may be limited to that captured automatically, perhaps with some additional contextual information provided by data creators, according to one interviewee (3:2). Record creators and information governance staff were concerned with the accuracy of metadata, but the presentation and ease of use of the data and explanation of the metadata may be more important to the end user (1:2). A lack of common metadata standards for open government data and lack of standardization of terminology hindered the publication and use of open government data, according to one interviewee (1:3).

Denis and Goëta (2014), in their ethnography of open government data projects in French administrations, noted three significant operations (exploration, extraction and ramification) needed to prepare open data for release. In our study, the quality of the data and the amount of work needed to make it open affected access: cleaner data, for example without any personal data or in simpler formats which are easier to reprocess, were more likely to be made open, simply because it was easier to deal with. “Trying to work out what can be published”, as well as the technical and resource problems, was complex. Even once a decision was made to release data, “when we say it’s going to be open”, is that “just going to be for those researchers who are asking for it” or something “that we’re going to stick on our website that anyone can come onto and look at” (3:1)?

What are the information management challenges of the open government data environment?

The final issue which we sought to examine in our case studies, was to draw out some of the information management challenges of open government data and the proactive release of government data, to consider how information managers might help their parent bodies to meet them. The case study organisations faced many information and records management challenges, including the management of risk, privacy and data security. Protecting personal data, especially sensitive personal data, from inadvertent disclosure is important and risky if not done well. Cleaning up data before proactive release is time-consuming but essential to safeguarding data quality and privacy.

If data is aggregated, linked, anonymised and released openly, data inaccuracies may be impossible to identify and correct and will affect the understanding of the data. Inaccuracies in the data can occur at many stages in the record creating process, through inadvertent or deliberate mistakes in recording, through inaccurate transcription and faulty reprocessing. This risk can be mitigated by reliable internal procedures, including staff training and well-established information management policies and procedures that help to ensure proper data management from creation to public access. The authors
would argue that accurate data is essential for internal corporate uses of data, as much as for open data release.

Technical capabilities of staff and of the institutional infrastructures were identified as issues by the interviewees. For instance, the large quantities of data and large size of data sets to be delivered through websites posed technical challenges, leading to websites freezing or collapsing and disruption to other digital services. Many local public sector organisations do not have the resources to establish sufficiently robust and scalable web services to deliver open government data. So far, shared open data portals outside national government have not emerged in England. Universities could develop shared open data sources for administrative and research data on the shared national models seen in the past to develop computing infrastructure (JANET network) and some research data (e.g. UK Data Archive and Administrative Data Research Network) but at present, most open data development is localised.

Metadata standards for open government data are currently lacking in principle and in practice. Metadata provision is not resource-neutral as most data is coded and described for its original business purpose rather than for re-use. At present the processing of data prior to opening is labour-intensive and, until technology-assisted routine processes are developed, is likely to remain so. The push to open large quantities of data has to be balanced with the need to ensure data and metadata quality and with effective use of scarce resources.

Many of the skills needed to deal with open government data are similar to those needed to manage access to information and many of the principles for managing open data mirror existing information and records management principles and standardised processes, such as provenance, functional classification and creation of standard metadata and description. Information managers are, therefore, well placed to play a leading role in open government data. However, to fulfill these roles and responsibilities effectively and support the development of re-usable and reliable open government data, they need to develop greater awareness of open data, better technical skills in digital data and systems, improved expertise in information security, in routines for anonymisation for personal data, in data analytics, in digital curation and in semantic web technologies. They need to deploy their skills in the assessment and management of risk, environmental and privacy impact assessment. Ensuring that information and records management skills are fit for purpose and used for the public good in an open government data setting is a critical challenge.

**Conclusion**

This study sought to investigate the impact of the open government data environment in local public authorities in England through the lens of the professional practice of information and records management. In particular, it aimed to identify key legislative and regulatory open government data frameworks and principles, through a study of the literature and to investigate existing organizational practices and job roles in delivering open government data through four case studies. The research results showed that in practice in the public authorities in the study, there was little consistency in the location of responsibility for open government data policy organisationally, nor agreement about which professional group should lead the activity, nor common approaches for the practical delivery of open data. This finding is perhaps not surprising given the different governance models adopted by the case study organisations and their different mandates. As a fairly new area of work, many different professions were involved: governance, law, information governance and records management, ICT, cybersecurity and data management. This
highlighted some of the managerial and organisational barriers, which public authorities currently face. Although, a single common approach would not be appropriate for such a variety of public organisations, the lack of consistency inhibits effective sharing of best practice. If public authorities shared good practice and benchmarked across different domains and between different professional groups, then the success stories could better inform authorities whose open government data policy and practice was not yet fully developed.

A number of other barriers to open government data were identified. The technical infrastructure needed to deliver open government data, website capabilities, storage of data, metadata and the long-term provision of access still need development. This was a resource issue, both the costs of implementing improved technical systems but also in terms of ensuring the necessary staff competencies, re-training and re-skilling staff on an ongoing basis. Other technical issues related to the internal systems used to create data and records, which are not yet attuned to open data as a business as usual issue. As a result, data needs extensive re-processing before opening.

Cultural barriers still exist in organisations. Authorities did not agree about the benefits of open government data, some saw it as an exercise in transparency and accountability, others means of ensuring internal data compliance and governance. Few seemed yet to have considered the external needs of open data users and this is an area in which further research would be beneficial to guide policy. If public authorities do not see the value to their business of making government data open, then they will not allocate the necessary resources to ensuring that it happens.

This research suggests that the skills of information and records management professionals could be better utilised to help public authorities to meet open government data challenges. The management of risk, balancing privacy and the public good in open data, against the reputational and individual risks of releasing data inappropriately, is a critical skill. Ensuring data accuracy by enabling datasets to be traceable to their original reliable data source, and ensuring the data governance systems which surround them, is also critical. Information and records managers are well placed to play a leading role in open government data but they need to explain their unique contribution more clearly in a crowded and confusing field.

This work makes three key recommendations:

(1) Open government data policy and structures should be supported by best practice case studies and guidance. As public bodies implement open government data functions, they would benefit from the shared experience and models from best practice.

(2) Designing information systems with the potential to support open government data could be improved if public bodies co-developed shared templates for systems requirements, including open government data metadata standards and standards for the creation of current data. At present, developments seem to be highly localised.

(3) The job roles and organisational structures for delivering open government data initiatives should be clearly articulated and take account of the full range of information expertise including, law, ICT, cybersecurity, information governance and information and records management.

The development of a code of practice for the management of open government data across the public sector would enable these recommendations to be taken forward.
References


Further reading


---


---

**Further reading**


---

RMJ 29,1/2


**Corresponding author**
Elizabeth Shepherd can be contacted at: e.shepherd@ucl.ac.uk
The role of information governance in e-discovery – the case of China

Guanyan Fan
School of Information Resource Management, Renmin University of China, Beijing, China

Abstract
Purpose – This paper aims to examine the situation of organizational information governance (IG) and its relationship with e-discovery in China.

Design/methodology/approach – This study collects laws, court opinions, cases and relevant literature as data and analyzes their content under the guidance of the framework of Information Governance Reference Model of the Electronic Discovery Reference Model (EDRM).

Findings – Inspired by discussions on the challenges of e-discovery and, in particular, the relationships between organizational IG and e-discovery in English literature, the present study attempts an examination of the relevant situations in China. It is the belief of the study that the connection between IG and the legal risk as framed in the EDRM is a necessary one for China as the country is opening its door wider and continues to seek multilateral cooperation. The study found out, through observations and analyses, the following distinctions of e-discovery and its relationship with IG in China. Despite the very similar US and Chinese digital technological environments and the similar acceptance of electronic evidence into litigations, the situations with e-discovery/electronically stored information (ESI) and IG are different within a Chinese context. Legal provisions regarding electronic evidence are brief and vague, litigating procedures rely on the explanations of the Supreme Court and the Supreme Procuratorate and, most relevantly, there is only a small portion of litigations that features a large quantity of ESI in the context of dramatically increased cases involving electronic evidence. The evidentiary qualifications of ESI, e.g. authenticity and reliability, are discussed intensively in academic writings, which, however, was done in a rather isolated manner, without referring to the relationships between and among them. The concept of proportionality, which was one of the key constructions in e-discovery discussions in English literature, was not found in these writings. As a result, organizational IG in China is not discussed in relation to e-discovery or electronic evidence, raising the question as to how e-discovery of a large quantity of ESI will be handled, should such cases emerge.

Research limitations/implications – Extracted mainly from available literature in legal and information fields, this study is necessarily neither exhaustive nor definitive. However, it can be used to further strengthen other empirical data studies. It could be extended within a Chinese context with interviews with legal and IG professionals. In this regard, the reasons that lead to the distinctions as exhibited in the findings could be explored in future investigations. This study does serve as a marker of the position in China compared to the USA. This research suggests that there is an opportunity for comparable studies at a national level, thus generating complementary knowledge for the IG and e-discovery community internationally.

Practical implications – The findings of the study may be instructive to countries with similar situations, that is, a weak linkage between IG and e-discovery. It may serve as a call for more comparable studies, thus generating complementary knowledge for the IG and e-discovery community internationally.

Originality/value – The study reported in this paper is the first of its kind in terms of exploring the relationships between IG and e-discovery in the Chinese context.

Keywords Information governance, E-discovery, Electronic discovery, Electronically stored information, ESI

Paper type Research paper

This research was funded by Renmin University of China (grant number 15XNL032).
Introduction
Information governance (IG) is the specification of decision rights and an accountability framework to encourage desirable behavior in the valuation, creation, storage, use, archival and deletion of information. It includes the processes, roles, standards and metrics that ensure the effective and efficient use of information in enabling an organization to achieve its goals (Gartner, 2018). As framed by The Sedona Conference (2014a), the Electronic Discovery Reference Model (EDRM, at Duke Law School, 2016) has become an integral part of the discovery process that aims at providing a framework for electronically stored information (ESI). According to the US Federal Rules of Civil Procedure, ESI refers to information existing in any electronic/digital format (USA Supreme Court, 2017); or as The Sedona Conference (2014b) puts it, “as opposed to stored in hard copy (i.e. on paper).” Hence, the word “electronic discovery” or “e-discovery.” This broad scope, combined with the fact that organizations are increasingly relying on digital technologies to conduct their businesses, has brought tremendous challenges to litigations involving electronic evidence and to the legal communities in general; the wider the implementation of digital technologies in organizations, the longer the time needed for locating, preserving and collecting relevant ESI (Canadian Lawyer, 2013). Although particular litigations are difficult to predicate, it is safe to assume that the likelihood of litigation exists for most organizations. IG, the field conceived to bring efficient and effective management to organizational information, is, thus, agreed by the legal communities as the necessary preparation for e-discovery (Hailemariam and Marcos, 2018). In China, the implementation of digital technologies has been gaining momentum in the past decade, and electronic evidence has also found its place in both civil and criminal laws that were updated in recent years. What is the situation with organizational information governance in China and what are the relationships between e-discovery and IG in the Chinese setting? Literature searches within the Chinese major academic databases did not return any existing studies that were highly relevant to the inquiries. As a result, a study was designed to explore the ESI and IG situations in China, and this paper reports on its main findings.

Methodological approach
To serve the objectives of the study, the approach of inquiry included the following steps:

- analyzing the litigating procedures that are relevant to e-discovery and ESI (or their equivalents);
- distilling and analyzing provisions from relevant laws and judicial interpretations that concern e-discovery and ESI;
- identifying and analyzing litigated cases that reflect e-discovery and ESI;
- identifying and analyzing legal writings that focused on e-discovery and ESI; and
- identifying and analyzing academic writings that focused on IG and its role in e-discovery.

Data were collected mainly from laws, legal cases and academic writings. The cases are 50 samples recommended by pkulaw.cn for lawyers to better understand ESI and e-discovery rules. Pkulaw.cn (2018) is claimed to be the most comprehensive, professional and advanced legal information retrieval system in China. It was founded by the Law School of Peking University in 1985 and has a good reputation in the legal communities for its professional comments on cases. Legal and academic writings were selected from law reviews and journals indexed by the Chinese Social Sciences Citation Index (CSSCI) and Peking University Core Periodical Catalogue (PUCPC). CSSCI and PUCPC are the top two
interdisciplinary citation index programs highly recognized by scholars in social science, including those from the legal communities.

Guiding data analysis is the conceptual establishment of the Information Governance Reference Model (IGRM) of the EDRM. IGRM is a framework and responsibility model for cross-functional and executive dialog that serves as a catalyst for defining a unified governance approach to information by linking business value and legal duties to the information assets (EDRM Duke Law, 2012a). It distinguishes value from IT efficiency or regulatory obligations and categorizes the stakeholders involved into three groups in the top level: business users, whose responsibility is to categorize, define and declare the specific value of information; IT departments, whose primary focus is on increasing efficiency and decreasing costs for managing information assets; and legal, RIM and privacy and security departments, who understand the organization’s duty to preserve information beyond its immediate business value and manage risks for the company (EDRM Duke Law, 2012b). Effective IG offering effective management of ESI can lead to more efficient e-discovery processes by reducing volume, increasing efficiency and lowering related risks and costs (EDRM Duke Law, 2012c).

Analyses and findings
*Litigating procedures relevant to e-discovery and electronically stored information*

Just like “ESI” is the term used in the US Federal Rules of Civil Procedure for electronic evidence, “electronic data” is the term used in Chinese laws. Electronic data are data “created in the case and stored, manipulated and communicated in digital form” (Supreme People’s Court, 2016). They contain a scope of digital entities, varying from information on network platforms and in Web apps to registration and documented information (Supreme People’s Court, 2015).

According to the Civil Procedure Law in China, a litigant at the discovery stage may ask the court to collect necessary evidences that are out of his control or custodianship, including requests for documents that are in the possession of the opposing parties, but the requests must be specific, not categorical inquiries (Standing Committee of the National People’s Congress, 2017). Similarly, disclosure and review of evidences are accomplished through authorizing lawyers with the right to read all the case files (including any evidence the opposing parties intend to use in court). Evidence exchanges in pre-trial conferences organized by the court offer another way for evidence disclosure (Supreme People’s Court, 2001). However, it is the judge who always has the final say during the trial to determine whether a specific evidence is adopted in court and how much value it may contribute. In short, e-discovery in China is achieved through a combination of reading rights, evidence collection requests and evidence exchanges guided by the court. E-discovery in the USA allows a party to obtain evidence from other parties regarding any non-privileged matter that is relevant to any party’s claim or defense (USA Supreme Court, 2017). Clearly, e-discovery in the USA is broader and more aggressive, and the Chinese one is more limited.

*Legal provisions concerning e-discovery and electronically stored information*

Table I lists all the laws and judicial interpretations that contain provisions concerning e-discovery and ESI.

Figure 1 shows the frequency of appearance of the main participants, litigating processes and evidence concerns in those provisions.

The analysis shows that the court plays an important role when it comes to evidence discovery, especially on the obligations of collecting evidence on request and reviewing and verifying evidence (including admissibility and weight). However, this assignment raises
questions as to the practicality of handling a large quantity of ESI by the court, which in return generates an urgent need for experts specialized in electronic evidence. This gives reason for the rapid growth of a large number of e-discovery judicial expert institutions/departments in recent years. As for evidence concerns, the analysis found that integrity and

<table>
<thead>
<tr>
<th>No.</th>
<th>Name</th>
<th>Category</th>
<th>Issuing authority</th>
<th>Document no.</th>
<th>Articles</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Criminal Procedure Law of the People's Republic of China (2012 Amendment)</td>
<td>Laws</td>
<td>National People’s Congress</td>
<td>Order No. 55 of the President of the People’s Republic of China</td>
<td>48</td>
</tr>
<tr>
<td>2</td>
<td>The Civil Procedure Law of the People’s Republic of China (2017 Revision)</td>
<td>Laws</td>
<td>Standing Committee of the National People’s Congress</td>
<td>Order No. 71 of the President of the People’s Republic of China</td>
<td>63</td>
</tr>
<tr>
<td>3</td>
<td>The Administrative Litigation Law of the People’s Republic of China (2017 Revision)</td>
<td>Laws</td>
<td>Standing Committee of the National People’s Congress</td>
<td>Order No. 71 of the President of the People’s Republic of China</td>
<td>33</td>
</tr>
<tr>
<td>4</td>
<td>Contract Law of the People’s Republic of China</td>
<td>Laws</td>
<td>National People’s Congress</td>
<td>Order [1999] No. 15 of the President of the People’s Republic of China</td>
<td>11, 16,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>26, 34</td>
</tr>
<tr>
<td>5</td>
<td>Electronic Signature Law of the People’s Republic of China (2015 Amendment)</td>
<td>Laws</td>
<td>Standing Committee of the National People’s Congress</td>
<td>Order No. 24 of the President of the People’s Republic of China</td>
<td>1-26</td>
</tr>
<tr>
<td>6</td>
<td>Interpretation of the Supreme People’s Court on the Application of the Civil Procedure Law of the People’s Republic of China</td>
<td>Judicial interpretation</td>
<td>Supreme People’s Court</td>
<td>Interpretation No. 5 [2015] of the Supreme People’s Court</td>
<td>116</td>
</tr>
<tr>
<td>7</td>
<td>Interpretation of the Supreme People’s Court on the Application of the Criminal Procedure Law of the People’s Republic of China</td>
<td>Judicial interpretation</td>
<td>Supreme People’s Court</td>
<td>Interpretation No. 21 [2012] of the Supreme People’s Court</td>
<td>93, 94</td>
</tr>
<tr>
<td>8</td>
<td>Provisions on Several Issues Concerning the Examination and Judgment of Evidence in Death Sentence Cases</td>
<td>Document of Judicial Interpretation</td>
<td>Supreme People’s Court, Supreme People’s Procuratorate, Ministry of Public Security</td>
<td>No. 20 [2010] of the Supreme People’s Court</td>
<td>29</td>
</tr>
<tr>
<td>9</td>
<td>Provisions on Several Issues concerning the Collection, Taking, Examination and Judgment of Electronic Data in the Handling of Criminal Cases</td>
<td>Document of Judicial Interpretation</td>
<td>Supreme People’s Court, Supreme People’s Procuratorate, Ministry of Public Security</td>
<td>No. 22 [2016] of the Supreme People’s Court</td>
<td>1-30</td>
</tr>
</tbody>
</table>

Table I. Legal provisions concerning e-discovery and ESI
authenticity of ESI, rather than relevance, are more emphasized in laws. Furthermore, when it comes to the authentication of ESI, the court relies more on technological methods such as verifying checksums or reviewing the access-logging records after the capture of the ESI, rather than any self-authenticating or judicial presumption rules.

Cases concerning e-discovery and electronically stored information issues
The 50 sample cases are very representative in terms of dispute issues and ESI categories. The samples cover several types of civil cases processed by courts in 16 provinces and three municipalities, including contract disputes (16), intellectual property (12), (virtual) property disputes (8), financial disputes (3), labor disputes (1) and right infringement (1). The ESI involved in the cases demonstrate the most common record types in various forms and formats, including emails, text messages, websites and online purchase records. Other types include communication information in apps such as QQ and WeChat, single records such as photos, videos, electronic contracts, meeting minutes and memorandum, information systems and databases for business transactions or administration, software, e-books, websites, databases, logs, and source code.

Nearly half of the cases were commercial disputes between companies. Of these, 44 cases had at least one litigant who was a corporate entity offering e-commerce or other online services. However, further examination on these cases shows that only a small portion involved a large quantity of ESI in the setting-up of organization in China. These cases were mostly related to intellectual- and virtual-property disputes among companies, which required large quantities of network data, such as online transactions or product quotations, to evaluate the loss caused by infringement. In the case of Wuzhou Ceramics Ltd. v. Jingtian Ceramics Ltd. (CLLC.9805645), Wuzhou accused Jingtian of infringing its intellectual property on the work of art called “Barrel Water Tank.” The court, on the request of evidence preserved by Wuzhou, obtained 4,000 pirated products on the site of Jingtian that exactly matched the design of “Barrel Water Tank,” together with transaction records in excel form, which documented a total of RMB 200,200 orders. Wuzhou submitted the manuscript of design on the computer and related emails demonstrating the release of the
work in its company. It requested a compensation of RMB 200,000 from Jingtian. The court confirmed the intellectual property of Wuzhou but only provided a verdict of compensation of RMB 120,000 as Wuzhou failed to offer detailed, authenticated online transaction records and reliable evidence for the product price. As a result, the court had to decline its proposal and evaluate the loss according to the electronic records obtained from the accused company – Jingtian.

Apart from intellectual property cases, internet service providers are more likely to be accused, compared to traditional ones. The search engine issues for Google in case CLI.C.855450 and CLI.C.884376 and for Heyi Information Technology Ltd and PPTV Communication Technology Ltd in case CLI.C.1762633 serve as good examples. Among the 50 cases, Google was charged twice by two Chinese companies – once in 2008 by a Baoding law firm for tagging its website as a malicious and threatening site and later in 2009, by Hegao Magneto-electricity Company for fraud charges on Google AdWords service. Both cases involved access logging, codes and online contracts, but the former focused on deciding whether possible codes could lead to Trojan virus and the latter hanged on the legal effect of online contracts. Another case came from the video-sharing field. Shengshi Company, the owner of a TV program named “Husband and Wife,” found its TV programs were posted online by Youku (an online video-sharing site owned by Heyi). PPlive, also a video-sharing and retrieval website owned by PPTV, when searched, permitted its users to click the link to Youku and watch the program on its own website. Both companies offered evidences, including expert opinions on video-searching and video-playing functions of the website, to prove their innocence. In China, Rule 22 of the Regulation on the Protection of the Right to Communicate Works to the Public over Information Networks identifies five conditions for video-sharing websites to be immune from prosecution (“Safe Harbor Rules” as they are called), but the key point is to determine whether the video-sharing site was aware of the infringement before informed. The court examined the operating mode of Youku website and the retrieval techniques of PPlive. The judge determined that Heyi was responsible for the infringement as the videos containing the TV programs were stored in its Web server and tagged under the category systems on Youku website. Although the video can also be played on PPlive as it adopted the “deep link” configuration, PPTV had no way to know of the infringement before a user’s searching, or to stop directing the user to the video posted on Youku. So, PPTV was, in the end, judged as having no responsibility for the infringement, a verdict which is controversial even today.

Legal writings focusing on e-discovery and electronically stored information

Focusing on topics of e-discovery and ESI, the study selected 117 articles from legal reviews and journals indexed by CSSCI and PUCPC for the past ten years (2008-2018). Figure 2 shows the keywords related with e-discovery processes and concerns that rank high in the articles.

An overall review of the articles found that within the academic legal discipline, there is a critical interest in discussing rules concerning the review and verification of electronic evidence. The role of lawyers in Chinese courts do differ. They do care about collection of ESI in the discovery stage but focus, to a greater extent, on how the operations in the collection process may affect the admissibility and weight of ESI in court. This focus leads to the special concern of the authenticity of ESI, rather than relevance or proportionality. This finding is verified by the research conducted in 2016 by the Law School of Renmin University. The research studied 181 civil cases typically involved with e-discovery issues from January 2013 to July 2015 and found lawyers/litigants in 65.7 per cent cases raised inquiries concerning the authenticity of ESI in court, while the number for relevance
accounts for only 40.3 per cent (Liu, 2016). However, the research also pointed out that despite the higher rate of inquiries on authenticity, the lawyers achieved more when questioning the relevance of ESI compared with authenticity, as it is not easy to offer strong evidence to convince the judge of the fabrication or inaccuracy of the ESI without in-depth investigations.

**Information governance and its relationship with e-discovery**

The concept of IG came into being in 2001 in China but was primarily referred to as the prevention of false accounting information (Li and Guan, 2001), which later extended to the control of online junk information or rumors for crisis response in public management (Xie, 2009). In recent years, IG is also used to name a package of strategies or plans for information industrial development at the national level (An, 2015). There are also a handful of journal articles (for example, Li, 2013) on corporate IG, which centers on system management and business process integration. Yet, none of these contexts indicate any relationship with the mode of information management in the setting of the organization, as suggested by IGRM. Rather, information in Chinese organizations and IG-relevant academia are typically being discussed as “resources” only, which, when well managed and/or shared, offers profit-producing opportunities and competitive advantages. This trend is closely related with the “informatization” movement in the nation. The informatization movement can be dated back to the first National Conference on Informatization in 1997, in which national informatization was defined as:
[...] the application of modern information technology in all sectors including agriculture, industries, science and technology, national defense and social life under unified planning and organization to facilitate the national modernization process.

Over the decades, the national informatization program in China has been propelled by six main strategies: exploiting and utilizing information resources, building national internet network, promoting IT applications, developing IT industries, training information talents and formulating information policies. The whole movement has been focusing on using information technology to promote industrialization and actualize the expeditious development in productivity (General Office of the Communist Party of China, 2006). In this legal/litigation context and policy environment, IG in China is mostly perceived as possessing only one of the five functions in the IGRM, that is, business profit. The other functions, in particular the risk-featured ones (i.e. legal risk, privacy and security risk and records and information management risk) do not appear to be IG concerns. Likewise, the links between e-discovery and IG can hardly be perceived in China. While optimizing e-discovery processes using the IGRM has been a hot topic abroad (Ledergerber and Knouff, 2012), the situation in China shows a sharp contrast.

Conclusion
Inspired by discussions on the challenges of e-discovery and, in particular, the relationships between organizational IG and e-discovery in English literature, the present study attempted an examination of the relevant situations in China. It is the belief of the study that the connection between IG and the legal risk as framed in the EDRM is a necessary one for China as the country is opening its door wider and continues to seek multilateral cooperation.

The study found out, through observations and analyses, the following distinctions of e-discovery and its relationship with IG in China:

- Despite the very similar US and Chinese digital technological environments and the similar acceptance of electronic evidence into litigations, the situations with e-discovery/ESI and IG are different within a Chinese context.
- Legal provisions regarding electronic evidence are brief and vague, litigating procedures rely on the explanations of the Supreme Court and the Supreme Procuratorate and, most relevantly, there is only a small portion of litigations that features a large quantity of ESI in the context of dramatically increased cases involving electronic evidence.
- The evidentiary qualifications of electronically stored information, e.g. authenticity and reliability, are discussed intensively in academic writings, which, however, was done in a rather isolated manner, without referring to the relationships between and among them.
- The concept of proportionality, which was one of the key constructions in e-discovery discussions in English literature, was not found in these writings.
- As a result, organizational IG in China is not discussed in relation to e-discovery or electronic evidence, raising the question as to how e-discovery of a large quantity of ESI will be handled, should such cases emerge.

Extracted mainly from available literature in legal and information fields, this study is necessarily neither exhaustive nor definitive. However, it can be used to further strengthen other empirical data studies. It could be extended within a Chinese context with interviews.
with legal and IG professionals. In this regard, the reasons that lead to the distinctions as exhibited in the findings could be explored in future investigations. This study does serve as a marker of the position in China compared to the USA. The research suggests that there is an opportunity for comparable studies at a national level, thus generating complementary knowledge for the IG and e-discovery community internationally.

References


Standing Committee of the National People’s Congress (2017), *Order No. 71 of the President of the People’s Republic of China: The Civil Procedure Law of the People’s Republic of China (2017 Revision)*, Standing Committee of the National People’s Congress, Beijing.

Supreme People’s Court (2015), Interpretation No. 5 [2015]: Interpretation of the Supreme People’s Court on the Application of the Civil Procedure Law of the People’s Republic of China, Supreme People’s Court, Beijing.

Supreme People’s Court (2016), No. 22 [2016] of the Supreme People’s Court: Provisions on Several Issues concerning the Collection, Taking, Examination, and Judgment of Electronic Data in the Handling of Criminal Cases, Supreme People’s Court, Beijing.


Corresponding author
Guanyan Fan can be contacted at: fanguanyan2012@163.com
Participatory information governance
Transforming recordkeeping for childhood out-of-home Care
Joanne Evans, Sue McKemmish and Gregory Rolan
Centre for Organisational and Social Informatics, Monash University, Melbourne, Australia

Abstract

Purpose – This paper examines the recordkeeping governance requirements of the childhood out-of-home Care sector, with critical interlaced identity, memory, cultural and accountability needs. They argue that as we enter a new era of participation, new models for governance are required to recognise and dynamically negotiate a range of rights in and to records, across space and through time. Instead of recordkeeping configured to support closed organisations and closely bounded information silos, there is a need for recordkeeping to reflect, facilitate and be part of governance frameworks for organisations as nodes in complex information networks.

Design/methodology/approach – The paper reports on a key outcome of the Setting the Record Straight for the Rights of the Child National Summit held in Melbourne Australia in May 2017, the National Framework for Recordkeeping in Out-of-Home Care, and the research and advocacy agenda that will support its development.

Findings – The authors argue that as we enter an algorithmic age, designing for shared ownership, stewardship, interoperability and participation is an increasing imperative to address the information asymmetries that foster social disadvantage and discrimination. The authors introduce the concept of participatory information governance in response to social, political and cultural mandates for recordkeeping. Given the challenges associated with progressing new participatory models of recordkeeping governance in the inhospitable environment of existing recordkeeping law, standards and governance frameworks, the authors outline how these frameworks will need to be re-figured for participatory recordkeeping.

Practical implications – The National Framework for Recordkeeping for Childhood Out-of-Home Care seeks to address the systemic recordkeeping problems that have been most recently highlighted in the 2013-2017 Royal Commission into Institutional Responses to Child Sexual Abuse.

Social implications – The National Framework for Recordkeeping for Childhood Out-of-Home Care will also address how a suite of recordkeeping rights can be embedded into networked socio-technical systems. This represents an example of a framework for participatory information governance which can help guide the design of new systems in an algorithmic age.

Originality/value – The proposed National Framework represents a new model for recordkeeping governance to recognise and enact multiple rights in records. Designed to support the lifelong identity, memory and accountability needs for those who experience childhood out-of-home Care, it aims to foster the
transformation of recordkeeping and archival infrastructure to a participatory model that can address the current inequities and better enable the design and oversight of equitable algorithmic systems.

Keywords  Social justice, Social care, Information governance, Participatory recordkeeping

Paper type  Research paper

Introduction
Emerging discourses on governance respond to a number of political, societal and technological changes. As faith in monolithic hierarchical bureaucracies has broken down, network forms of delivering public services have emerged in which governments coordinate public, private, commercial and not-for-profit actors. While not necessarily new, growing concerns with how these networks operate in a transparent, inclusive, responsive and participatory manner is reflected in increased interest in governance, not just as a buzz word, but as it applies across all kinds and layers of societal organisations and systems (Bevir, 2012). For example, the following UNESCO definition highlights the role of governance frameworks in distributing power for fairness, equity and justice and the need for accountability and transparency in and across management and operational systems.

Governance has been defined to refer to structures and processes that are designed to ensure accountability, transparency, responsiveness, rule of law, stability, equity and inclusiveness, empowerment, and broad-based participation [...] Governance systems set the parameters under which management and administrative systems will operate. Governance is about how power is distributed and shared, how policies are formulated, priorities set and stakeholders made accountable (UNESCO, 2015).

In Australia, a major focus of recommendations of the recent Royal Commission on Institutional Responses to Child Sexual Abuse (RCIRCSA) is the development of a National Framework for Child Safety (RCIRCSA, 2017a, p. 317) to co-ordinate cross-sectoral and interdisciplinary action. The RCIRCSA (2017a, p. 316) was critical of the domination of existing governance frameworks by government child protection agencies and outsourced service providers, finding that child safety requires national leadership and “a coordinated interdisciplinary response across multiple sectors and all jurisdictions” – justice, child protection, health, education, disability services, out-of-home care, the faith-based sector and community services[1]. It recommended mandatory implementation of ten Child Safe Standards to ensure institutions fulfilled their responsibility to uphold the United Nations Convention on the Rights of the Child (UN General Assembly, 1989) and to always act in the best interests of the child (Article 3). The Australian Human Rights Commission has subsequently developed the Standards into a suite of National Principles for Child Safe Organisations, currently with COAG (Council of Australian Governments) for endorsement (Australian Human Rights Commission, 2018). The Royal Commission also recommended five high level principles for recordkeeping (RCIRCSA, 2017b, pp. 22-23) to supplement the Child Safe Standards, as illustrated in Figure 1.

The Commission viewed recordkeeping principles as particularly relevant to Standard 1 and embedding child safety in institutional leadership, governance and culture. Quality recordkeeping is equally critical to decision-making, engaging other stakeholders, providing authoritative sources of information and supporting complaints processes. Specifying the elemental role of comprehensive high-quality recordkeeping in good governance, particularly in the out-of-home Care sector, the Commissioners stated:

They help promote consistency of practice, retention of organisational memory and institutional accountability. They also help institutions to maintain descriptions of their processes, decisions,
Figure 1. Recordkeeping principles for child safe organisations

Recommendation 8.4 Records and recordkeeping principles

1. Creating and keeping full and accurate records relevant to child safety and wellbeing, including child sexual abuse, is in the best interests of children and should be an integral part of institutional leadership, governance and culture.

2. Full and accurate records should be created about all incidents, responses and decisions affecting child safety and wellbeing, including child sexual abuse.

3. Records relevant to child safety and wellbeing, including child sexual abuse, should be maintained appropriately.

4. Records relevant to child safety and wellbeing, including child sexual abuse, should only be disposed of in accordance with law or policy.

5. Individuals’ existing rights to access, amend or annotate records about themselves should be recognised to the fullest extent.

Recommendation 6.5 Child safe standards from the Royal Commission into Institutional Responses to Child Sexual Abuse Final Report (volume 8)
activities and responses to critical incidents, providing a level of transparency and evidence of practices that can be relied on in the future (RCIRCSA, 2017b, p. 38).

They also acknowledged that:

Creating and keeping accurate records about children, and the care and services provided to them, promotes the best interests of the child by fostering accountability and transparency and recognising individuals’ character and experience. Importantly, these records matter to individuals when they are adults – to satisfy their essential human needs in relation to identity and personal history and for practical reasons, including in relation to redress and civil or criminal proceedings (RCIRCSA, 2017b, p. 62).

The Commission’s findings on the role of recordkeeping in good governance, transparency and accountability align closely with the views of records continuum scholars. The records continuum is predicated on the role of quality recordkeeping (encompassing archiving) in governance frameworks as instruments for individual, group, corporate and collective accountability, identity, memory and authoritative resource management in and through time (McKemmish, 2001; Reed et al., 2018). How well recordkeeping systems and their role in governance are designed for “accountability, transparency, responsiveness, rule of law, stability, equity and inclusiveness, empowerment and broad-based participation” is a professional, transdisciplinary and ethical challenge. It is essential that recordkeeping governance frameworks and systems are themselves accountable and transparent. The Royal Commission found many instances of poor or absent recordkeeping frameworks and practice in child welfare and out-of-home Care. Allied with this is growing concern about the lack of transparency and accountability in IT and data governance which is particularly critical to the design of accountable recordkeeping frameworks, infrastructures and systems for an algorithmic age.

**Participatory information governance**

In contrast to the definitions of governance above, definitions of information governance focus narrowly on the frameworks for managing information within organisations and from organisational perspectives (Hagmann, 2013; Lomas, 2010). For example:

IG is the art of trusted interaction between the major stakeholders of an IG programme (IT, Business, Legal and Compliance, RIM, Security and Privacy). They aspire to joining up to minimise information risks to the enterprise while maximising the value of information assets through building desirable behaviours and enabling cross-functional decision making (Hagmann, 2013, p. 231).

Here, information governance is conceptualised as a subset of corporate governance where information is an asset, singularly owned by the organisation and managed for organisational liability and risk. Recordkeeping governance frameworks as reflected in international and national standards and legislation are largely driven by the concerns of government, corporate enterprises and collecting archival institutions. They embed and perpetuate the construct of a singular records creator, who has ownership and control over the records created and managed in their systems, with very limited rights for the powerless subjects of the record.

The focus of information governance is often on internal accountability and organisational self-interest, self-protection and self-preservation, with societal obligations filtered through this lens. The goal is legal compliance rather than direct engagement with concepts of information equity, inclusiveness and empowerment. For example, while freedom of information and privacy laws reflects some of the
information rights of those with whom an organisation interacts, such laws are restricted to rights of access and consent to information sharing as opposed to being frameworks for shared ownership and control. ISO 15489-1: 2016, *Information and documentation — Records management* presents a digital-ready set of recordkeeping principles, as well as key techniques, tools and processes for the creation, capture and management of records in all forms. However, although it references organisational recordkeeping in collaborative and multi-jurisdictional contexts, its main focus is on the design of accountable recordkeeping policies and systems in siloed organisations in government and corporate contexts. It acknowledges the:

> [...] increased expectations of transparency of decision-making from business and government, the general public, customers, users of services, records’ subjects, and others with an interest in how records are created, captured and managed (International Organization for Standardization, 2016, p. 5)

However, the recordkeeping requirements of the “subjects” of the records are largely ignored. Notions of multiple provenance and agency in records, the human rights and social justice roles that recordkeeping might play, the potential for networked recordkeeping governance models and the recordkeeping accountability of the organisation to the multiple parties in business and recordkeeping transactions are mostly absent. Similarly missing are considerations of equity and inclusiveness, empowerment, affect and broad-based participation[2]. The emergence of data science and automated decision-making using machine-learning models as core planks of information systems design (Metz, 2016) is an additional imperative for adopting participatory information governance.

Organisational culture also impacts on how liberally or narrowly governance frameworks are implemented. As Wanna (2018, p. 11) argues:

> Good governance flourishes not only where citizens have rights of access to information, procedures and documentation, but also where a culture of openness and accountability permeates the relations between government and citizens.

This paper therefore departs from narrow organisation-centred views of information and recordkeeping governance as the frameworks in which one particular kind of entity in societal systems (i.e. an organisation) manages its data, information flows and recordkeeping practice for a more holistic discussion. In records continuum terms, this represents a shift from focussing on third dimension perspectives to privileging fourth dimension ones – from recordkeeping regimes that service organisational requirements to those that carry records beyond the boundaries of individual organisations in response to social, political and cultural mandates for recordkeeping (McKemmish *et al.*, 2010). We align with what Terry Cook identified in 2001:

> "Governance" includes being cognizant of the interaction of citizens with the state, the impact of the state on society, and the functions or activities of society itself as much as it does the inward-facing structures of government and its bureaucrats. [...] This citizen-state interactive relationship, I should note here, would be reflected in other jurisdictions by interaction of members with their church or union, students with a university, customers with a company, and so on - this broader “governance” perspective is not only for government archivists, but all archivists. The challenge for archival science in the new century is to preserve recorded evidence of governance, not just of governments governing. [...] Archivists serve society, not the state, even though they may work for an agency found within the state’s bureaucracy (Cook, 2001, p. 19).
Again, as continuum scholars, we substitute the term recordkeeping professionals for archivist “as being concerned with the multiple purposes of records” and taking “current, regulatory and historical perspectives on recordkeeping simultaneously not sequentially” (McKemmish, 1997).

**Recordkeeping for out-of-home Care**

Out-of-home Care is the term used in Australia to describe temporary, medium- or long-term living arrangements for children and young people who cannot live in their family home because of concerns regarding physical, sexual and emotional abuse or neglect. As in many other countries, through various waves of reform, we have gone from children growing up under quite frightening and brutal conditions in children’s homes, orphanages and other residential institutions to placement in foster, family or other supervised care when it is deemed not safe for them to live with their parents. Supervised group housing facilities are now a placement of last resort once other options have been exhausted (Commission for Children and Young People, 2015).

There have been a myriad of inquiries into Australia’s state-based child protection systems with the RCIRCSA latest in a long line of inquiries into “systemic and enduring” recordkeeping problems. They have all highlighted the lifelong identity, memory, cultural, accountability and information accessibility challenges for those caught up in child welfare and protection systems in the twentieth and early twenty-first centuries. Past and present recordkeeping regimes and archival access frameworks have failed to provide answers to fundamental questions such as:

**Q1.** Where do I belong?

**Q2.** Who took me from my family and why?

**Q3.** How were decisions made about where I ended up? How were other decisions made about my time in care? How were decisions made to keep me in care?

**Q4.** What about my family while I was in care?

**Q5.** What was I like as a child and young person?

Testimonies, submissions and other reports have described how Care leavers find government, organisational and institutional archives wanting when they turn to them to make sense of the dislocation, disconnection, neglect, trauma and abuse suffered during childhood out-of-home Care. The Royal Commission heard from abuse survivors that the damaging effects of the absence or poor quality of records and recordkeeping included:

- disconnection from family and community;
- lack of knowledge about personal and family medical histories;
- loss of ethnicity, language and culture;
- loss of childhood experiences and memories; and

Current standards for child protection emphasise the need to put the physical, emotional, spiritual and social health and well-being of children and young people at the centre of service provision (FaHCSIA, 2011). However, their implementation is constrained by recordkeeping infrastructure and cultures from previous eras of child protection and welfare.
and the kind of information governance structures mandated in extant legislation and standards. Elsewhere, we have explored how Australia’s child welfare systems and their recordkeeping have been indelibly shaped by colonisation (McKemmish et al., under review). Although many may consider colonisation as a matter of history, society in former colonies continues to be structured by colonial institutions, legal frameworks, policies, practice and philosophies. In Australia, classist, heteropatriarchal, sexist and racist colonial constructs of child welfare, the neglected and criminal child and indigeneity persist into the twenty-first century in principles and values embedded in recordkeeping.

A national framework for recordkeeping in out-of-home Care

The immediate and lifelong recordkeeping needs for childhood out-of-home Care cannot be addressed by incremental improvements. Extant laws, standards and infrastructure designed for a different age, different values and a different technological paradigm puts the rights of the organisations, institutions and governments responsible for child protection and welfare ahead of those of children and their adult selves.

The future lies in moving to a participatory recordkeeping paradigm (Evans et al., 2015, 2017):

- transforming frameworks, processes and systems around respecting, representing and enacting multiple rights in records;
- taking advantage of affordances in digital and networking technologies; and
- re-imagining, re-designing and re-building an integrated child/person centred recordkeeping infrastructure driven by the experience and expertise of stakeholder communities; involving a range of community, professional and disciplinary stakeholders in gaining deeper and better understanding striving for innovative solutions; and transcending the current limits and boundaries of any particular stakeholder’s knowledge and expertise.

Faced with the size, scope and nature of this challenge, we have been working with community advocacy organisations – Care Leavers Australasia Network (CLAN), an independent, peak membership body to represent, support and advocate for people who were raised in out-of-home care; the Child Migrants Trust, which supports and campaigns for the rights of children deported from Britain to Australia and other countries; Connecting Home, a Victorian advocacy and support service for Stolen Generations survivors; the CREATE Foundation, a national, peak advocacy organisation representing children and young people in statutory care, and supporting young Care Leavers – and allied research units – the eScholarship Research Centre at the University of Melbourne, and the Collaborative Research Centre in Australian History (CRCAH) at Federation University Australia – to establish the Setting the Record Straight for the Rights of the Child Initiative. In May 2017, the Initiative held a National Summit to set an agenda for recordkeeping advocacy, action and research over the next decade. This participatory design approach (Spinuzzi, 2005) has identified the key elements of a National Framework for Recordkeeping for Childhood Out-of-Home Care and associated strategies to transform legislation, frameworks and resourcing models, theories and practice (Evans, 2017; Reed et al., 2017; Setting the Record Straight for the Rights of the Child Initiative, 2017).

The proposed National Framework for Recordkeeping for Childhood Out-of-Home Care aims to address the “full gamut of identity, memory and accountability needs for all those who experience childhood out-of-home Care” building on the Recordkeeping Principles for...
Child Safe Organisations from the Royal Commission. At its heart is the idea of Independent Lifelong Living Archives as a secure, distributed, participatory recordkeeping network, in which children and young people share in their recordkeeping and have access and control of the records of their childhood experiences throughout their lives.

Rights to agency in recordkeeping is defined through a Charter of Rights in Childhood Recordkeeping in alignment with the UN Convention on the Rights of the Child, and the emphasis on the active participation of children in decision-making that impacts on their lives (FaHCSIA, 2011). It builds on research identifying a more extensive suite of rights in records to address the social injustices embedded in existing archival infrastructures (Gilliland and McKemmish, 2014).

Participatory governance is built into the framework through a Recordkeeping and Rights of the Child Advocacy Body with development, auditing and oversight responsibilities, to oversee the design and implementation of a national cross-jurisdictional, cross-sectoral legislative and policy framework to promote efficient and accountable recordkeeping by all agencies involved in child care services. A Network Governance Model will provide oversight of the technical infrastructure and accountability for the network as a whole.

An integrated transdisciplinary research and development agenda aims to identify, progress, support, evaluate and monitor transformations, including interoperable infrastructure and legal and standards frameworks at state, national and international levels which better accommodate participatory recordkeeping, co-design approaches and multiple rights in records (Evans et al., 2015, 2017). The ultimate goal is to support the development of the Framework by:

[... repositioning of children in out-of-home Care and Care leavers from passive subjects of records owned and controlled by government, Care organizations, and archival collecting institutions, to “active participatory agents” with an extended suite of rights in records and a role in decision-making relating to records of their childhood (McKemmish et al. under review).

A related action and advocacy agenda seeks to embed participatory values and constructs of co-creation and archival autonomy in recordkeeping governance and systems in the sector, and in relevant national and international frameworks, laws and standards. For example, while the 2011 National Standards for Out-of-Home Care (FaHCSIA, 2011) emphasise the meaningful participation of children and young people in decision-making that impacts on their lives, there is little evidence of their participation in contemporary recordkeeping. The inclusion of impacted communities is also recognised in the requirement for Aboriginal and Torres Strait Islander peoples to “be involved in the design, development, implementation, monitoring and evaluation of all programmes, policies and legislation that affects us” (Australian Human Rights Commission, 2010, p. 25).

Current records management frameworks, processes and systems lack the capacity to adequately monitor recordkeeping for the childhood out-of-home Care[3]. A major design challenge is to model participatory recordkeeping governance that can effectively account for recordkeeping practices, not just within organisations, but also across the network of institutions involved in the provision of out-of-home Care. As evidenced by the Royal Commission and other inquiries, the absence of such governance has seen many records fall through the cracks, particularly when responsibilities for childhood Care ceases, organisations exit the sector, government contracting arrangements change and the services within providers are re-configured. At these moments there is little advocacy for the “subject” of the records, and for resourcing of quality records and archives management as part of ensuring continuity of care.
Rights instruments and standards in the sector, and more generally instruments and standards relating to children at global and local levels (for example, in the UN Charter of Child Rights and local rights instruments based on the Charter), often include references to identity, memory and cultural rights; agency or a degree of participation in decision making; and information accessibility as essential requirements. In most cases the recordkeeping requirements to support such rights are not specified. The Royal Commission’s explicit linking of recordkeeping requirements to Child Safe Standards is a rare example. In relation to Indigenous children and children from marginalised ethnic communities, cultural safety is also a major issue. The Royal Commission formed a view, based on research findings, that:

Empirical data now supports the idea that connection to culture is associated with improved emotional, social and physical health for Aboriginal and Torres Strait Islander peoples. Positive cultural connection can increase the protective factors available to Aboriginal and Torres Strait Islander children by helping them to develop their identities, fostering high self-esteem, emotional strength and resilience. Our commissioned research also highlights that positive cultural connection indirectly increases protective factors by supporting the social conditions necessary for all adults in a kinship placement to be available, responsive and protective of children in the community (RCIRCSA, 2017c, p. 327).

Recordkeeping requirements relating to cultural safety have not as yet been established but are being explored by Kirsten Thorpe in her Monash PhD thesis *Culturally Safe Recordkeeping and Archival Places* (McKemmish et al., under review). Another critical challenge is to ensure that the role of quality recordkeeping in governance and accountability is explicitly acknowledged in related sector frameworks, rights instruments and standards. Explicit statement of relevant recordkeeping rights and explanations in implementation guidelines of the recordkeeping requirements associated with various rights and standards instruments in the out-of-home Care sector are essential.

**Information governance in the data age**

As egregious as the inequities inherent in conventional socio-technical recordkeeping systems may be, the emergence of data science and automated decision-making using machine learning models as core planks of systems design is an additional imperative for exploring and adopting participatory information and recordkeeping governance models. The technical characteristics of machine-learning approaches have led to decision-making automation that:

- can manifest at orders of magnitude greater than previous, function-oriented design;
- is essentially inscrutable, resisting easy inspection and explanation of decision-making rationales (though possibly amenable to labour-intensive post-hoc analysis); and
- unchecked, can form tight data/decision/effect/data feedback loops that serve to entrench social biases and inequities (O’Neil, 2017).

Conventional recordkeeping systems can exhibit these characteristics. Those in, or having left Care, are never beyond the reach of the documented surveillance that is often used for control and decision-making beyond the original Care context. For the Care-affected, recordkeeping has an all-encompassing scale, opacity of purpose and utility and can be the source of continual affect and effect over multi-generational timescales (Mendes, 2009; Wilson and Golding, 2016). Nonetheless, the sheer scale, opacity, emergent nature and capacity for negative sociological reinforcement of emerging data-driven technologies
demand additional scrutiny and oversight of their application. The risks and ambiguity inherent in data-science techniques are at odds with the popular, technologically deterministic conception of such automation as “objective”, “comprehensive” or “beyond reproach”. While the phenomenon of “silver bullet” solutions is as old as the industrial revolution (Smith and Marx, 1994), it is surprising how lay-people and professionals alike defer uncritically to application-mediated information or decisions (Van Dijck, 2014). Moreover, the ever-shifting foundations (Stone et al., 2016) of data-driven application necessitate close attention to its governance.

In this section, we address four recordkeeping aspects of the governance of such applications. The first concerns the use of the data that forms the basis of decision-support analysis or visualisation in general, or the training of automated decision-making models. These data – or, rather, these records (as they must constitute authoritative records or they would not be useful as the basis for decision-making) – need to be obtained in an ethical manner. There are real questions about the transparency of both the collection of data and the downstream uses to which it may be put. Governance in this context involves not only demonstrable mechanisms that ensure the free and prior consent for the collection and use of data in recordkeeping systems, but also participation in systems development and use. Without such governance, we are left with a recordkeeping landscape reminiscent of a totalitarian surveillance state; moving through essentially unregulated cyberspace, never knowing what is being recorded, accessed and used, or who is informing about our movements, transactions, and expressions (Wolle and Selwyn, 1992). The shift of surveillance technology from the state to the private sector has sharpened this discourse (Van Dijck, 2014) and altered notions of privacy and the possibility of individual and collective consent to the collection of data.

The shift becomes more problematic when coupled with the outsourcing of service and IT provision as is the case in the out-of-home Care sector, and particularly to those with for-profit motivations and obligations. Regulatory frameworks do not manage service delivery recordkeeping or data management well – particularly where authority and decision-making has been delegated to either a human agent or automated application (Carney, 2018; Dickerson, 2018; Powles and Hodson, 2017). Nonetheless, some jurisdictions are addressing these challenges. For example, the European GDPR (European Commission, 2018) legislation is an attempt to shift power back to the subjects of records and propose new contours of privacy. However, such regulation focuses on generalised notions of privacy and the treatment of data as a resource for exploitation. This treatment glosses over individual and collective evidence, identity, memory and accountability affordances of recordkeeping and the ways these data could systemically be used adversely for documented people. Concern over “consumer rights” over data (NTIA, 2018) misses the point of the role that records play in a wide range of rights. Governance must involve mechanisms of proactive disclosure of collection and use, even if this happens at some distanciation spatially or temporally from the activity of participants.

This governance is applicable not only within the public and private sectors where much of the data gathering takes place but also to research institutions where investigation of data-driven techniques cannot happen in a data-vacuum. Sufficient recordkeeping regarding the use of data beyond its immediate transaction utility is essential for accountability in the child protection sector – especially where it is used for research purposes (Wilson et al., 2018). This accountability is further complicated by the gathering of information without an explicit use in mind, acknowledging the emergent application of data science. Such purposeless data gathering is difficult to protect through regulation. Nonetheless,
governance in the research context needs to make explicit the processes for proactive disclosure and participation.

The second aspect to be considered is the problem of bias (Eubanks, 2018; O’Neil, 2017). An obvious source derives from the automation of sociotechnical systems. If one goal of data-driven analysis and decision-making (often with an economic/efficiency rationale) is its “objectification”, then how are “good” decision-making cases identified from the body of historical data? Information governance must include the critical analysis (Evans et al., 2017) of the end-to-end sociotechnical system that is being improved and acknowledgment of flaws, biases, and long-term affect. If not, there is the danger of simply redoubling the problems.

Another, more subtle reason for this bias is the limitations of datafication (Van Dijck, 2014). Not every facet of a given application domain is amenable to measurement and/or recording. Data science, therefore, must rely on proxy measures of aspects of human behaviour – for example, using residential location as a proxy for economic risk. Such proxies can exhibit more or less nuanced and hidden biases. In fact, one must be particularly diligent about data features to ensure they are not proxies for proscribed decision-making – e.g. race, age, gender, marital status and so on. For example, Eubanks has shown how the measurement proxies used for the automation of child protection assessment in Allegheny County in the USA exhibit bias against those families already documented in the system – assessments that are at odds with actual observations by caseworkers. Furthermore, she concludes that “the activity that introduces the most racial bias into the system is the very way the model defines maltreatment” (Eubanks, 2018, p. 255) (Author’s emphasis).

Additionally, techniques that limit input into decision-making to only that which can be routinely or automatically captured and quantified decreases the possibility of participation and self-determination, increasing the possibility of the tight feedback loops described above. For example, a loan decision-based on credit score and other collated data may lead to increased and entrenched poor economic circumstances, which may, in turn, inform future welfare, housing and employment prospects (O’Neil, 2017, p. 149). Information governance must identify the limitations and potential biases of datafication, making explicit what is not being taken into account in the new system.

A third aspect of information governance is the imperative to subject the end-to-end development, deployment and maintenance of data-driven applications to formal oversight and active governance. If un-biased training data can be ethically obtained and refined for a given application, any proposed data-driven application must be demonstrably fit-for-purpose, exhibiting both efficacy and minimal adverse side effects across space and through time. As with other regulated enterprises, this involves the consideration of benefit and affect beyond the immediate transactional context to make explicit the through-time consequences of its use. It requires multiple phases of testing from a variety of participant perspectives together with critical analysis of test results and comprehensive recordkeeping of the development process.

Thereafter, the deployment and ongoing use must be monitored through time to ensure that the application remains within pre-established bounds of tested-for contexts and that any emergent deleterious impacts are identified and amended. Data-driven applications are inherently brittle with respect to changing use contexts (Marcus, 2018). The risk of unforeseen biases and socio-technical feedback or the drift of the domain with respect to the application model because of external economic, societal or other structural change (Tsymbal, 2004) means that such systems must be subject to ongoing scrutiny.

The final aspect is the use of data science techniques in recordkeeping governance itself. This may seem circular; however, it is difficult to conceive of any information system that
does not need to provide authoritative recordkeeping for at least one stakeholder in some context. Importantly, this explosion of heterogeneous diversity in recordkeeping has become another “wild frontier” (McDonald, 1995); decentralised and fractured; and subject to pressures that include increasing data volumes, reliance on commercial and propriety systems and evolving forms of records and formats (Cumming and Picot, 2014).

Faced with dealing with this maelstrom of data, we must trust that “innovative techniques for mining, recovering, and reusing digital materials and their traces” (Gilliland, 2014) may eventually be found to separate out the good oil of meaningful records from vast quantities of information sludge (Upward et al., 2017, pp. 19-20). The use of data-science techniques for the creation, capture, organisation and pluralisation of authoritative records has commenced and is subject to the same biases, limitations and risks as any other data-driven system. Therefore, recordkeeping itself must embrace all of the foregoing governance as well. Put simply, without appropriate oversight (and automation techniques), we will drown in the sludge.

Information governance in the twenty first century means confronting the biases, datafication and, perhaps, blind faith in provenance and authority that has led recordkeeping systems and the records they contain to become weapons of affect for marginalised communities (Wilson and Golding, 2016). Governance must involve the equitable participation of all parties in the design of recordkeeping frameworks that have the potential to affect their lives.

Conclusion
In Australia, the only national or state-level recordkeeping frameworks established in legislation and standards lie within the government or corporate sectors. There are no holistic, pluralising recordkeeping frameworks for contemporary or historical recordkeeping. We have argued in this paper and elsewhere (Evans et al., 2017) that government and corporate recordkeeping privileges the needs of the singular creator of the records and information elites, and that recordkeeping processes are driven by and designed for the operational needs of government agencies and business organisations. Community advocacy groups representing the “subjects” of recordkeeping have not as yet been invited to participate in the development of standards at national or international levels. Nor has their development or recordkeeping and archival law reform as yet been informed by human rights and social justice frameworks and instruments, the testimony of the “subjects” of recordkeeping in a number of sectors including child welfare, the findings of royal commissions and inquiries based on that testimony, extensive engagement with stakeholder communities and research findings.

Values and principles that could inform the development of recordkeeping governance frameworks for participatory recordkeeping that fit UNESCO’s definition of governance quoted earlier in this paper include:

- enabling pluralisation in recordkeeping that facilitates self-determination as defined in UN instruments relating to human rights, child rights and the rights of Indigenous peoples;
- embracing Hurley’s concepts of co-creation, multiple simultaneous provenance and parallel provenance (Hurley, 2006a, 2005b) and Evans, McKemmish, Daniels and McCarthy’s (2015) concept of archival autonomy;
- prioritising the lifelong identity, memory, accountability and cultural recordkeeping needs of those whose lived experience is captured by recordkeeping processes;
prioritising the recordkeeping requirements of those who have been the victims of human rights abuse and social injustice;

valuing the long term and affective functions of recordkeeping rather than focussing mostly on transactional and operational utility; and

designing flexible, rights-based and person-centred recordkeeping, recognising that one-size-does-not-fit-all.

Embedding these principles and requirements in governance frameworks is a vital step towards participatory recordkeeping that can fully address the lifelong identity, memory and accountability needs for childhood out-of-home Care.

Notes

1. Child welfare in Australia has a long history of involving a range of providers – government, non-government, commercial, private and faith based organisations running orphanages, children’s Homes, other institutions and administering foster and other alternate care services.

2. Authors Evans and McKemmish were both directly involved in the development of ISO recordkeeping standards, particularly metadata standards. As we have become more engaged with participatory, community-centred research, we have reflected critically on the issues raised here about the development and content of global standards in the field.

3. An example is the 2015 investigation by Victoria’s Commissioner for Children and Young People into the adequacy of responses to sexual abuse or exploitation in residential care services (Commission for Children and Young People, 2015). The inquiry’s file audit found little to no evidence of the raising, progress or status of quality of care investigations in the case files reviewed, and other major deficiencies in currency and quality of recordkeeping.


References


Corresponding author
Joanne Evans can be contacted at: joanne.evans@monash.edu

For instructions on how to order reprints of this article, please visit our website:
www.emeraldgrouppublishing.com/licensing/reprints.htm
Or contact us for further details: permissions@emeraldinsight.com
Balancing information governance obligations when accessing social care data for collaborative research

Malkiat Thiarai, Sarunkorn Chotvijit and Stephen Jarvis

Department of Computer Science, University of Warwick, Coventry, UK

Abstract

Purpose – There is significant national interest in tackling issues surrounding the needs of vulnerable children and adults. This paper aims to argue that much value can be gained from the application of new data-analytic approaches to assist with the care provided to vulnerable children. This paper highlights the ethical and information governance issues raised in the development of a research project that sought to access and analyse children’s social care data.

Design/methodology/approach – The paper documents the process involved in identifying, accessing and using data held in Birmingham City Council’s social care system for collaborative research with a partner organisation. This includes identifying the data, its structure and format; understanding the Data Protection Act 1998 and 2018 (DPA) exemptions that are relevant to ensure that legal obligations are met; data security and access management; the ethical and governance approval process.

Findings – The findings will include approaches to understanding the data, its structure and accessibility tasks involved in addressing ethical and legal obligations and requirements of the ethical and governance processes.

Originality/value – The aim of this research is to highlight the potential use of use new data-analytic techniques to examine the flow of children’s social care data from referral, through the assessment process, to the resulting service provision. Data held by Birmingham City Council are used throughout, and this paper highlights key ethical and information governance issues which were addressed in preparing and conducting the research. The findings provide insight for other data-led studies of a similar nature.

Keywords Public sector, Ethics, Governance, Information management, Legislation

Paper type Case study

Introduction

Researchers wanting to work with or use personal data within their research will be familiar with the requirement to ensure that the use of the data meets both legal and ethical standards. In support of these requirements, there are established legal and ethical frameworks within which research using personal data must be conducted.
In the UK, the Data Protection Act 2018 (which repealed the Data Protection Act 1998 in May 2018) is the principal piece of legislation governing the use of personal data. Several additional sources of guidance and good practice are available for researchers in the UK, including the UKRIO Code of Practice for Research: Promoting good practice and preventing misconduct (UKRIO, 2009) and the RCUK Policy and Guidelines on Governance of Good Research Conduct (RCUK, 2013) that set out key principles to effective research governance.

Background
The data associated with this research project is held by Birmingham City Council and are recorded as part of the Council’s statutory duty to provide social services for a “child in need”: This term is statutory and is defined in the Children Act 1989 (the “1989 Act”). Any child can be a “child in need”, even if they are living with their family. A child is someone who is under 18 years of age.

There is no need for a court order to be made for a child to be deemed in need. It is the role of a local authority’s children’s services department to assess and provide services in this regard. Being a child in need is therefore broader than just those children in local authority care further to a care order, or those provided with accommodation by the local authority under section 20 of the 1989 Act.

Section 17 of the 1989 Act defines a child in need as follows:

• He is unlikely to achieve or maintain, or to have the opportunity of achieving or maintaining, a reasonable standard of health or development without the provision for him of services by a local authority under this Part.
• His health or development is likely to be significantly impaired, or further impaired, without the provision for him of such services.
• He is disabled.

Under the 1989 Act, “every local authority shall take reasonable steps to identify the extent to which there are children in need within their area”, as well as to publish information about the services it provides to children in need (and other groups) and to “take such steps as are reasonably practicable to ensure that those who might benefit from the services receive the information relevant to them”.

In addition to the services that local authorities provide for all children, the 1989 Act specifies the range of services that can be made available for a child in need:

• advice, guidance and counselling;
• occupational, social, cultural, or recreational activities;
• home help (which may include laundry facilities);
• facilities for, or assistance with, travelling to and from home for the purpose of taking advantage of any other service provided under the 1989 Act or of any similar service;
• assistance to enable the child concerned and his family to have a holiday;
• maintenance of the family home if the child is in need (but is not a looked after child) and is living apart from their family to either to enable the child to live with their family, or to promote contact between the child and their family;
• day care if the child is under 5 years of age but is not yet attending school;
• care or supervised activities (either outside school hours or during school holidays) for a child attending any school; and
• providing accommodation to a child and their family.
Consequently, the depth, breadth and sensitivity of data that may be recorded as a result of a local authority carrying out its statutory functions are significant. The volume of data is likely to be much greater than that collected either from an adult receiving social care services or an individual receiving health or healthcare services. A further distinction in the recording of children’s data is likely to be the absence of consent for the collection, use and processing of the data given the statutory obligations imposed upon the local authority.

An international review by Deloitte (2016) into the “Secondary use of health and social care data and applicable legislation” found that across the six countries reviewed (England, Netherlands, New Zealand, Israel, Canada and Australia), all had started to recognise the value of collected health records, but that there is no separate legislation for secondary use of health and social care data in any of these countries, rather privacy laws in each country defined how the personal health and social care records can be used.

It is important for organisations to have clarity as to the legal basis for processing personal data. Where legal obligations are being fulfilled then the basis for processing is provided. Changes to EU law following the introduction of the General Data Protection Regulation (GDPR) in 2016 (EUR-Lex, 2016) have provided for a higher standard for consent compared to previous legislation. It requires that, where there is a requirement for consent, an indication of consent must be unambiguous and involve clear affirmative action and furthermore, be able to be withdrawn at any time.

The GDPR requires that there should be distinct (“granular”) consent options for distinct processing operations. It could be argued, therefore, that processing data for research purposes is a distinct processing operation, separate from the original purpose for which the data was collected and, as such, the relevant obligations would apply.

The Information Commissioner’s Office’s (ICO) guidance on “consent” concludes:

Consent is one lawful basis for processing, but there are alternatives. Consent is not inherently better or more important than these alternatives. If consent is difficult, you should consider using an alternative.

As such, an early determination in this research was that the basis on which the data could be processed for research purposes as set out in Section 33 of the Data Protection Act (DPA) 1998. The DPA 1998 does not define “research”. The ordinary meaning of “research” is therefore used when determining whether personal data is being processed for research purposes – research is a systematic investigation intended to establish facts, acquire new knowledge and reach new conclusions.

Section 33 of the DPA makes it clear that “research purposes” includes statistical and/or historical research:

(1) “research purposes” includes statistical or historical purposes; “the relevant conditions”, in relation to any processing of personal data, means the conditions:

• that the data are not processed to support measures or decisions with respect to particular individuals; and

• that the data are not processed in such a way that substantial damage or substantial distress is, or is likely to be, caused to any data subject.

(2) For the purposes of the second data protection principle, the further processing of personal data only for research purposes in compliance with the relevant conditions is not to be regarded as incompatible with the purposes for which they were obtained.

There are, however, several challenges that researchers face in understanding the social care data they wish to utilise as well as adhering to a range of different guidance, whether on governance or ethics, issued across the sector.
First, there is a plethora of sector and professional specific guidance that provides a framework that those working with social care data need to follow. Examples include:

1. The Department of Health (2010) resource pack, which is designed to support the implementation in social care of the DH Research Governance Framework. The Framework contains information, guidance and a range of resources for supporting research governance and is primarily aimed at those involved in setting up and running governance systems in local authorities or for people who take part in the review of relevant research.

2. The Information Governance Review (Caldicott, 2013) concluded, as part as its review that accredited safe havens should be required to meet requirements for data stewardship that included:
   - Robust governance arrangements that include, but are not limited to, policies on ethics, technical competence, publication, limited disclosure/access, regular review process and a business continuity plan including disaster recovery.
   - Clear conditions for hosting researchers and other investigators who wish to use the safe haven.

3. The Department for Children and Youth Affairs in Ireland published specific guidance on research involving children, in part driven by the principles of the United Nations Convention of the Rights of the Child, in particular Articles 2, 3, 4 and 6. The guidance, recognising that there was no single regulatory system and no body responsible for research ethics in the country, set out a number of core ethical principles and concepts that needed to be followed by all those who carry our research with, and for, children in Ireland.

4. The International Medical Informatics Association developed and published a distinct code of ethics for health information professionals, individuals who, in their professional capacity, provide health informatics services, arguing that they play a unique role and occupy a unique position that is distinct from that of informatics professionals who do not specialise in health care data and who do not work in the health care setting.

The Archives and Records Association published a Code of Ethics setting out the standards of professional behaviour expected of archivists, archive conservators, records managers and those occupied in related activities who are individual members of the association (Archives and Records Association, 2018).

These examples of ethical and governance practices within different sectors and organisations reflect the views of the UK ICO, who noted in the paper on “Big data, artificial intelligence, machine learning and data protection” when discussing the ethical approaches emerging in the field of data protection that it was:

Notable that these ethical frameworks have been developed not by regulators but by companies and other organisations themselves.

A further example of an organisation developing its own approach is that of the Nuffield Foundation where the Trustees have decided to establish the Nuffield Family Justice Observatory (Broadhurst et al., 2018). The aim of the Observatory is to support the best possible decisions for children by improving the use of data and research evidence in the family justice system in England and Wales. This work is also linked to the Children in Family Justice Data Share (Ministry of Justice, 2019), a collaborative project that has resulted in a database of child data linked from across the Ministry of Justice (MoJ), the
Department for Education (DfE) and Cafcass’ management information systems. The MoJ’s report into this project includes a reflection on the “significant legal issues to overcome in relation to compliance with the DPA” and whilst a formal agreement to share the data was established, challenges remain, not least the unforeseen technical issues associated with IT infrastructures.

Nevertheless, many aspects of these frameworks echo key data protection principles and demonstrate the strong link between these ethical approaches and data protection law.

**Ethical considerations**

The EU Data Protection Directive of 1995 made no mention of a human right to data protection. In contrast, the General Data Protection Regulation (GDPR) is framed in terms of rights, with the protection of “fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data” set out in Article 1 of the Regulation.

Furthermore, with the enactment of the Lisbon Treaty, the Charter of Fundamental Rights of the European Union in 2009 saw, for the first time, a stand-alone fundamental right to data protection. The significance of this right is discussed by McDermott (2017), examining the parameters of this right and its links to key values of privacy, transparency, autonomy and non-discrimination in other legal European statutes.

The opinion of the European Data Protection Supervisor (2015), called for a four-tier “big data protection ecosystem” to respond to the digital challenge requiring a collective effort, underpinned by ethical considerations. The proposed ecosystem encompassed:

- **Future-oriented regulation**: urging simpler rules for handling of personal data which stay relevant for a generation.
- **Accountable controllers**: putting in place internal policies and control systems that ensure compliance and provide relevant evidence.
- **Privacy conscious engineering**: empowering individuals who wish to preserve their privacy and freedom through anonymity.
- **Empowered individuals**: focussed on a “prosumer” environment, consent and control and data ownership.

The opinion called for dignity to be at the heart of new digital ethics arguing that “better respect for, and the safeguarding of, human dignity could be the counterweight to the pervasive surveillance and asymmetry of power which now confronts the individual”.

In its submission to the Select Committee on Artificial Intelligence (AI), the ICO commented that:

Despite robust data protection compliance, the law only takes us so far. We believe that it can be highly challenging to apply certain data protection concepts such as fairness and relevance to advanced AI applications. For example, empathic computing involves the use of AI to examine an individuals’ on-line behaviour. It considers the vocabulary individuals use, the way they input type and the pictures they look at longest to assess that individual’s mood and deliver content accordingly.

This certainly involves the processing of personal data and therefore engages data protection law. However, whilst the pure data protection compliance aspects of using AI in empathic computing and other contexts can be addressed using the compliance steps outlined in the annex, the use of AI raises wider ethical issues of significant public interest.

The range of problems to be found in the practical use of social care data are explored in Gillingham and Graham’s paper (Gillingham and Graham, 2017) that highlights issues such as data integrity, subjectivity in decision making at the recording stage and hidden biases.

Furthermore, the paper considers the impact of the extracted data if it is rendered
meaningless because of removing it from the system as well as the fact that narrative accounts or in-depth social explanations of complex problems being lost or replaced by simpler descriptions.

The paper also highlights several ethical concerns with consent to use personal data being one and confidentiality being another. In the context of children’s social care data, as explained above, the basis for collecting the data is to meet statutory obligations, so consent at data collection stage is not the issue. One ethical issue is whether the statutory obligations extend to other uses, such as research, which from a legal perspective would be considered a compatible purpose.

Accessing data for research purposes also raises issues of the quality of the data and the methods for records management in the curation of the data for research, particularly, where it is for a secondary purpose.

A review of “Digital records management in Australian government” suggests that the basic tenets for records management – create, capture, manage, access, secure, describe and dispose – remain the same, the methods seem to have stagnated and that the method for how we keep and manage records needs to be adjusted for digital times (Stuart, 2017; Maroye et al., 2017).

The challenges in utilising data obtained in the course of child social work or welfare provision is discussed in Naccarato’s paper on Child Welfare Informatics (Naccarato, 2010). It proposes the possible evolution of this topic as a sub-speciality in social work, highlighting that “concerns exist as the discipline has ties to face-to-face interactions and there is a minimal amount of time available for practitioners and policy makers to focus on data-related needs” whilst at the same time needing to protect and manage sensitive information and data linking capabilities.

The ethical challenges posed by “Big Data” are also discussed in the Metcalf and Crawford paper (Metcalf and Crawford, 2016) on the emerging ethics divide. The paper argues that big data is stretching the concept of ethical research and that existing ethical regulations promote a particular approach towards “research subjectivity” that is being eroded by data science. Further, it suggests that the traditional concept of a “human research subject”, that is, what constitutes an intervention, when and how consent should occur and what types of harm are relevant, are out of step with large-scale data practices. The paper questions, “Who is the data subject in a large scale data experiment and what are they owed?”

The Metcalf and Crawford paper offers a preliminary examination of how critical data studies may generate a theory of data subjectivity, to enable responsible scientific practice with Big Data methods and thereby address some of the ethical issues that exist and avoid the human subject becoming invisible or irrelevant to data science.

Organisational approaches/controls
The Royal Society and British Academy’s report Data management and use: Governance in the 21st Century (The Royal Society, 2017) addressed the changing data landscape, recommending a principled approach to data governance and calling for stewardship of the entire data governance landscape. The Academies hosted a seminar to explore the priorities across sectors for such a stewardship body. Discussions at which, set out governance needs, practical challenges and conceptual concerns that any such a body could take on.

The UK Government announced in its budget statement on 22 November 2017 the creation of a new Centre for Data Ethics and Innovation (The Royal Society, 2017) to enable and ensure safe, ethical and ground-breaking innovation in AI and data-driven technologies.

Training needs have been expressed, for example, the introduction of ethical thinking at the core of and during the continuing education of all professionals, so that they can develop
the necessary analytical tools to respond to ethical situations as and when they arise (Lacovino, 2002). It is also argued that codes should be used to focus on professional duties and virtues and as a collective consensus of professional values.

Organisations are also investing in and implementing internal control systems which include a set of elements such as integrity and ethical values (Rubino et al., 2017). This reflects changing attitudes in management in the field of data control and this can, and perhaps should, shape the way data is viewed as part of the overall control objective.

Design/methodology/approach
This paper discusses the approaches taken to identify and obtain approval for the use of social care data for a research project titled “Data continuity analysis of the assessment process in children’s social care” within Birmingham City Council and the steps taken to demonstrate compliance with legal and ethical frameworks.

The city of Birmingham is the UK’s largest and most populous city outside of London. Birmingham has a population of over 1.1 million people, and the population is growing faster than the UK average. Birmingham is a young and diverse city; half of the population are aged 30 or under. It is the sixth most deprived local authority in the UK; 40 per cent of the city is ranked in the most deprived 10 per cent of areas in England. There are significant levels of child poverty; 30 per cent of the city’s children live in a deprived household.

Birmingham City Council (BCC) is the largest local authority in Europe. Income and expenditure in 2016/17 was £3.094bn, of which £782m was spent on schools, £550m spent on benefits, £805m spent on services for people and £287m spent on housing (Birmingham City Council, 2016). Managing BCC’s priorities has been difficult in the context of recent fiscal challenges. Birmingham City Council is expected to make total savings of £815m over the 9 year period 2011/12 to 2019/20.

The most recent Ofsted inspection report (Ofsted, 2016) for Birmingham City Council showed that at 31 August 2016, 1,816 children were being cared for by the local authority (a rate of 64 per 10,000 children); this is similar to that seen in March 2015 (also 64 per 10,000 children).

Methodology
The research seeks to use data analytic methods to examine the flow of children’s social care data from referral through the assessment process to the resulting service provision. In this example, the research is collaboration between a UK local authority and an UK University. The methodology used to address the information governance and ethical issues aims to balance the respective obligations of the partner organisations. For example, accessing the proposed dataset for research purposes for the local authority represents a secondary use of data that is deemed to be compatible with the original purpose for which the data was obtained. For the University, however, the data is being processed for the primary purpose of research.

The determination that s33 of the DPA is the appropriate gateway for the legitimate use of the data for research purposes means that adhering to the “relevant conditions” must be met throughout the whole life of the data. It also informs partner organisations at the onset of the research of these conditions and the subsequent limits imposed on the use of the data.

As such, each party needs to document and demonstrate to the other how they meet these respective obligations. Using this research as an example, the Table I shows a series of activities undertaken and by whom to demonstrate compliance with the information governance and ethical requirements.
The key components within the methodology are the initial research governance application within the Local Authority (Data Custodian) and the ethical review process within the University (Collaboration partner) as they establish the boundaries for the research partners in meeting their respective obligations. Both organisations required appropriate training to be undertaken.

For the research governance application, this incorporates outlining the legal framework and setting out the scope and structure of the data. The ethical review process allows for the collaboration partner to assess the research proposal in the context of their own organisational frameworks. How these respective obligations are managed are discussed in further detail below.

Legal framework
As highlighted above, the Data Protection Act is the principal piece of UK legislation governing the use of personal data. The application for ethical approval was in progress as this legislation was being amended because of the General Data Protection Regulation (Regulation GDP, 2016).

However, both the 1998 and 2018 Data Protection Acts (The National Archives, 2018) make provisions for research.

This exemption can apply if you process personal data for:

- scientific or historical research purposes; or
- statistical purposes.

It does not apply to the processing of personal data for commercial research purposes such as market research or customer satisfaction surveys. It exempts you from the GDPR’s provisions on:

- the right of access;
- the right to rectification;
- the right to restrict processing; and
- the right to object.

### Table I.
Data custodian and collaboration partner activity

<table>
<thead>
<tr>
<th>Steps</th>
<th>Data custodian activity</th>
<th>Joint activity</th>
<th>Collaboration partner activity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Research governance application</td>
<td>Collaboration agreement</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td></td>
<td>Training in data ethics and governance</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td></td>
<td>Ethical review and questions</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>Ethical approval application</td>
<td>Data sharing agreement</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td></td>
<td>Data receipt and security measures applied</td>
<td></td>
</tr>
<tr>
<td>Step 6</td>
<td>Additional information provided</td>
<td>Data retention for research purposes</td>
<td></td>
</tr>
<tr>
<td>Step 7</td>
<td></td>
<td>Ongoing monitoring</td>
<td></td>
</tr>
</tbody>
</table>

Social care data for collaborative research
The GDPR also provides exceptions from its provisions on the right to be informed (for indirectly collected data) and the right to erasure. However, the exemption and the exceptions only apply:

- To the extent that complying with the provisions above would prevent or seriously impair the achievement of the purposes for processing.
- If the processing is subject to appropriate safeguards for individuals’ rights and freedoms (see Article 89(1) of the GDPR – among other things, you must implement data minimisation measures).
- If the processing is not likely to cause substantial damage or substantial distress to an individual.
- If the processing is not used for measures or decisions about particular individuals, except for approved medical research.
- As regards the right of access, the research results are not made available in a way that identifies individuals.

There are some notable changes in the new laws that it is important to consider when using data for research purposes. First, the GDPR requires that “technical and organisational measures” are put in place to ensure that data controllers process only the personal data necessary for the research purposes, in accordance with the principle of data minimisation outlined in Article 5(c). In addition, Recital 33 states that controllers should act “in keeping with recognised ethical standards for scientific research”. Whilst not elaborating any further on what those recognised ethical standards are, the Regulation makes the linkage between research and ethical re-use of personal data. Furthermore, GDPR Article 89(1) specifically references the use of “pseudonymisation” as a method by which a data controller could comply with the mandate for technical and organisational measures obligations.

Understanding the structure of the data

One of the first tasks in preparing the research governance application was to understand the nature of the data held, its format and structure. The data required in this case are primarily collected and stored to support the Local Authority’s social care case management. As Best (1990) sets out, there are challenges in utilising information that has been collected for a specific purpose in a related level of the organisation and its subsequent re-use for a secondary purpose within another level of the organisation.

To access this data, several meetings took place with Local Authority employees who had detailed technical knowledge of the system, the structure of the data and the changes that had occurred over time (whether technical, legislative or organisational) that impacted the way the data was recorded and categorised. Data was extracted using an Open Database Connectivity (ODBC) connection through Crystal Reports, which is the application in use in the Local Authority. A series of extracts were produced, and the data was then joined together using IDEA (Data Analysis and Extraction) software. The information generated was validated throughout and checked against the live application to prove its integrity.

As Gillingham and Graham (2017) highlight, data extraction presents one of the key ethical challenges in converting data into a suitable form for re-use. Notably, big data requires that the “raw data” is available in a format that is better suited to statistical analysis and computation. The problem with this process, as their paper points out, is that the decisions taken at this stage may not only affect the research but may also be invisible in the findings. This is true to some degree here, in that to understand the structure of the data,
we are reliant on the knowledge and expertise of those familiar with the technology to be able to describe what data is held and the relationships between different data types.

The data

The data extract is of administrative data related to the social care assessment and agreement process (Table II).

Assessment data details the flow of information through the system of a referral to Children’s Social Care and the outputs from this process. Agreement data details those referrals that result in an “agreement” which relates to a service that is subsequently provided to the child.

The data are pseudonymised prior to its release to the researchers. Individual names are removed, however, the “Person Identifier”, which is key to making the data identifiable, is retained. This is to allow for analysis of the data and the number of unique individuals receiving the services. The importance of this level of detail in the research governance application cannot be overstated. This establishes both the intent of the research but also the risks posed to those individuals whose data is the subject of research. For example, retention of the full postcode will allow for much more granular analysis of the data at a geographical level but loss or unauthorised access to the data could allow for the identification of the individual possibly causing substantial damage or substantial distress to any data subject, thereby contravening one of the “relevant conditions” in s33 DPA that established to legal basis for the research.

Ethical approval process

The ethical approval process at our collaborating university requires all those involved in delivering, supervising, or supporting research (whether staff, students and/or their supervisors)

<table>
<thead>
<tr>
<th>Record</th>
<th>Description</th>
<th>Assessment</th>
<th>Agreement</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASM_ID</td>
<td>Assessment Identifier</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>PERID</td>
<td>Person Identifier</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>DOB</td>
<td>Date of birth</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>AGREEMENT_START</td>
<td>Start date of the agreement</td>
<td>–</td>
<td>X</td>
</tr>
<tr>
<td>AGREEMENT_END</td>
<td>End date of the agreement</td>
<td>–</td>
<td>X</td>
</tr>
<tr>
<td>ASSESSMENT_START</td>
<td>Start date of the assessment</td>
<td>X</td>
<td>–</td>
</tr>
<tr>
<td>ASSESSMENT_END</td>
<td>End date of the assessment</td>
<td>X</td>
<td>–</td>
</tr>
<tr>
<td>SERVICE</td>
<td>Alphanumeric coding of the service</td>
<td>–</td>
<td>X</td>
</tr>
<tr>
<td>SERVICE_DESCRIPTION</td>
<td>Description of the service</td>
<td>–</td>
<td>X</td>
</tr>
<tr>
<td>ELEMENT</td>
<td>Alphanumeric coding of the element</td>
<td>–</td>
<td>X</td>
</tr>
<tr>
<td>ELEMENT_DESCRIPTION</td>
<td>Description of the element</td>
<td>–</td>
<td>X</td>
</tr>
<tr>
<td>QSA_DESCRIPTION</td>
<td>Quality standard assessment process description</td>
<td>X</td>
<td>–</td>
</tr>
<tr>
<td>QSA_GROUP</td>
<td>Quality standard assessment process group</td>
<td>X</td>
<td>–</td>
</tr>
<tr>
<td>ASSESSMENT_REASON</td>
<td>Reason of taking assessment</td>
<td>X</td>
<td>–</td>
</tr>
<tr>
<td>FORM_OUTCOME</td>
<td>Outcome of assessment form</td>
<td>X</td>
<td>–</td>
</tr>
<tr>
<td>SERVICE_TEAM</td>
<td>Corresponding assessment team</td>
<td>X</td>
<td>–</td>
</tr>
<tr>
<td>SERVICE/ELEMENT_COST</td>
<td>Cost of service/element where available</td>
<td>–</td>
<td>X</td>
</tr>
<tr>
<td>POSTCODE</td>
<td>Postcode (unit level)</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>GENDER</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>ETHNICITY</td>
<td>Ethnic classification</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>CLIENT_GROUP</td>
<td>Disability status</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>WARD</td>
<td>X</td>
<td>–</td>
<td></td>
</tr>
<tr>
<td>CONSTITUENCY</td>
<td></td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>

Table II. Administrative data fields for social care assessment and agreement extraction
and research support staff (technical and administrative), to complete data governance and research ethics training.

Scrutiny with regard to research ethics and governance is undertaken for each individual research project. If ethical approval is required, this involves completion of an application form and a supporting protocol. The protocol includes two mandatory fields for completion, one of which is the Ethical Considerations, which as a minimum, should contain subsections examining Informed Consent, and Participant Confidentiality and Data Security.

It should be noted that in the application for ethical approval, confirmation was required that the research was “limited to the use of previously collected identifiable data” which was reflective of the whole data held in the social care system.

The data selected were solely to support the aims of the research, which is to understand the flow of data through the assessment process and identify any temporal or spatial analysis, errors, data quality issues or other patterns in the data that may inform current practice and processes.

Data analysis was to focus on the aggregate number of users. Using Excel, R, Python and spatial mapping tools including QGIS, the research sought to generate results that showed:

- service assessments/agreements over time;
- service assessments/agreements by time and by postcode district;
- number and type of assessments/agreements at different stages in the assessment/agreement workflow;
- analysis of assessments/agreements by user type, including age group, gender, ethnicity and disability, and by commissioning team; and
- an assessment of how this analysis might support Council priorities.

This level of detail is an important component in a collaborative research environment as it provides the collaboration partner with background information as to the origin of the data, its structure, how it will be accessed and the how the data will be manipulated.

Information governance issues
The review of the submitted ethical application resulted in several information governance issues requiring further clarification ranging from queries on:

- data minimisation;
- data security;
- damage and distress to data subjects;
- data loss;
- data sharing; and
- data retention.

In reflecting on the information governance issues raised by the reviewers in respect to this ethical application, it is interesting to note that the nature of the issues raised equate to those that the ICO included in their consultation document on what should be considered, assessed and addressed as part of a Data Protection Impact Assessment (DPIA).

This process involves assessing the necessity and proportionality of research plans to achieve its stated purpose, including:

- your lawful basis for the processing;
- how you will prevent function creep;
• how you intend to ensure data quality;
• how you intend to ensure data minimisation;
• how you intend to provide privacy information to individuals;
• how you implement and support individuals rights;
• measures to ensure your processors comply; and
• safeguards for international transfers.

The next stage of the process required the identification and assessment of risks where consideration of the potential impact on individuals and any harm or damage that might be caused by the processing – whether physical, emotional or material. The assessment considered whether the processing would possibly contribute to:

• inability to exercise rights (including but not limited to privacy rights);
• inability to access services or opportunities;
• loss of control over the use of personal data;
• discrimination;
• identity theft or fraud;
• financial loss;
• reputational damage;
• physical harm;
• loss of confidentiality;
• re-identification of pseudonymised data; and
• any other significant economic or social disadvantage.

The third step required how to identify mitigating measures to the risks identified. For example:

• deciding not to collect certain types of data;
• reducing the scope of the processing;
• reducing retention periods;
• taking additional technological security measures;
• training staff to ensure risks are anticipated and managed;
• anonymising or pseudonymising data where possible;
• writing internal guidance or processes to avoid risks;
• adding a human element to review automated decisions;
• using a different technology;
• putting clear data sharing agreements into place;
• making changes to privacy notices;
• offering individuals, the chance to opt out where appropriate; and
• implementing new systems to help individuals to exercise their rights.

Many of these issues would now be captured by a DPIA, in particular in relation to detailed assessment of the mitigation of risks and harm to individuals and addressed this at an earlier stage.
Conclusions and recommendations

In setting out the experience of preparing, submitting and gaining approval for research using social care data, this paper seeks to highlight some of the key issues identified in this process and their relationship with current legal processes and requirements. These include, understanding and demonstrating the key legal basis for accessing the data for the purposes of processing it for research, understanding the structure of the data, how it can be extracted and the way it needs to be secured, navigating through the ethical approval process and responding to the issues raised by the reviewers of the application.

The information governance issues raised by the reviewers of the ethical application demonstrate consistency between the Council and the university collaborators and the level of scrutiny provided by each was extremely supportive to the research team involved.

The frameworks and structure for the ethical use of social care data continues to be developed and the challenges highlighted may in part be addressed not just through sector specific frameworks but through the approaches organisations take to the capture, use and re-use of data as part of their wider control measures. For example, the impact of an IT governance framework on the internal control environment (Rubino et al., 2017), which states that the:

Essence of a firm is effectively controlled and represented by the attitude of its management. If top management believes that control is important, the other members of the organisation will feel so and will respond with a conscientious respect for the controls established.

This could facilitate a more clearly defined approach to use of data from the onset.

This statement could apply equally to an information governance framework and the approach taken within an organisation, particularly as one of the seven categories of factors in the control environment are the ethical values and integrity standards within the organisation. In a local authority context, approaches to managing ethical and information governance standards could be incorporated into the constitution of a local authority to raise the profile of this topic.

With the introduction of new data protection legislation, there is the possibility of considering how the new law may be applied. For example, while research is not explicitly designated as its own lawful basis for processing, in some cases, it may qualify under Article 6(1)(f) of the GDPR as a legitimate interest of the controller.

Gillingham and Graham (2017) propose that to counter the inaccuracy and incompleteness of datasets, it may be worth developing policies that promote the collection of ever more detailed and full data sets about service users and service activity. From a data protection perspective, this would be considered as “data protection by design and by default”. The GDPR requires organisations that process personal data to put in place appropriate technical and organisational measures to implement the data protection principles and safeguard individual rights. This means integrating data protection into processing activities and business practices, from the design stage right through the lifecycle and that would include subsequent re-use. This concept is not new; however, as the key change with GDPR is that it is now a legal requirement. Adopting this approach should also assist organisations in their obligations to be transparent as to the use of the personal data they process and, in turn, demonstrate how they fulfil their ethical obligations to this data.

The GDPR also contains specific provisions that adapt the application of the purpose limitation and storage limitation principles when personal data is processed for scientific, historical or statistical purposes and as discussed there are specific obligations within the GDPR that relate to the use of personal data for research purposes. The absence of the consideration of these obligations in research proposals could therefore result in breaching data protection law.
In addition to the GDPR, the UK Parliament has enacted legislation, through Chapter 5 of Part 5 of the Digital Economy Act 2017, that facilitates the linking and sharing of datasets held by public authorities for research purposes.

The power set out in Chapter 5 (“the Research power”) broadly enables information held by one public authority to be disclosed to another person for the purposes of research. In making use of this power, public authorities must be able to demonstrate and meet a number of conditions. These include, establishing processes for “de-identifying” personal information to be shared under the power; adhering to a published Code of Practice, containing seven principles of data sharing for research purposes, concerning the disclosure, processing, holding or use of personal information intended to collectively ensure that the provision of personal information is ethical and legal under this provision; requiring parties involved in the disclosure of this information to be accredited.

With the introduction of these new legislative obligations and codes of practice in different settings and the range of issues being raised as to the ethical use of personal data, this is an appropriate time for the UK regulator to exercise powers within the Data Protection Act 2018 to publish a Code of Practice specifically related to the ethical re-use of data, rather than allow these standards to emerge as part of either organisational or sector activity.

Note
1. European Data Protection Supervisor (EDPS) is an independent institution of the EU, responsible under Article 41.2 of Regulation 45/2001 ‘With respect to the processing of personal data […] for ensuring that the fundamental rights and freedoms of natural persons, and in particular their right to privacy, are respected by the Community institutions and bodies’, and ‘ […] for advising Community institutions and bodies and data subjects on all matters concerning the processing of personal data’.

References
Caldicott, F. (2013), “Information: to share or not to share: information governance review”, Information: to share or not to share.


Further reading


**Corresponding author**
Malkiat Thiarai can be contacted at: m.s.thiarai@warwick.ac.uk
The role of archives and records management legislation after colonialism in Africa
Case of Southern Africa
Nkholeleni Sidney Netshakhuma
University of Mpumalanga, Mbombela, South Africa

Abstract

Purpose – This paper aims to analyse the current Southern African countries’ archives and records management legislations to identify the gaps and challenges. It is important to assess the role played by National Archives legislations within the preservation of heritage and history; private archives known as liberation archives; the transfer of archives; the disposal and retention of records, access, copyright management and skills; and development of staff.

Design/methodology/approach – The study used a qualitative methodology through document analysis, interviews and observation. The sampling of the study comprised representatives from the selected Southern African National Archives (South Africa, Mozambique, Botswana and Namibia).

Findings – The key findings revealed gaps of the archives and records management legislations in terms of definitions, transfer, disposal and transfer of records and accessibility. Some of the Southern African countries failed to use archives and records management legislation to promote accountability and governance.

Research limitations/implication – The research is limited to the following countries: Botswana, Mozambique, Namibia and South Africa.

Practical implications – Archive and records management legislation which has gaps creates problems in terms of effective implementation of archives and records management programmes.

Social implications – The failure by Southern African countries to revise their National Archives legislations and clarify the role of National Archives will lead to loss of archival materials if not addressed.

Originality/value – Updated archives legislation contributes to the development of effective archives and records management programme.

Keywords Heritage, Archives, Colonialism, Institutional memory, National Archives act

Paper type Research paper

Introduction

This article aims to analyse the current selected Southern African countries (SAC) archives and records management legislation (ARML) to identify the gaps and challenges to make recommendations based on the findings. The enactment and implementation of comprehensive, up-to-date ARML is a prerequisite for the establishment of an effective, integrated system for managing archives and records. Effective archives and records management are guided by sound legislative frameworks which define records to avoid ambiguity about the scope of the responsibilities of National Archives. ARML provides exclusive authority to carry out archives and records management functions such as acquiring private archives, appraisal and disposal of records, rights of inspection, access to records and transfer of archives. The ARML provides a basis for detailed regulations on the recruitment, appointment, promotion, professional qualification and training of archives staff. The effective ARML can enhance governance and accountability. Effectiveness and
efficiency of government systems are the core feature of good governance. This is alluded to by Yusuf and Chelle (2005: 129) who said that ARML is acknowledged as a tool which has an impact on the development of a nation. This meant that ARML can support human rights and improve financial management. ARML can also be utilised as a form of anti-corruption strategy. The land reform in Africa can be enhanced through effective ARML.

Problem statement
According to Lihoma (2008: 06), Ngulube and Tafor (2006: 58) and Okello–Obura, (2011), most African countries lack effective legal frameworks to support archives and records management programmes. This means that weak institutional capacity and the absence of ARML is the cause of lack of governance and accountability. Even though most of Southern Africa has ARML, most of their legislations were not reviewed and updated to clarify the role of National Archives (Ngoepe and Keakopa, 2011). Therefore, a gap in the ARML has led to the gap in the implementation of effective archives and records management programmes.

Purpose and objectives
The main research aim of this article was to assess the role of ARML to promote accountability and transparency. The following were specific research objectives:

- analysis of the current selected Southern African ARML to identify the gaps and challenges; and
- to make recommendation based on the findings.

A brief historical background of archives and records management legislation in the selected Southern African countries
The attainment of independence by SAC marked the beginning of the relegation of archives as a form of accountability and transparency. After independence had been attained, the SAC shifted their focus to other priorities like reconstruction and development projects. The issue of strengthening ARML was not attended as the priority by some of SAC. This is alluded to by Asogwa (2012: 199) who states that archives and records management in most of SAC declined because of a failure by some States to review and update their ARML.

Preservation of archives is dependent on the development and implementation of ARML. The fundamental development of a country starts with the development and implementation of ARML. Most of the SAC has ARML in place to some degree. However, their ARML have not been revised even though they were inherited during the colonial period. This is asserted by Nsibirwa et al. (2014: 55) and Ngoepe (2014: 7) who said that lack of archival and revised legislations leads to loss of memory of the nation and create archival dispute. This is because some of archives and records management elements of ARML have excluded the preservation of the history of African people. Furthermore, other states do not function effectively despite the availability of ARML.

The foundation for South African archives and records management system to preserve records commenced in 1876 in the Cape Colony under the British Colonial Administration. South Africa gained independence from British government authority in 1910. In 1910, the Union of South Africa government was established (Archival Platform, 2014). The Public Archives Act No. 9 of 1922 established the National Archives in South Africa (NARSSA). The Archives Act No. 6 of 1962 extended to public records. The Act was amended in 1964, 1969, 1969, 1977 and 1979 to ensure the protection of public records and was primarily
meant to make adequate provision for the archival records of the national, provisional and municipal administration. The National Party (NP) government came to power in 1948. NP came with the policies of an apartheid system which led to the passing of the legislation known as the Archives Act No. 22 of 1953. The act made a provision to separate the preservation of archives based on race.

Change has been experienced in South Africa, following transition from the apartheid system to the democratic form of government in 1994. Subsequently, in 1996, the National Archives and Records Services (NARSSA) Act 43 of 1996 came into place. Most of South Africa records management policies were established based on NARSSA Act. This is asserted by Keakopa’s study (2007) who stated that South Africa has established the policies to guide the management of records based on the NARSSA Act Keakopa, 2007. NARSS Act issued guidelines to assist government bodies to manage their records to improve transparency and accountability. According to Muchaonyerwa and Khayundi, 2014: 43 all South African governmental bodies are required by NARSSA act to provide for proper management of records in all formats and to give effect to the regulatory instrument namely NARSSA Act, The Public Finance Management Act (No. 1 of 1999), The Promotion of Access to Information Act (No. 2 of 2000), The Promotion of Administrative Justice Act (No. 3 of 2000), The Electronic Communications and Transactions Act (No. 25 of 2002) and Municipal Finance Management Act (No. 56 of 2003). According to MacNeil and Eastwood (2017: 254), NARSSA act No.43 of 1996 was revised in 2005 to include preservation of private archives.

Namibia is one of the SAC that experienced a challenge of ARML in terms of definition and role of Namibia National Archives (NNA). Namibia was formerly known as South West Africa and was under German administration from 1883 until 1915 when it was occupied by South Africa. The NNA was established in 1939. The National Archives was known as the Archives Depot of the Territory. Because Namibia was a colony of South Africa, even their archives were under the administration of the South African Director of Archives. The NNA dealt with collection, preservation and organisation use of historical materials. The duty of the NNA was to collect historical materials of state authorities after their retention period in offices had ended and to preserve them. In a nutshell, Namibia gained independence in 1990. Archives legislation of Namibia was enacted in 1992 (Nengomasha and Nyanga, 2015: 89).

Mozambique was a colonial government of Portugal. In 1938, the Portuguese colonial government investigated the organisation of administrative services including books systems for records registration. Mozambique gained independence in 1975. After the end of colonial rule in Mozambique, the first legislation on Mozambique’s national archival and records systems was launched on 1992 through Act No.33/92. The implementation of the Mozambican National Archives and Records Management Act was a challenge because of lack of clarity on the definition of records and role of its National Archives. Despite the availability of archival legislation guiding the management of records in Mozambique, archivists and records managers are struggling to comply with the models of legislation (Ngoepe and Saurombe, 2016).

Botswana became independent in 1966 from the British Colonial rule. The 1965 Botswana constitution led to the first general elections and to independence on 30 September 1966. Botswana National Archives (BNA) was established in 1967. In 1978, Archives legislation was formally passed by the Republic of Botswana. According to Ramokate and Moatlhodi (2009) National Archives was viewed as a societal memory which had to play a meaningful role for the preservation of history of Batswana. The BNA is responsible for the management of public records. The BNA also preserves colonial records. Like any National
Archives in SAC, BNA experiences a challenge of unappraised records which create a challenge of lack of space for the preservation of archival records.

After the independence of the above SAC, they were not well prepared to govern. This was caused by the failure of the colonial power to enact strong and credible ARML in their colonies (Asogwa, 2012: 199). This led to the newly established independent SAC to be dependent to the colonial master for the establishment of ARML.

After independence, SAC experienced challenges of disputes about the colonial archives (Shepard, 2015: 876). Colonial archives in this study refer to records created during the colonial period in Africa by European countries. According to Ngoepe and Netshakhuma (2018) most disputes relate to archives seised within a colony. The repatriation of archives was associated with a variety of legal, political, ethical and professional disputes. The colonial power in Africa i.e. Britain, France and Portugal transferred records during the colonial period to their countries. After colonialism, a series of archives were removed from colonial states and relocated to a colonial power e.g. Britain, France and Portugal. Colonial powers wanted to inherit archives from the colonial state. Furthermore, colonial powers were not willing to transfer colonial archives to new African Administration states (Williams and Banton, 2014: 43). This led to the conflict between newly formed African states and former colonial powers.

**Why archives and records management legislation?**

ARML plays a role on the management of government records as it provides the legal framework under which the National Archives operate (Mnjama, 2005: 464). ARM is the fundamental instrument of accountability of the state. The government is accountable to preserve the societal memory as required by the law.

The establishment and development of National Archives acts in SAC was driven by beliefs, principles and ideals that ARML will contribute to transparency and accountable government. According to MacNeil and Eastwood (2017: 250) archives and records management programmes play a meaningful role in providing accountability, transparency and good governance. Accountability is a component of good governance. Brazys and Kumah (2016: 289) alluded that there is a link between reviewed legislation and accountability. This is because records provide evidence that supports the investigatory phase of the accountability process. Without reliable recordkeeping activities, accountability could not be proven. ARML is a management tool for the African government to ensure the management, preservation and access of a country’s national documentary heritage (Okeahalam, 2004).

Governments are expected to be transparent and honest when they engage with their citizens. Up to date ARML are important to promote citizen’s trust and commitment to good government. Each and every sovereignty state is governed by legislation. Archives Institutions play a role in the restoration of state, sovereign, democratic and social rights. Archives preservation explains the development of national sovereignty (Shepard, 2015: 870). It is impossible to be accountable to government without proper management of archives and records management. Sovereignty, rights of citizens, is managed in terms of ARML. This means that accountability and transparency of government is dependent on how the public can access information.

There is a link between National Archives and national development. According to Guilder (2016), National Archives contribute to government’s programme of action in relation to nation building and social cohesion by ensuring that archives and records are accessible to various users. The freedom of access to information is recognised as a fundamental aspect of the goals for accountability, transparency and openness.
Access to information is important to good governance administration. Access to information is also a key variable for accomplishing the objectives of good governance. This is because there is fairness and public responsibility if citizens can access reliable information. According to Khan and Akhter (2017: 151), SAC have recognised the right to information as a basic human right.

ARML support human rights (Guilder, 2016). This means that government is able to support the rights of citizens and to improve the citizen-public interaction. This implies that rights and entitlements of citizens are protected through archives and records management. The government can enhance human rights through development and implementation of policies, standards and practices as guided by ARML.

ARML were formulated to enhance the preservation of archival material. According to Mnjama (2005: 463) development of preservation facilities has been disturbed by lack of facilities and a lack of trained staff. ARM provides a framework of management and maintenance of archives and records (Choy, 2006: 11).

Africa experienced land redistribution caused by the colonialism and the apartheid system in South Africa. According to Guilder (2016), land reform and land restitution were the major issues implemented by government in Africa. Effective records management system is a key to understanding the distribution of land in Africa.

**Literature review**

The literature was reviewed according to the elements of the ARML, the definition of archives, the role of legislations on National Archives, with the aim of identifying the gaps and challenges.

**Definition of terms**

The review of literature showed that most of SAC failed to define electronic records in their existing legislations. According to Dearstyne (2002:32) if electronic records are not fully defined this poses a challenge to the management of electronic records. The issue of defining records is complex because of the introduction of technology and digital platforms Yusuf and Chell (2005: 32). This is alluded to by Marutha (2018: 3) who said that most African countries’ scope of ARML covers only basic models of paper together with the most basic records archiving and the archival responsibilities of the institution. The most basic elements of electronic records management were not covered. The electronic records definition needs to consider aspects of medium, content, form, persons, archival bonds and transmissions (Yusuf and Chell, 2005: 116).

**Role of national archives**

According to Garaba (2007, P. 61), ARML is to define the roles of National Archives and various governmental departments for appraisal and destruction of records. Appraisal of records is the process of determining value for records which in turn determines what records are to be retained and what records are to be disposed of Yusuf and Chell (2005: 92). The SAC National Archives are due to adjust their ARML to ensure that there is systematic disposal of records. The disposal of records is a process of destroying ephemeral records and selecting records with an archival value (Yusuf and Chell, 2005: 92).

The ARML is to make a provision for the public to access archives. The review of literature showed that most of National Archives in SAC restrict its citizen access to information. On a positive note, in South Africa, NARSSA Act was reviewed in 2001 to include ERM (MacNeil and Eastwood, 2017: 255).
The ARML is to determine what records should be preserved by their National Archives. Baker et al. (2016: 21) alluded to the fact that the role of ARML is the archival collection preservation. Preservation leads organisations to retain records with historical, cultural and scientific significance. The determination of value of records can be achieved through the process of appraisal and the development of retention schedules. According to Garaba (2007: 59), archival appraisal remains a challenge in Africa. This is because most of SAC did not embark on a process to appraise records as a result of lack of appraisal skills and knowledge. The retention schedule determines the value of records in relation to operational, regulatory and legal requirements to define retention periods for records under each of the categories of requirements and determining a maximum retention period (Yusuf and Chell, 2005: 79).

National value archives are to be preserved in the National Archives repositories. Archives repositories play a role in safeguarding national archival resources as national properties, societal memories and public assets and providing the public with knowledge based archives services. (An, Bai, Deng, Sun, Zhong, Dong, 2017: 20). However, the review of literature found that there was less archiving of the history of Africa. The researcher assumed that when Britain and Portugal colonised SAC, they never took initiatives to document the history of local people. This is because of the limited archival collection of local history in the archives.

As a result, archives were regarded as the most important past, memory and information play an important in the culture and society of African (Oliver and Konsa, 2012: 99).

What is covered by ARML and what is acquired and preserved are public archives. ARML were to be utilised as indicators to determine role played by national archival institutions in the management of public archives and records management (Ngulube and Tafor, 2006: 61). It is the role of National Archives to preserve public and non-public records in their repositories. This means that ARML is to stipulate preservation of private records with historical and cultural significance. According to Garaba (2012: 139), ARML that govern National Archives of SAC are inadequate on the management of private records of national importance.

ARML is not being enforced in most of the SAC (Abbot, 2007: 7). Enforcement of legislations requires standardisation of archives and records management programme. Effective ARML provide basis for the development of standardization of archives and records management which is lacking in most of SAC. This is acknowledged by Ngulube and Tafor (2006) who said that archives and records management processes of National Archives in Southern Africa were neither governed by standards nor guided by a professional code of ethics. Standardisation of records management practices can be realised in the SAC if ARML is enacted. The review of literature showed lack of maintaining records management standards. The absence of standards and guidelines for the management of records in SAC has been reported (Nemgomasha, 2009; Ngulube and Tafor, 2006; Mnjama, 2005 and Ngulube and Tafor, 2006).

Review of archives and records management legislation

The legislative framework in most of the SAC has not been updated. According to Marutha (2018:3), legislative prescripts need to be updated and improved on a regular basis. This is also alluded to by Ngulube and Tafor, 2006: 63) Khumala and Baloyi (2017: 6) who said that most of ARML in Southern Africa are outdated. For example, the National Archives of Zambia Act of 1969 and the National Archives of Malawi Act were not yet updated since the end of British colonial rule. As a result of being out of date, most of these legislations are not linked to present archives and records management programmes.
The review of literature also showed that SAC have legislative framework in place that may be used for management of records (Marutha, 2018: 2). However, the challenges lie in the implementation delivery to ensure that records are managed. The existing ARML in SAC does not address archives and records management issues comprehensively (Asogwa, 2012).

Methodological/Approaches issues
Following an extensive literature review, a qualitative research method in the form of case study was adopted to explore the issue of archival legislation in Southern Africa. Potential interview participants were identified. Initially, it was envisaged that ten interviews would be conducted with the National Archivists of selected Southern Africa countries.

Unstructured interviewing was the main data collection method. Interview was conducted with the representative of National Archivist of Botswana, who is now working at the University of Botswana and representative from the NARSSA, Archivist from Namibia and Mozambique during the South Africa Society of Archivists conference held in East London, South Africa on 03 to 05 July 2018. The participants were selected and interviewed because they were aware of trends and developments of ARML in their countries. They were also responsible for the management of the archives repositories in their home countries. They all have background information on the legislations governing ARML.

An interview guide was developed before conducting the interviews to ensure that relevant themes of the research would be covered. Interviews questions centred on the following; asking the participants the aspects covered on the definition, usage of archives in their archives repositories, challenges experience by their National Archives, preservation of archives, access to archives materials and the role of archives in the development of state.

Data analysis
Data were analysed according to the objectives of the research in terms of assessing the role of ARML to promote accountability and transparency. Analysis was also based on the definition of electronic terms, role of National Archives and review of the National Archives of South Africa, Namibia, Mozambique and Botswana legislations.

Definition of archival and records terms
The participants for the interviews were asked as to whether their ARML define electronic records clearly. Participants from the National Archives of Namibia, Mozambique and Botswana acknowledged that their National Archives legislations never define electronic records and other aspects like public records in a clear manner. This means that there is ambiguity when the law makers try to define the electronic records. The participants from the NARSSA stated that the definition of electronic records is well defined to include all formats of records preserved in the archives. Both participants agreed that definition of electronic records is to be included in the preparation of policy of every organisation.

The role of national archives
The participants were asked if their national ARML provides the role of archives with regard to appraisal, disposal, preservation, access of records and implementation of the National Archives and records services.

The participants from NARSSA, Botswana stated that their ARML make a provision for a proper programme to implement appraisal and disposal of records. This means that
records were regularly appraised and disposed on a regular basis to identify records with historical and archival value.

The participants from Namibia and Botswana said that although their ARML make a provision for access to public records, access to information is always denied to member of public. The participants from South Africa stated the Promotion of Access to Information Act No. 2 of 2000, NARSSA Act make provision for the public to access information.

Participants stated that ARML were not enforced within public institutions because of lack of capacity in their National Archives. Lack of enforcement of the legislation led to the lack of compliance with the legislation which compromises the value of records.

The participants from NARSSA stated that their National Archives adopted various standards to manage records of different kind. These standards include International Organisation Standards (ISO) 15489. Other participants from other National Archives acknowledged the importance of standards but such standards were not effectively implemented in their National Archives.

Some participants indicated that archives management and administration was very new to the African states after colonialism. During the first year of independence in SAC, National Archives was prepared to seek the social and economic roots for history and to preserve African history.

Review of the archives and records management legislation
The review of the SAC ARML showed that most of their legislations were not reviewed Ngoepe and Keakopa (2011). Even the legislation which was reviewed, such as the Botswana National Archives and Records Service Act (Act 3, 1978), still had no clarity about the definition of electronic records.

Table I shows the name of the countries, name of the legislature and date of which the act was reviewed.

Findings
The findings were organised around the research objective under the following section:

- Analysis of the currently Southern Africa ARML to identify the gaps and challenges.

Definition of terms
The researcher found that on the selected countries, only the NARSSA Act defines concepts of management of ERM. NARSSA act made provision regarding management of ERM in their environment. In 2000, NARSSA developed a comprehensive guide to the management of electronic records in government bodies. While other countries archive legislations did

<table>
<thead>
<tr>
<th>Selected Southern Africa countries</th>
<th>Legislation and date of enactment</th>
<th>Date for the review</th>
</tr>
</thead>
<tbody>
<tr>
<td>South Africa</td>
<td>NARSSA Act (No.43 of 1996)</td>
<td>2001</td>
</tr>
<tr>
<td>Namibia</td>
<td>The Archives Act of 1992</td>
<td>Not yet reviewed</td>
</tr>
<tr>
<td>Mozambique</td>
<td>Mozambican National Archives and Records Management Act</td>
<td>Not yet reviewed</td>
</tr>
<tr>
<td>Botswana</td>
<td>Botswana National Archives and Records Service Act (Act 37, 1978)</td>
<td>2007</td>
</tr>
</tbody>
</table>

Table I.
not address aspects of the definition of electronic records. This statement is alluded to by Khumala and Baloyi (2017: 6) who said that most of the ARML of Southern Africa did not address the issue relating to electronic records management. Most of the National Archives has no proper, written and clear policy on electronic records Management.

The incorporation of ERM system requires NARSSA to collaborate with the Sate Information Technology Agency (SITA) in a proposed project to formulate SITA in a proposed project to formulate standards for records management in governmental bodies in the electronic environment. The standards address the issue of definitions, metadata, migration strategy, retention and disposal, filing systems, long-term preservation format, storage standards, vital records, security and encryption. However, the NARSSA lacks the expertise to manage electronic records management system.

The challenges of the SAC have been concerned with adopting the new technologies without clear strategy for managing the information created with them. The introduction of Information Communication technology in Africa posed a challenge to an archival institution in Africa. Most of the National Archives legislations in Africa were formulated without consideration of ERM systems. The failure of archival legislation to tackle the issues associated with ERM was a concern in Southern Africa (Mnjama, 2005: 465).

According to Brendan (2013: 796), African countries did not consider the aspects of information technology competence, system design competence, legal and organisational competence when introducing records management.

The role of national archives
The study found that most of the Southern Africa ARML is outdated. The regulatory framework dealing with the management of archives are outdated. The amendments of outdate ARML which have been cited as reasons for lack of implementation of records management programme.

Most of archival materials preserved in National Archives are not accessible to the public. This has happened despite the establishment of ARML to provide access to society (An, Bai, Deng, Sun, Zhong, Dong, 2017: 26). A few archival institutions, namely, the National Archives of South Africa, Botswana and Botswana, have provided online access to the archives resources that they manage. However, this is only limited to a few archival repositories. Most of the Southern Africa countries do not have policies for open access to archives resources. Furthermore, there is lack of standards for sharing archival collections in African countries. According to Nengomasha and Nyanga (2015), Namibia has not enacted Freedom of information or data protection laws yet.


The finding also revealed lack of awareness on the value of ARML. This means that archives had been neglected through poor funding. According to Ngoepe and Saurombe (2016), lack of implementation is partially because of the fact that most archival legislation in SAC is not budgeted. There is less scope for allocating resources, services or archives facilities based on political considerations when programmes are administered (Hugue, 2013: 398). Most of the budget allocated for archival programme was used for war purposes. A pattern of inadequate archives management systems has been found common among African countries (Yusuf and Chell, 2005: 133).
Amended legislations will empower archival institutions to carry out their mandate of managing records throughout their lifecycle. National Archives can implement records management systems which would ensure the physical and intellectual controls of records for retrieval, transfer and general management purposes.

There was proven poor archives management for both government and citizens and affect a government ability to manage resources effectively and to comply with international conventions (Thrson and Cain, 1996). The development of human resources is the strategy to improve performance (Yusuf and Chell, 2005: 134). Most of the African archivists had no access to adequate and qualitative local and international training.

No digitisation programme had been put in all National Archives in SAC which attempted to implement digitisation programme experience challenges of shortage of skills and lack of collaboration. Studies conducted about Zimbabwe National Archives by Sigauke and Chabikwa (2012) found that the National Archives digitisation project experience a challenge of preserving the authenticity and integrity of electronic records, some digital materials were lost, inaccessible because of the original software being outdated or incompatible with modern operating systems. There was no donation from national and international organisations. There were also challenges of technological obsolescence when they implement ERM system. This demonstrates that there was a lack of proper planning on development and implementation of digital programmes in the National Archives of Zimbabwe. According to Mnjama (2005: 463), digitisation project in Africa failed because most governments adopts ICTs strategy without consulting the National Archives on how best to develop and implement ERM systems.

On a positive note, most of National Archives in Africa adopted ERM system to market their collection (Mnjama, 2005: 463). Archives which adopted ERMS include BNA, NNA, Mozambique National Archives, South Africa National Archives and others.

Despite that most of SAC has archives legislation in place, they have no policies on handling archival materials. This was caused by a low priority and the supporting legislation in archives and records management. This challenge contributes to lack of infrastructure, i.e. archival buildings. According to Mnjama (2005: 465), inadequate records storage facilities is one of the challenges which hinder development of archive in Africa.

Most of archival material preserved in the Southern Africa National Archives states is not accessible by researchers. This statement is acknowledged by Ngoepe and Ngulube (2011), Mneni Saurombe and Mosweu (2013), Ngulube and Tafor (2006) who said that access to archival materials in Africa is a major challenge. The inaccessibility of the archival materials is also influence by lack of arranged and described archives to enhance accessibility to archival materials.

Archives and Records Management profession in SAC is a scarce skill. According to Yusuf and Chell (2005:135), the development of human resources is the strategy to improve performance of organisations. National Archives in SAC faced challenges to retain national archivist because of the low salary and low benefits. Hence, the private sector lured them at higher salary. According to Mnjama (2005:464), trained staff resigned from national archival institutions to take up private sector positions where they were well paid. The resignation of senior archivists' impact on the appraised records within organisations (Ramokate and Moatlhodi, 2009). A higher level of professionalism and expertise and administrative and managerial skills is necessary to strong archival organisation.

Most of the National Archives in SAC have no control over the management of private archives held by private institutions. Private institutions have a tendency to preserve their own collection e.g. church archives and political organisations archives like the African...
National Congress (ANC) Archives. Mnjama (2005: 468) said that there is lack of awareness to preserve both private and public archives in Southern Africa.

It is the responsibility of National Archives to preserve any records created by organisations. This means that it is still the responsibility of National Archives to preserve records like audio visual material. The review of literature found that most of the audio visual materials in SAC were neglected. Lack of management of audio visual materials may be influenced by lack of skilled professional archivist to manage archives. According to Mnjama (2005: 46), National Archives have done little to develop their audio-visual archiving programmes. Namibia has collections of audio visuals. However, these collections are poorly managed. In South Africa, audio visual division which is tasked to collect all audio visual materials about South Africa are still preserved.

**Review of the archives and records management legislation**

The researcher found that most of South African legislations were not revised. This posed a challenge on because of the excluded archives from the national system. This includes liberation archives which occurred mostly in SAC Jonker (2009) indicating that archival legislation which focuses on public records cannot ignore the importance of private records to underpin the fabric of society’s archival memory. Most of the former liberation archives in the SAC were not incorporated into the National Archives because of a lack of provision in the ARML to preserve private collection. This is alluded to by Garaba (2014: 30) who indicated that National Archives do not have records of former liberation movements in its custody. The liberation movements included ANC of South Africa, Pan Africanist Congress of Azania (PAC) of South Africa, ZANU PF of Zimbabwe, The Liberation Front of Mozambique (FRELIMO), Popular Movement for the Liberation of Angola (MPLA), South West African People’s Organization (SWAPO), Zimbabwe African National Union Patriotic Front (ZANU PF), and the Zimbabwe People Revolutionary Army (ZIPRA). Records created by the above mentioned liberation movements represent an important history of their countries which deserve to be included in their ARML. Records created by the liberation movements are unique and there is a need to document the history. Only NARSSA Act of South Africa made provision in their legislation to preserve private collection which includes liberation archives.

**Recommendation**

- National Archives should be established within the main stream of public administration under a minister.
- There should be periodic reviews of ARML as a results of the emergence of ICT
- ARML is to direct National Archives to develop, approve and review advisory and mandatory standards and regulations for adequate and accurate recordkeeping in organisations and audit their records management.
- ARML to enforce organisations to transfer public and private archival records of public interest to the National Archives repository.
- ARML is to be considered as a cornerstone of democratic governance, accountability and the promotion of human rights.
- ARML to identify the responsibility of the National Archives for the acquisition and care of liberation archives that warrant permanent preservation in the National Archives of SAC.
• There is a need for the allocation of resources to archives and records management programme to enhance implementation of ARML
• National Archives of SAC to collaborate and partner with former liberation movements to incorporate liberation archives into the national systems.
• SAC to embark on oral history project to close gap of undocumented history of previously disadvantaged African caused by colonial powers.

Conclusion
In conclusion, it can be stated that ARML elements define the terms, role of archives and review of legislation were taken into consideration by Southern Africa countries. Further empowerment and review of the ARML is required to meet the demands of current records and archives management situation of digital management to enhance accountability and transparency. Based on the finding of the study, there is a need for a state to allocate resources (funding, human resources and technology) to amend ARML to enhance, appraisal, disposal and access training.

References


About the author
Nkholezeni Sidney Netshakhuma is a Deputy Director Records and Archives at the University of Mpumalanga in South Africa. Prior to this position, Netshakhuma worked for SANPArks as the records manager and the African National Congress as the archivists. Netshakhuma holds Masters of Information Science from the University of South Africa, and he is currently enrolled for doctoral programme in archives and records management at UNISA. Nkholezeni Sidney Netshakhuma and can be contacted at: Sidney.Netshakhuma@ump.ac.za

For instructions on how to order reprints of this article, please visit our website: www.emeraldgrouppublishing.com/licensing/reprints.htm
Or contact us for further details: permissions@emeraldinsight.com
The inevitability of digital transfer

How prepared are UK public bodies for the transfer of born-digital records to the archives?

Lale Özdemir
Marmara Universitesi Fen-Edebiyat Fakultesi, Istanbul, Turkey

Abstract

Purpose – This paper aims to assess how prepared public bodies are for the transfer of born-digital records to the National Archives (TNA) of the UK in line with the reduction in the transfer rule from 30 to 20 years.

Design/methodology/approach – The change in the transfer rule means that records of UK public bodies will be transferred to TNA for permanent preservation at 20 years as opposed to 30 years old. This move, which has been described as a major change that is going to be introduced in a manageable and affordable way (20-year rule, The National Archives), will inevitably witness the transfer of born-digital records to the archives much earlier than would have been the case if the change in the transfer rule had not been made. This paper reports on research carried out in the winter of 2017 on the extent to which UK public bodies are prepared for the transfer of born-digital records to TNA. Research was based on a survey of 23 public bodies which included ministries, charities and non-departmental public bodies. The target population was predominantly public bodies that had the highest level of transfer of records to TNA. The justification for this lies in the fact that these bodies, amongst others, transfer the most records to TNA, thus it would be interesting to gain an insight into how prepared these relatively larger public bodies are with regard to born-digital transfer. The remaining public bodies were chosen randomly amongst non-ministerial departments. The primary areas under analysis are plans of public bodies for the transfer of born-digital records, processes for transfer to be undertaken such as selection, appraisal etc., the use of technology in sensitivity review and the trigger date for the transfer of records.

Findings – An analysis of the research findings found that while a few UK public bodies surveyed had transferred datasets within the framework of the TNA Government Datasets (NDAD) initiative or as part of an inquiry, only one public body had transferred other born-digital records to TNA. The findings also reveal that most public bodies are yet to plan for, or to adjust, their current archival processes to take into account the different mind-set and skills required for the transfer of born-digital records. The level of preparedness is therefore limited primarily because public bodies have yet to undertake a transfer of born-digital records to the archives. The research findings also revealed that public bodies had not as yet made adjustments or changes to current practice to take into account the issues relating to the processing of born-digital records prior to transfer.

Research limitations/implications – The findings of the research at hand are based on a survey submitted electronically to twenty-three public bodies with the aim of assessing how prepared they are for the transfer of born-digital records to the National Archives (TNA). The survey was sent to 27 public bodies with responses received by 23 public bodies. The survey sent to these bodies comprises eight questions that were deemed to be important in the current digital landscape with regard to the processes involved in the transfer of records, beginning from their creation. Thus, an element of subjectivity exists with regard to the outcome of the research, as the public bodies chosen were guided in prioritising any issues about digital transfer through the questions posed. The research carried out is also limited in that it focuses primarily on ministerial departments (14 of the 23 surveyed) and also constitutes a very small sample of UK public bodies overall. However, the originality of the data obtained through the study carried out by far outweighs the limitations of the research methodology.

Originality/value – This paper highlights that the transfer of born-digital records through original research amongst the 23 public bodies surveyed is not widespread, and that processes and procedures specifically for the management of processes for born-digital records are yet to be implemented. The study
concludes that long-term planning for the transfer of born-digital records is yet to be undertaken and that public bodies are more likely to deal with the issue when their digital records are closer to reaching the point of transfer.

**Keywords**  Records management, Born-digital records, Digital transfer

**Paper type**  Research paper

**Introduction**

This article will focus on the preparedness of UK public bodies to transfer born-digital records to TNA in terms of the comprehension, and planning for, of the processes that are required for the transfer of born-digital records to the archives. Archives are legally charged with preserving the national memory through the transfer of records that are now, almost always, created in a digital environment. Effective information governance in organisations is achieved through the management of information assets in terms of transparency, accountability and risk management, with the aim of supporting corporate governance to meet business outcomes. Information governance is important within the context of archiving for a number of reasons, but, namely, for the following: first, archivists, and by extension all information professionals, are no longer solely the keepers of records but also need to be pro-active as auditors (Kallberg, 2012). Those responsible for knowledge and information management play a critical role in the management of information assets. This in turn, contributes to the effective implementation of information governance through the management of digital information from its creation. Second, some of the born-digital records managed as assets in the public sector in terms of regulatory, legal and operational requirements will later be transferred to TNA. The management of born-digital records through the application of processes and procedures bespoke to the management of digital records should be undertaken, such as digital appraisal and sensitivity review, by information professionals, thus ensuring that the nation’s official historical memory is preserved and accessible in the future. In terms of information governance, The Advisory Council on National Records and Archives which has a statutory role as an independent body to advise the Secretary of State for Digital, Culture, Media and Sport on issues relating to records management, also plays an important role in the UK public records system. The Council represents the public interest with regard to the preservation and access to public records and thus adds an additional layer of scrutiny to the decision of public bodies to close records upon transfer to the archives. In the way of an example, The Council was content to recommend that permission be granted to retain their legacy records for the 12-month period requested by HM Land Registry but the Department for Work and Pensions was given a two-year retention period instead of the requested five years (Advisory Council Reports). This highlights the role the Council plays in helping to ensure that record keeping in UK public bodies is and remains transparent and accountable.

The approach of the UK National Archives to digital transfer is changing in line with developments in the technological and legislative landscape. In terms of its strategic goal on all digital things, TNA aims to transition from being a first generation archive to becoming a second-generation archive. The current practice of the first generation archive leans heavily on archival practice devised for the preservation of paper records (Digital Strategy, The National Archives). The vision to develop into a second-generation archive was published in 2017 and focuses on the disruptive nature that TNA plans to adopt over the next few years. This will entail the overhaul of
current archival practice to allow for the changing nature of born-digital records, which will render the transfer and preservation of structured databases as well as computer code possible (Digital Strategy, The National Archives). TNA’s digital strategy that also aims to rethink the contextual nature of digital records will also impact directly on the information professionals of government departments who will have to be attuned to TNA’s new way of thinking on the second-generation archive. Ultimately, a second-generation archive will have to preserve born-digital information in new and different forms, which includes mixed media content, based on new archival practice because digital records are unlike physical records in their structure and raise different issues with regard to volume and sensitivity.

Current archival practice across government is firmly embedded in the first generation archive practice and it could be argued that it is still the case that practice and processes relating to born-digital records are a hot topic for the archival profession, that won’t be resolved anytime soon (Sloyan, 2016). This should be considered in light of the fact that the majority of UK public bodies are yet to transfer born-digital records to the archives.

The current study examines the extent to which public bodies are adopting the archival processes that are unique for digital records. For all intents and purposes, the digital strategy of TNA can be viewed as a high-level policy that should cascade down to the information professionals in government through the advice and guidance that TNA is legally bound to provide through the provision of the Public Records Act. However, if considered within the framework of methodologies, TNA’s strategy is not, as yet, prescriptive in terms of how those on the ground working in knowledge and information management across government will actually manage their records with the intention of transferring to a second-generation archive. The current study reveals that the current state of play is that public bodies are, generally speaking, not at a stage where they can, or indeed are legally obligated to, implement the archival processes required to transfer born-digital records in line with the changes to the transfer rule to the archives. Thus, the notion of a second generation archive that ensures the long term preservation of computer code and copies its collections to the cloud may be a far off notion for the vast majority of knowledge and information professionals across government, despite the fact that, in the long term, the burden on them may be reduced because metadata requirements will inevitably change to suit the new disruptive archive model (Digital Strategy, The National Archives).

The change in the transfer rule
Public bodies are now required to transfer their records to TNA once they reach 20 years old, rather than the previous transfer rule that required records to be transferred at 30 years old. The Public Records Act states that:

Public records selected for permanent preservation under this section shall be transferred not later than 20 years after their creation either to the Public Record Office or to such other place of deposit appointed by the [Secretary of State] under this Act (c.51, s3(4)).

On 25th October 2007, the then Prime Minister Gordon Brown announced that he had asked Paul Dacre, working with Professor David Cannadine and Sir Joseph Pilling, to chair an independent review of the Review of the 30-Year rule, under which most government records are transferred to The National Archives and made available to the public by the time they are 30 years old (30-year rule review, The National Archives). The review found that more than 80 per cent of the general public
favoured a reduction of the “transfer rule” from 30 years, whereas public bodies, notably the Foreign and Commonwealth Office (FCO) and the Department for Business, Enterprise and Regulatory Reform (now part of the Department for Business, Energy and Industrial Strategy (BEIS)) tended to err on the side of caution, citing drawbacks of the premature disclosure of official records (Review of the 30 Year Rule, The National Archives). Interestingly, the report recommended a reduction in the transfer rule to 15 years; however, the government at the time adopted a reduction to 20 years.

The introduction of the UK Freedom of Information Act (FOIA), which came into force in 2005, fundamentally changed the right of access to information. The public no longer had to wait for the closure period of records such as gruesome unsolved murder files, Home Office naturalisation files or FCO files on diplomatic relations with particular countries that had been transferred to TNA, to expire. Requesting access to official information was no longer bureaucratic and appeals against public bodies withholding sensitive information became routine. In the way of an example, the Information Commissioner’s Office, established to uphold information rights, issued a decision notice, in 2017, upholding the decision of TNA to withhold information contained in Metropolitan Police files relating to the “Nude Murders’’ committed in 1960s London (Information Commissioner’s Office). In an era of the right to request official information, the 30-year transfer rule was regarded as being outdated and concerns were raised that the advent of FOIA had eroded the conventions of good record keeping in light of fears that information may be released to the public (Review of the 30 Year Rule, 2009). It was thought that the possibility that official information might be released to the public would result in less information being recorded. Such concerns about poor record keeping were justified in high profile inquiries such as the BSE Inquiry and Hutton Inquiry (Moss, 2012). However, the fact that FOIA has been in operation in the UK since 2005 and that responding to requests for access to official information has become the norm, it could be argued that public bodies are now more likely to be better at record keeping because they need to be able to find and retrieve with ease the information they may need to review in the light of an FOIA request.

The reduction in the transfer rule to 20 years has resulted in the introduction of the phased implementation of this transition in 2013. Based on this approach, and in theory, it is envisaged that two years’ worth of government records will be transferred every year to TNA, resulting in records dating from 2001 and 2002 being transferred in 2022 (20-year rule, The National Archives). This is against the backdrop of The National Archives receiving records dating from 1983-1984 in 2013. Despite the fact that the transition to the new transfer rule is being introduced in, what is being referred to, as a manageable and affordable way over a period of 10 years, (20-year rule, The National Archives) the research carried out for the current study indicates that public bodies may be unlikely to meet the target of transferring two years’ worth of records until 2022. This is due to the fact that the transfer of born-digital records is, not of yet, a practice embedded in government, just four years away from the target of a single year’s worth of records that are 20 years old being transferred to TNA (The National Archives, 20-year rule). Therefore, the theory of the implementation of the phased approach to the transfer digital records is somewhat different in reality to the actual practice of digital transfer.

Sources used
The main source of data for this article is a survey sent electronically to 23 UK public bodies containing eight questions relating to the transfer of born-digital records.
Following are the survey questions:

(1) Has your organisation transferred born-digital records to TNA?
(2) If not, when do you anticipate that you will transfer born-digital records to TNA?
(3) Which of the processes for born-digital records is the most resource intensive?
(4) Which of the processes for born-digital records is the least resource intensive?
(5) Is the sensitivity review of born-digital records in your department technology assisted?
(6) Which Freedom of Information exemptions, if any, most apply/will apply to your department’s born-digital records at transfer stage?
(7) What date does/will your department use for the trigger date for the transfer of digital records?
(8) Does your department use outsourced IT?

The UK Government consists of 26 ministerial departments, 401 agencies and other public bodies, 3 devolved administrations, 78 high profile groups and 12 public corporations. Owing to the size of the target population, it would have been highly impractical to attempt to survey all public bodies. A sample of only 23 public bodies, of various sizes and remits, is not representative of UK public bodies in terms of size, and thus the sample is limited in scale. Although the sample size may not provide a preliminary insight into the way public bodies are preparing for the transfer of born-digital records to the archives, it certainly allows for observations to be made regarding the progress of the organisations surveyed. The study is particularly useful for gauging the progress of ministerial departments in terms of digital transfer, as they constitute the largest group surveyed. This is also significant because ministerial departments are among the bodies that transfer the most records to TNA, and will thus be in a position, sooner rather than later, to transfer born-digital records. The requests for information, in survey form, were processed in accordance with the Freedom of Information Act by some bodies, whilst others responded to the request within the framework of a request for official correspondence. The requests for information were made at the beginning of 2017 and the online platform for requesting official information from public bodies WhatDoTheyKnow, was used to make the majority of requests. The requests for information and the subsequent survey findings can be publically accessed on the WhatDoTheyKnow site (WhatDoTheyKnow, Information regarding digital transfer of records to The National Archives). Requests made directly to the public body have been published by some of the public bodies on their official website (for example, Office for National Statistics, 2017, Release date: 9 February).

In addition to the data obtained from the survey findings, the Business Intelligence Review on the digital landscape in government 2014-2015 is also used as a source for the study. The survey findings have been compared, where feasible, with the findings of the above review (The National Archives, 2016b). This ensures that the findings of this study can be used to gauge whether the issues identified by the review have changed, to any extent, in terms of how public bodies are for the inevitable transfer of born-digital records.

The current rate of transfer of UK born-digital records

Public bodies surveyed

The public bodies surveyed included 14 that transfer the most records to TNA (The National Archives, Record transfer report). The public bodies surveyed that fall within this

Transfer and anticipated transfer
The first question posed to public bodies was as follows: Has your organisation transferred born-digital records to TNA? Table I contains the answers provided by public bodies to the question of whether or not they have transferred born-digital records.

The data obtained from the survey reveal that 19 of the 23 public bodies surveyed had not yet transferred born-digital records to the archives, whereas three public bodies can be categorised as having partially transferred born-digital records in that they had either participated in TNA’s National Digital Archive of Datasets (NDAD) scheme that collected and provided access to the archived datasets of central government departments, dating from as far back as 1963 (The National Archives, Government datasets), or had transferred born-digital records that originated from an inquiry that they were the lead department for. The public bodies that have transferred datasets to the TNA, are the Department for Transport and the Metropolitan Police Service (datasets containing statistical information). Whereas the Ministry of Defence has transferred born-digital records in the form of public inquiry records. The responses from the Department for Transport and Metropolitan Police Service are as follows:

Department for Transport has not transferred any born-digital records to The National Archives. There are a small number of datasets available at TNA from the department’s predecessor, which were acquired via the National Digital Archive of Datasets. These records can be found in TNA series LM 1.

<table>
<thead>
<tr>
<th>Responses</th>
<th>Public bodies surveyed</th>
<th>No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>The Welsh Government (devolved administration)</td>
<td>1</td>
</tr>
<tr>
<td>Partially</td>
<td>Metropolitan Police Service, Ministry of Defence, Department for Transport</td>
<td>3</td>
</tr>
</tbody>
</table>

Total 23

Table I.
The Metropolitan Police Service: some data sets (statistical information) have been transferred to TNA, however we have not transferred any documents to TNA.

In response to the survey, the Ministry of Defence stated that it had carried out a partial digital transfer of Al-Sweady public inquiry records:

The MOD has not transferred born-digital records to The National Archives (TNA). However, copies of born-digital records originating from the MOD have been transferred by the Al-Sweady Public Inquiry to TNA, and these are catalogued in the ASI series. Originals of these records have been retained in MOD.

The Welsh Government was the only public body surveyed that declared that it had carried out a transfer of born-digital records to TNA within the framework of the Digital Records Infrastructure (DRI) Transfer Pilot between August 2014 and January 2015. The aim of the pilot was to deliver a scalable server-to-server digital Transfer process compatible with TNA’s Digital Records Infrastructure. The Arts Council England, one of the bodies surveyed, stated that it had not transferred born-digital records to TNA and that it was not technically subject to the Public Records Act. The digital landscape in government 2014-2015: Business Intelligence Review carried out by TNA in 2016, states that from 2016 onwards public bodies will begin to transfer born-digital records – those records created originally in born-digital formats such as emails, documents and spreadsheets. The review stresses that TNA has been developing innovative new digital technology and practices to prepare for the transition from paper to born-digital records from government departments (The National Archives, 2016b). The data collected by the review, indicate that, by 2016, there are expected to be twelve departments scheduled to transfer digital records, with an approximate total of 50 in 2021 (The National Archives, 2016b). The data obtained from the 23 public bodies to determine whether digital transfer is becoming a reality across government, show that the aim of TNA for twelve public bodies to be ready for transfer by 2016, has not materialised. However, the fact that the current study only surveyed a proportion of UK public bodies, which may not be included in TNA’s short-term transfer targets, may render the outlook bleaker than it actually is. In addition, TNA publishes comprehensive data on the annual anticipated transfers of public bodies. This also includes information on the quantity of legacy records that will be transferred, or those records covered by retention instruments, which allows public bodies to retain them rather than transferring them to TNA. As an example, the Metropolitan Police Service has two thousand three hundred and forty-two legacy records that it plans to transfer to TNA in 2018, and The Royal Parks has two hundred and twenty-two records awaiting disposal (The National Archives, Record Transfer Report). However, the data provided by TNA do not state the format of the record being transferred (physical or digital), thereby limiting an insight into the anticipated transfer levels of born-digital records. This is most likely due to the fact that digital transfer is not yet a widespread business as usual activity because public bodies are still in the transitional period for transferring their digital records.

The review of the UK’s government’s strategy for managing its digital records and archives carried out by Sir Allan (2014) that was published in highlights issues faced by public bodies in being able to adhere to the transitional period for the transfer of records at 20 years (Records Review, Sir Alex Allan, August 2014). The primary obstacle to meeting the transitional period under the new transfer rule was cited as the backlog of legacy paper records yet to be transferred to the archives. Legacy records are those that are legally overdue for disposal or transfer by the public body.
In accordance with the recommendations of the review carried out by Sir Alex Allan, records dating from 1989-1990 should be transferred to TNA in 2016, records dating from 1991-1992 should be transferred in 2017 and records from 1993-1994 should be transferred in 2018. Despite the fact that TNA has been issuing guidance on electronic records management since 1999, it is highly likely that the majority of records dating from 1989-1994 will still be in paper format. Therefore, public bodies are likely to have to deal with hybrid transfer, both of physical and digital records, which respectively require a different mind-set and set of processes. According to Sir Allan’s review, some of the issues faced by public bodies, that it could be argued, may hinder the preparedness and transfer of born-digital records are as follows; the Department for Culture, Media and Sport, as of 2014, held at least 45,000 records that date from 2000 and earlier for which they did not have accurate data on dates; the Department for the Environment, Food and Rural Affairs held 14,000 files overdue for appraisal or destruction inherited from Arms Length Bodies; and the Ministry of Defence was dealing with approximately 50,000 legacy files at the time that the review was published (Records Review, Sir Alex Allan, August 2014).

**Anticipated date of born-digital transfer**

The second question asked public bodies when they anticipated they would transfer born-digital records to TNA. Table II details the date range that public bodies envisage they will start transferring their born-digital records to the archives. The Welsh Government, as mentioned above, is the only public body to have carried out a full transfer of born-digital records to TNA as part of a pilot project. The data obtained showed that six of the twenty-three bodies surveyed did not know when they would begin to transfer born-digital records. These six public bodies are as follows; the British Council, the Department for Education, the Department for Work and Pensions, Historic Royal Palaces, Foreign and Commonwealth Office and the Metropolitan Police Service. The research results reveal interesting insights into why some government departments have issues relating to the uncertainty of when they will start to transfer digital records. The Department for Work and Pension stated that it currently has a print-to-paper policy and undertakes all transfer activity on paper files and was therefore unable to provide any further information as to when the department would be in a position to transfer born-digital records to The National Archives. There is a likelihood, therefore, that some public bodies will not meet their statutory duty to transfer records at 20 years old, given that they do not yet envisage when transfer will commence. The digital landscape in government 2014-1: Business intelligence review, raised concerns that some public bodies were using the end of

<table>
<thead>
<tr>
<th>Anticipated date of transfer</th>
<th>No. of public bodies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not subject to Public Records Act</td>
<td>1</td>
</tr>
<tr>
<td>Unknown</td>
<td>6</td>
</tr>
<tr>
<td>2013-2016</td>
<td>1</td>
</tr>
<tr>
<td>2017-2020</td>
<td>5</td>
</tr>
<tr>
<td>2021-2024</td>
<td>7</td>
</tr>
<tr>
<td>2025-2028</td>
<td>1</td>
</tr>
<tr>
<td>2029-2032</td>
<td>2</td>
</tr>
<tr>
<td>Total</td>
<td>23</td>
</tr>
</tbody>
</table>
their print-to-paper policy as a marker for their digital records transfers (The digital landscape in government 2014-2015: Business intelligence review, 2016). However, it is also a concern, perhaps of greater magnitude, that some public bodies such as the Department for Work and Pensions still adopt a print-to-paper policy in the digital age where the use of information management systems across government is commonplace. The Foreign and Commonwealth Office (FCO) was also one of the departments unable to confirm when the transfer of digital records would begin. This may not come as a surprise given that the Records Review detailed how the department had the greatest difficulties meeting its obligations under the Public Records Act and the Constitutional Reform and Governance Act. This was in addition to having to deal the release of regular departmental records in line with the transfer and also had to handle two other sources of records: the “migrated archives” and the “special collections.” According to the Records Review, the FCO current plan does not entail the department meeting the requirements of the 20-year rule until well after the end of the transitional plan in 2023 (Records Review, Sir Alex Allan, August 2014). However, in accordance with the research findings of the current study, the FCO may be unable to meet the transitional plan in 2023, given that it was unable to state when it would commence digital transfer in 2017.

As shown in survey questions, approximately 22 per cent (5) of public bodies stated that they aimed to transfer digital records in 2017-2020. For example, the Department for Communities and Local Government, HM Customs and Revenue and the Home Office are among the departments that aim to be prepared for digital transfer in the above period. Whereas, approximately 30 per cent (7) of the bodies surveyed, the highest proportion of those bodies surveyed, planned to transfer digital records between 2021 and 2024. The public bodies that chose the above date range in the survey include the Department for Business, Energy and Industrial Strategy, the Food Standards Agency, the Office for National Statistics and the Ministry of Defence. The Royal Parks stated that it would commence digital transfer in 2025-2028 and Highways England and the Department for Transport both declared that they would start transferring digital records between 2029 and 2032. The digital landscape in government 2014-2015: Business Intelligence Review was compiled from several different sources of data including a digital questionnaire from April 2015 with replies from 60 departments. Therefore, a direct comparison on the predicted rate of business-as-usual digital transfer is not completely helpful given that the bodies surveyed in 2016 as part of the Business Intelligence Review and those surveyed in 2017 as part of the current study are not identical. However, the current research findings point to the possibility that an approximate total of 50 departments would not have undertaken digital transfer as stated in the Business Intelligence Review by 2021.

Processes for born-digital records

The changing digital landscape

Times have changed and so have archival user expectations. Approximately 300 records are now downloaded for every one delivered to the public in the reading rooms at TNA in London (Gledhill, 2018). The digital sphere presents untold opportunities that only a couple of decades ago were unheard of. TNA has digitalised huge collections of records including NHS registers and home guard papers and the UK Government Web Archive which hosts the official websites of public bodies as part of TNA’s holdings, can be considered to be a significant achievement in terms of
providing long term access to digital records (Johnson et al., 2014). Scholarly output and the policies and changing practices of TNA reflect the urgency in the need to develop new practices that primarily rely on the use of innovative technology, for processes relating to the management of digital information. The practices applied to paper records in terms of the appraisal, selection, sensitivity review and transfer are not sufficient for digital records. New processes that take into account the intangible and complex nature of digital records are required. Volume is also an issue, recent figures suggest that the information/data created and copied is doubling in size every two years and will reach 44 zettabytes (44 trillion gigabytes) by 2020 (McLeod, 2015). This is why, as mentioned, TNA is working on a disruptive model for a second-generation archive. The piece-by-piece approach used for the appraisal, selection and sensitivity review of paper records is not realistically possible in the digital world. This dilemma does not stem solely from the evolution of digital records, even though this is the primary factor stressed in the literature on the subject, but from a number of factors. The concepts of authenticity and integrity for digital records are not as straightforward as is the case for paper records because they are intangible. Trusting that digital records are what they purport to be, especially after the lapse of several years is tricky. The research project ARCHANGEL, with TNA as one of its stakeholders, is investigating such issues as the changing nature of digital records over time, in terms of a general abstract process, to ascertain if they can be deemed to be the same when archived as when they were created twenty years previously. The project is also investigating the role of blockchain (records linked using cryptology) in achieving this (Green, 2018).

Time for change: processes and practice for digital records
The third and fourth questions of the research survey focused on the processes public bodies would have to undertake to be able to transfer born-digital records to TNA. The public bodies surveyed were asked which processes for born-digital records they deemed would be the most and least resource intensive, (e.g. appraisal and selection, sensitivity review, transfer process, other). Approximately 65 per cent of public bodies (fifteen) stated that they did not know what the most or least resource intensive processes for born-digital records would be. This is because they were yet to embark on the process of transferring born-digital records to TNA. Arts Council England, is not technically subject to the Public Records Act, and stated that they had many and varied digital records and processes, which rendered it impossible to answer the above two questions. Amongst these, the Department for Environment, Food and Rural Affairs stated that it currently had no actual experience of the digital transfer process, while HM Revenue and Customs stated that it was yet to develop the processes for their digital records management. Historic Royal Palaces declared that it was not in a position to comment, as they had not yet gone through the process of digital transfer. However, Historic Royal Palaces stated that for physical records the sensitivity review and subsequent applications for closure was the most resource intensive process. Highways England stated that it did not hold the information required to answer the above two questions as its electronic records did not meet the requirements to transfer to TNA) and that resources would be determined closer to the required transfer date of 2029. In the way of a final example of a public body that could not state which processes would be the most or least resource intensive, the FCO declared that it was currently working on the design of a process to transfer digital records to TNA and was therefore not currently in a position to answer the two questions.
As stated, the vast majority of UK public bodies had yet to transfer born-digital records to TNA thus it is understandable that 65 per cent of bodies surveyed were unable to specify which processes would be the most or least intensive. However, this overwhelmingly uncertainty also points to the fact that these organisations have not yet embedded new processes or have made concrete adjustments to current practices, for digital transfer. Nonetheless, the research findings provide an insight into the processes that some public bodies anticipate that they will find resource intensive, or the opposite, when digital transfer is embarked upon. Overall, appraisal and selection were cited as the processes that bodies envisaged would be the most resource intensive. Interestingly, they were also cited as the processes that were deemed to be the least resource intensive. This indicates that uncertainty is prevalent regarding the digital transfer process. The Department for Communities and Local Government, the Department for Business, Energy and Industrial Strategy and the Office for National Statistics took the view that appraisal and selection would be the most resource intensive. The Department for Digital, Culture, Media and Sport stated that appraisal and sensitivity review would be the most resource intensive processes. Appraisal is the process of distinguishing records of continuing value from those with no further value and selection is a decision-making process that encompasses initial appraisal judgements and determines which records will be transferred to The National Archives or other approved place of deposit (The digital landscape in government 2014-2015: Business intelligence review, 2016). The selection process tends to focus, based on operational selection papers, on the selection of records that hold historical value in terms of preserving national memory. Thus, the format or media of the record should not affect the selection decision-making process. However, it is not as straightforward in the digital age, as digital records can be held across many different systems and platforms which are problematic for public bodies. TNA’s Business Intelligence Review sought to identify whether public bodies had mechanisms for identifying records of enduring value and how evenly these were applied. The review also examined email management and social media capture and probed how public bodies would appraise and select digital records in a scalable way (The digital landscape in government 2014-2015: Business intelligence review, 2016). The review found that 15 per cent of the public bodies they collected data from, were either revising their guidance for digital records, or had no up-to-date guidance for digital records. Half the departments surveyed by the review tried to apply their retention rules across paper and digital platforms with varying degrees of success (The digital landscape in government 2014-2015: Business intelligence review, 2016). The use of technology to aid appraisal in the digital age is an absolute must because the processes embedded for paper records will not suffice. This probably accounts for why four out of the eight bodies that named a process as being anticipated to be the most resource intensive, cited appraisal. TNA has been working on how to best apply technology to digital processes and technology-assisted review which can be defined as a combination of input from expert human reviewers and computer software to partially automate the classification of records and to identify patterns and similar content (The National Archives, 2016a). The use of technology to categorise and cluster information and email visualisation are a few of the tools that could be used to help undertake appraisal and selection across government. The automation of processes for digital transfer has not been established in public bodies, as the current study reveals. However, some of the public bodies surveyed were aware of the issues relating to the need for different processes. The Food Standards Agency stated that:
We have yet to undertake this process, although the process of transferring records from a legacy to current EDRMS in preparation for future transfer which.

[...] covered selection only has proved to be resource-intensive and should be considered as a factor in any study on this issue.

Whereas the Department for Communities and Local Government took the following view:

Appraisal and Selection given the difficulties in reviewing electronic records. Such difficulties include Health and Safety concerns associated with screen reading material for extended periods, and also managing the large volume of electronic material that needs to be appraised.

Sensitivity review was also cited by two public bodies and one devolved administration as the process that would be the most resource intensive; the Welsh Government, Department of Health and the Ministry of Justice. It was also cited by one public body as the process that they envisaged would be the least resource intensive; The Royal Parks. Crucially, the departments that raised concerns about sensitivity review being the most resource intensive process are those that hold and process significant amounts of personal data, whereas bodies like The Royal Parks are not likely to hold huge amounts of personal data that could be deemed sensitive. The changing nature of sensitivities in digital records has been well documented in literature over the last few years and highlights that the content of the record is no longer the only consideration in terms of sensitivity (for example, Moss and Gollins, 2017). The increased risks of digital information have been discussed above and the fact that associations can be easily established between digital information from various sources ensures that increased accessibility comes hand in hand with increased risk. In the digital era there is a heightened risk that apparently innocuous statements combined with information already in the public domain can result in serious breaches (Gollins et al., 2014). The findings of the study highlight that digital transfer is not yet widespread across UK public bodies and the lack of experience, thus far, of public bodies is apparent through the fact that sensitivity review was not highlighted by more bodies as an issue in the digital age. This indicates that public bodies are not yet aware of the new risks associated with digital sensitivity because processes for the digital sensitivity of records either have not been established or have not been put to the test through transfer. The risks posed by the use, preservation and sharing of sensitive information are more heightened in the digital landscape. It is easier for information to be inadvertently released or be shared. Sensitivity reviewing digital information across different systems and platforms can be like looking for a needle in a haystack if carried out manually, especially given that establishing context between information held in various places is crucial. Current guidance on sensitivity review has focussed on keyword searching but this approach does not address the issue of context (Sloyan, 2016). The TNA Business Intelligence Review found that only a small number of public bodies were currently thinking about and tackling the challenges of digital sensitivity review (The digital landscape in government 2014-2015: Business intelligence review, 2016). The Welsh Government that has carried out a transfer of born-digital records identified the following issues when surveyed for the purposes of the current study: extracting or exporting the data from an EDRMS after selection, sensitivity review in terms of establishing what digital information should be withheld, and why, expressed in terms of exemptions and the reasons they apply, with details of when the exemptions expire or should be reviewed. The sheer lack of experience of digital transfer rendered the vast majority of other public bodies unable to specify specific issues. The risks relating to the sensitivity review of digital information are exasperated by the fact that public bodies keep more digital information than necessary and information can be difficult to locate by staff due to sheer volume, coupled
with the fact that information was sometimes saved in the wrong parts of corporate systems (The National Archives, 2015).

Technology assisted sensitivity review

The fifth survey question asked public bodies the following, *is the sensitivity review of born-digital records in your department technology assisted?* Not surprisingly, only the Welsh Government who had experience of digital transfer stated that their sensitivity review of digital records was technology assisted in that they used an eDiscovery tool. The Arts Council England, despite having no experience of digital transfer, stated that they used Nitro Pro 9 to go through documents and make any redactions or changes to format required to pass the information for the purpose of FOIA requests. The remaining bodies surveyed did not use technology for the sensitivity review of their born-digital records.

Application of freedom of information exemptions

The sixth survey question asked public bodies the following, *which Freedom of Information exemptions, if any, most apply/will apply to your department’s born-digital records at transfer stage?* The survey findings are on the whole in line with the data of the TNA Business Intelligence Review which found that public bodies closed items and pieces related to personal sensitivities at a rate of 75 per cent. The current study found that approximately 61 per cent of departments cited personal sensitivities in the form of Section 40 as the exemption most likely to apply to digital records upon transfer. Some departments cited more than one exemption that would apply to their digital records, which is reflected in the data. This was followed by approximately 35 per cent of departments who were unable to state which exemptions were most likely to apply. Approximately 17 per cent of departments cited national security (Section 24) as the exemption most likely to apply, and approximately 13 per cent of departments cited the law enforcement exemption (Section 31) and 13 per cent of departments cited the commercial interests (Section 43) exemption. Only 9 per cent of the departments surveyed cited the health and safety exemption (Section 38). There are, as mentioned, increased risks associated with sensitivity in the digital age, and that it is no longer solely the subject that renders a document sensitive, sensitivity should be considered within the context of who said what to whom, when, in what context, and the jurisdiction of review (Moss and Gollins, 2017). It is likely given that digital transfer is not as yet a business as usual activity, that large collections of records will be transferred closed to TNA, as departments may err on the side of caution especially given the heightened legislative focus on privacy, for example the European Union GDPR, and the sheer volume of information that would need to be reviewed. The use of technology in sensitivity review as a commonplace practice would be likely over time to decrease the volumes of digital records transferred closed to the archives.

Trigger date for transfer and outsourced IT

The seventh survey question probed departments about the trigger date they use for the transfer of their born-digital records to TNA. The answers provided were varied but did, to an extent, demonstrate some consistency in principle, if not in the terminology used. The Business Intelligence Review examined the challenge of departments understanding their digital holdings and what date to use as a trigger date for transfer. The review found that most public bodies had little or no sight of their complete digital legacy holdings – something that constituted a problem for departments as they do not know when their digital records are due to be transferred to The National Archives (The digital landscape in government 2014-2015: Business intelligence review, 2016). The findings of the current study found that 17 per cent of public bodies did not know what the trigger date would be,
25 per cent said it would be the date the record was last modified, 13 per cent stated that it would be the declaration date of the record, the point at which the content of a record is fixed and will no longer be modified. Both of the responses above can be said to essentially carry the same meaning and reflect good practice. Ambiguity in approach and a lack of awareness is apparent in the response provided by some departments that the creation date of the record would be used as the trigger date. This suggests a lack of awareness of the issues relating to digital information management and subsequent transfer, as a record can be modified after the creation date unless it is deemed to be of permanent value and will no longer be modified after creation, which is perhaps rare in practice. The research findings are in agreement with the findings of the Business Intelligence Review, as uncertainty and a lack of awareness still prevails, to an extent, with regard to trigger dates for transfer.

Outsourced IT
The eighth and final survey question asked public bodies whether they outsourced their IT services. The Business Intelligence Review also explored the challenges of outsourced IT. Outsourced IT is considered to be challenge for digital transfer because it can actually cost public bodies significant amounts of time and resources to try to introduce new software onto their systems, which is required for digital transfer by TNA (these include DROID, CSV and Teracopy, which are used at various points of the transfer process) (The digital landscape in government 2014-2015: Business intelligence review, 2016). The research findings of the current study found that fifteen of the twenty-three bodies surveyed outsourced their IT, whereas eight did not. The Business Intelligence Review found that 76 per cent of those departments surveyed used outsourced IT. This roughly correlates with the current research findings which found that 65 per cent of departments currently use outsourced IT.

Conclusion
The research carried out determined that digital transfer is not currently a business as usual activity across UK public bodies and that there is likely to be cases where public bodies are unable to meet the requirements of the transitional period, that requires that two years of records are transferred every year until 2023. This would indicate that digital records are more likely to be retained by departments or transferred closed in their entirety to save on resource sensitivity reviewing large volumes of records, or to err on the side of caution given the risks associated with digital information. The advice and guidance provided by TNA in the form of encouraging technology-assisted review will eventually change the processes and practice of digital records transfer in public bodies. However, it is likely that departments will develop new processes while actually undertaking digital transfer and not years in advance. Effective information governance requires that information assets are managed to ensure that corporate risk is minimalised and that accountability is a priority. The fact that digital transfer is not yet commonplace paints the following picture: public bodies are not yet legally required to transfer their born-digital records or they do not have the processes in place to prepare digital records for transfer. Even the most robust of processes for digital selection, appraisal and sensitivity review can only be as effective as the information professionals that undertake them. Investment in additional resources, particularly for digital sensitivity, not only in terms of sensitivity reviewers but also in terms of technological tools that can aid the identification of, and relationship between, sensitive information, is unavoidable. This investment in the skills required to work with digital records and technology to aid the undertaking of these processes, will result in greater commitment towards digital recordkeeping. The huge volumes of digital information created across government, coupled with its complexity and lack of organisation, will most likely result in more, rather than less, information being kept for permanent preservation.
References


Further reading


Corresponding author
Lale Ozdemir can be contacted at: laleozdemir6@gmail.com
“The margin between the edge of the world and infinite possibility”

Blockchain, GDPR and information governance

Darra Hofman, Victoria Louise Lemieux, Alysha Joo and Danielle Alves Batista

University of British Columbia, Vancouver, Canada

Abstract

Purpose – This paper aims to explore a paradoxical situation, asking whether it is possible to reconcile the immutable ledger known as blockchain with the requirements of the General Data Protection Regulations (GDPR), and more broadly privacy and data protection.

Design/methodology/approach – This paper combines doctrinal legal research examining the GDPR’s application and scope with case studies examining blockchain solutions from an archival theoretic perspective to answer several questions, including: What risks are blockchain solutions said to impose (or mitigate) for organizations dealing with data that is subject to the GDPR? What are the relationships between the GDPR principles and the principles of archival theory? How can these two sets of principles be aligned within a particular blockchain solution? How can archival principles be applied to blockchain solutions so that they support GDPR compliance?

Findings – This work will offer an initial exploration of the strengths and weaknesses of blockchain solutions for GDPR compliant information governance. It will present the disjunctures between GDPR requirements and some current blockchain solution designs and implementations, as well as discussing how solutions may be designed and implemented to support compliance. Immutability of information recorded on a blockchain is a differentiating positive feature of blockchain technology from the perspective of trusted exchanges of value (e.g. cryptocurrencies) but potentially places organizations at risk of non-compliance with GDPR if personally identifiable information cannot be removed. This work will aid understanding of how blockchain solutions should be designed to ensure compliance with GDPR, which could have significant practical implications for organizations looking to leverage the strengths of blockchain technology to meet their needs and strategic goals.

Research limitations/implications – Some aspects of the social layer of blockchain solutions, such as law and business procedures, are also well understood. Much less well understood is the data layer, and how it serves as an interface between the social and the technical in a sociotechnical system like blockchain. In addition to a need for more research about the data/records layer of blockchains and compliance, there is a need for more information governance professionals who can provide input on this layer, both to their organizations and other stakeholders.

Practical implications – Managing personal data will continue to be one of the most challenging, fraught issues for information governance moving forward; given the fairly broad scope of the GDPR, many organizations, including those outside of the EU, will have to manage personal data in compliance with the GDPR. Blockchain technology could play an important role in ensuring organizations have easily auditable, tamper-resistant, tamper-evident records to meet broader organizational needs and to comply with the GDPR.

Social implications – Because the GDPR professes to be technology-neutral, understanding its application to novel technologies such as blockchain provides an important window into the broader context of compliance in evolving information governance spaces.

This paper was funded under a Mitacs Accelerate Project Grant (IT12057) on “Blockchain-based Consent Management for Personalized Medicine”. The authors would like to thank our industry partner, Molecular You, and our fellow research team members Dean Regier, Samantha Pollard, Deidre Weyman, Hoda Hamouda, Ravneet Kaur, Usman Mukaty, Wen Pan, Adrian Bogdan and Greg McLeod.
Originality/value – The specific question of how GDPR will apply to blockchain information governance solutions is almost entirely novel. It has significance to the design and implementation of blockchain solutions for recordkeeping. It also provides insight into how well “technology-neutral” laws and regulations actually work when confronted with novel technologies and applications. This research will build upon significant bodies of work in both law and archival science to further understand information governance and compliance as we are shifting into the new GDPR world.

Keywords Privacy, Blockchain, Distributed ledger technology, General data protection regulations

Paper type Research paper

Introduction
The arguments for, and challenges of, information governance are fairly well-known at this point: information is a vital asset that must be managed properly to reduce risk, ensure compliance, support decision-making and improve strategy (Naylor, 1993). Of course, meeting such broad objectives has led to the emergence of information governance as:

 [...] an all-encompassing term for how an organization manages the totality of its information [...] IG includes the set of policies, processes, and controls to manage information in compliance with external regulatory requirements and internal governance frameworks (Smallwood, 2015, p. 6, emphasis in original).

Information governance (IG) is still very much a developing field, but one that:

 [...] is capable of initiating a paradigm shift in the world of information management [...] integrating] elements and principles already exist[ing] under a well understood [Enterprise Information Management] approach [with] enforced integration and highly connected interaction (Hagmann, 2013, p. 229).

IG is broader than, but indivisible from, records and information management (RIM). All of the IG models that Hagmann considers have an orientation toward RIM, including ARMA’s Generally Accepted Recordkeeping Principles (GARP®), which includes the principle of privacy – a topic of growing concern to RIM professionals. Information and communication technologies (ICT) contributed thus far to significant concerns about privacy and personal data protection and a growing lack of trust in technology companies with business models that rely on gathering, processing and commoditizing personal data. Within the European Union, the response to these concerns has been to pass the General Data Protection Regulations (GDPR), which came into effect on May 25, 2018, to provide better safeguards for the protection of personally identifiable data.

Like the GDPR, blockchain technology has emerged out of individuals’ lack of trust (e.g. in centralized “trust” authorities). Blockchain seeks to by-pass centralized trust authorities to enable individuals to transact with one another “trustlessly,” without reliance on the traditional mediating trust authorities. While blockchain is being posited as a solution to the problem of trust, paradoxically, a growing number of projects exploring the application of blockchain technology for identity management and health recordkeeping raise questions about whether blockchain solutions may lead to infringement of individual’s right to privacy, perversely generating greater levels of social mistrust. This paper explores this paradoxical situation, asking whether it is impossible to reconcile the immutable ledger known as blockchain with the requirements of the GDPR, and more broadly privacy and data protection.

Methodology
This research used a critical interpretive synthesis (Dixon-Woods et al., 2006; McFerran et al., 2017) of the archival, legal, organizational and computer science literature to establish the
existing understandings of blockchain and information governance, blockchain and GDPR, GDPR and information governance, and the intersection of the three. A critical interpretive synthesis (CIS) “aims to develop new knowledge based on capturing and critiquing the key ideas from existing literature” (McDougall, 2015, p. 525). A critical interpretive synthesis is the appropriate choice for this research due to both the nature of the research questions and the study’s qualitative, exploratory nature. McDougall (2015, p. 526) describes why a critical interpretive synthesis is more appropriate to her field, bioethics, than the systematic literature review that is more common in other health fields: “In bioethics work, our questions tend to focus on ethical justifiability and deal in conceptual analyses and arguments”; a strong, justifiable argument is not weighed by one more study in the same way that a more quantitative question, such as the efficacy of a particular intervention, would be (McDougall, 2015, p. 527). This study, too, is interested in justifiable analyses and arguments; for the purposes of this research, a persuasive argument is more meaningful than one that merely appears frequently. Perhaps what most distinguishes CIS from conventional systematic review methods is its rejection of a “stage” approach to review. Processes of question formulation, searching, selection, data extraction, critique and synthesis are characterized as iterative, interactive, dynamic and recursive rather than as fixed procedures to be accomplished in a predefined sequence (Dixon-Woods et al., 2006, p. 9). To illustrate, in this study, we initially searched literature in English in which the keywords “GDPR,” “blockchain,” “information governance” and “information management” appeared in any combination. The initial literature found from this search was used to refine our analysis and guide future searches (for example, searches concerning “blockchain and right to erasure” or “information governance and privacy by design”). As represented in the authors’ depiction below, critical interpretive synthesis is a “more organic process that fitted better with the emergent and exploratory nature of the review questions. This combined a number of strategies, including searching of electronic databases; searching websites; reference chaining; and contacts with experts. Crucially, we also used expertise within the team to identify relevant literature from adjacent fields not immediately or obviously relevant” (Dixon-Woods et al., 2006), with the varying elements of analysis happening concurrently and iteratively. Because of the informal, organic process of analysis in a CIS, there are no analytical tools available that can be shared directly (Figure 1).

Findings

Introduction to GDPR: the principles and information governance

The GDPR is a response to the high-omnipresent surveillance state that modern ICT, in conjunction with the other regulatory forces at play, including our economic, legal and social systems, have permitted to flourish. The GDPR establishes data protection as a fundamental right of EU citizens and has fairly ambitious goals:

(1) The principles of, and rules on the protection of natural persons with regard to the processing of their personal data should, whatever their nationality or residence, respect their fundamental rights and freedoms, in particular their right to the protection of personal data.

(2) This Regulation is intended to contribute to the accomplishment of an area of freedom, security and justice and of an economic union, to economic and social progress, to the strengthening and the convergence of the economies within the internal market and to the well-being of natural persons (Recital 2).

In support of these goals, GDPR outlines six “principles relating to processing of personal data”: lawfulness, fairness and transparency; purpose limitation; data minimization; accuracy; storage limitation; and integrity and confidentiality (Article 5, Section 1); these six principles are...
underlined with a seventh, overarching principle of accountability on the part of data controllers. These principles will, by and large, seem familiar to RIM and IG professionals. This is because GDPR places the expectation of good information governance on data controllers and processors in their use personal data. Rom mapped ARMA’s GARP® to a non-exhaustive set of GDPR provisions (Rom, 2018) (Table I):

Of course, ARMA’s is far from the only maturity model available for information governance; much work remains to be done in developing our understanding of the relationship between GDPR and IG. For example, future work mapping GDPR to the maturity model for information governance developed by Proença et al., given its European focus and Design Research basis, could provide rich insights into the interrelationship between GDPR and IG (Proença et al., 2016). Ultimately, however, Schoch makes much the same point as Rom: GDPR is an opportunity to put IG front and center in organizational decision-making.

[GDPR . . .] may help us build the business case for information governance (IG), providing the urgency required to bring the stakeholders to the table . . . Protection of privacy[1] becomes . . . the camel’s nose in the tent to bring IG to the forefront of organizational strategy (Schoch, 2016).

Data processing requirements and cross-border data flows

Decentralization, jurisdiction and compliance

Of course, while IG is concerned with all information across an organization, the GDPR is narrower in its scope. The GDPR applies only to “personal data” that is “processed” within both the material and territorial scope of the statute. There are no limitations under the GDPR to the transfer or processing of data that falls outside of these boundaries. For example, fully anonymized data is per se not personal data, and is therefore not subject to the GDPR. Similarly, data processors or controllers who are not “established” within the EU and who do not offer goods or services to EU residents or monitor the behavior of EU residents are beyond the territorial scope of the GDPR, and not subject to any restrictions on cross-border or third country data flow thereunder, though they may be subject to data protection, privacy or data localization laws within the jurisdictions in which they operate. For those activities which are
<table>
<thead>
<tr>
<th>GARP principle</th>
<th>Description</th>
<th>Mapping to articles in GDPR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Principle of accountability</td>
<td>A senior executive (or a person of comparable authority) shall oversee the Information Governance program and delegate responsibility for information management to appropriate individuals</td>
<td>Art. 37 GDPR (Data Protection Officer) Art. 24 GDPR (Controller) Art. 27 GDPR (Representation of the controller) Art. 28 GDPR (Processor)</td>
</tr>
<tr>
<td>Principle of transparency</td>
<td>An organization’s business processes and activities, including its Information Governance program, shall be documented in an open and verifiable manner, and that documentation shall be available to all personnel and appropriate, interested parties</td>
<td>Art. 5 Paragraph 2 GDPR (Controller’s responsibility) Art. 12 GDPR (Transparency) Art. 13 GDPR (Information and Access) Art. 14 GDPR (Information if data was not received from data subject) Art. 19 GDPR (Notification about Erasure and Rectification) Art. 25 GDPR (DP by Design and Default) Art. 30 GDPR (Records of Processing Activities) Art. 40 GDPR (Codes of Conduct)</td>
</tr>
<tr>
<td>Principle of integrity</td>
<td>An Information Governance program shall be constructed so the information assets generated by or managed for the organization have a reasonable guarantee of authenticity and reliability</td>
<td>Art. 5 Paragraph 1 lit b-e GDPR (Principles) Art. 16 GDPR (Rectification) Art. 17 GDPR (Erasure)</td>
</tr>
<tr>
<td>Principle of protection</td>
<td>An Information Governance program shall be constructed to ensure an appropriate level of protection to information assets that are private, confidential, privileged, secret, classified, essential to business continuity, or that otherwise require protection</td>
<td>Art. 5 GDPR (Principles relating to processing personal data) Art. 24 GDPR (Measures to be implemented by Controller) Art. 32 GDPR (Security of Processing) Art. 44 ff GDPR (Transfers of Personal Data to 3rd Countries and International Organizations)</td>
</tr>
<tr>
<td>Principle of compliance</td>
<td>An Information Governance program shall be constructed to comply with applicable laws, other binding authorities and the organization’s policies</td>
<td>GDPR in general and specifically Art. 6 GDPR (Lawfulness of processing) Art. 47 GDPR (Binding Corporate Rules)</td>
</tr>
<tr>
<td>Principle of availability</td>
<td>An organization shall maintain its information assets in a manner that ensures their timely, efficient and accurate retrieval</td>
<td>Art. 15 GDPR (Right of access by the data subject) Art. 20 GDPR (Data Portability)</td>
</tr>
<tr>
<td>Principle of retention</td>
<td>An organization shall maintain its information assets for an appropriate time, taking into account its legal, regulatory, fiscal, operational and historical requirements</td>
<td>Art. 5 Paragraph 1 lit. e GDPR (retention) Art. 15 GDPR (Right of access by the data subject)</td>
</tr>
<tr>
<td>Principle of disposition</td>
<td>An organization shall provide secure and appropriate disposition for information assets no longer required to be maintained, in compliance with applicable laws and the organization’s policies</td>
<td>Art. 5 GDPR (Principles) Art. 17 GDPR (Erasure) Art. 20 GDPR (Data Portability) Art. 30 Paragraph 1 lit. f GDPR</td>
</tr>
</tbody>
</table>
subject to the GDPR, the GDPR differentiates between “crossborder data flow” (data transfers in the context of multiple Member States) and transfers to third countries (countries outside the EEA). The transfer of data subject to the GDPR to a third country must occur under one of several conditions outlined in the regulation (and discussed in detail infra); in short, transfers must be to an “Adequate Jurisdiction” or pursuant to a legal data transfer mechanism, an exemption, or a derogation. Crossborder transfer of data already available through a “public register” is provided for in the regulation, although this is more limited than “public realm.” The broad question of data in the public realm, but outside of public registers, seems to have been answered in such cases where the data subject has shared the data in question. Pursuant to Article 9(2)(e), even sensitive personal data may be processed in such case where “processing relates to personal data which are manifestly made public by the data subject.” There remains an open question with regard to personal data that are in the public realm but have not been made so by the data subject.

The GDPR defines two different types of personal data, with different protections applied to each category: “personal data” and “sensitive personal data.” “Personal data,” as defined in Article 4(1), “means any information relating to an identified or identifiable natural person (“data subject”); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.” Thus, fully anonymized data sets are beyond the scope of the GDPR and not subject to regulation thereunder. Pseudonymization is insufficient to remove data from the category of “personal data” (and therefore from regulation), although it is recommended. Personal data may be processed only pursuant to a lawful basis; lawful bases for processing (Article 6(1)(a–f)) are:

- the data subject consents to the processing of his/her data for one or more specific purposes;
- contractual necessity (under a contract to which the data subject is party);
- complying with the processor’s legal obligation;
- protecting the “vital interests” of a natural person, including the data subject;
- performing a task in the public interest or to exercise the controller’s official authority; and
- “the legitimate interests” of the controller or a third party, unless those interests “are overridden by the interests of fundamental rights and freedoms of the data subject.”

These bases are largely similar to those under the EU’s previous data protection regulation, Directive 95/46, although the statute clarifies that the “vital interests” language applies to third parties and not just data subjects; furthermore, although “consent” as a lawful basis is consistent between the Directive and the GDPR, the bar to obtain consent is much higher under the GDPR.

Some personal data, however, is classified as “sensitive personal data” under the GDPR, and much more strictly regulated. The GDPR’s regulation of sensitive personal data restricts the processing of data:

[...] revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or that track union membership, and the processing of genetic data, biometric data for the purpose of identifying a natural person, data concerning health, or data concerning a natural person’s sex life or sexual orientation.

The processing of such data is prohibited unless one of ten grounds applies, such as explicit consent on the part of the data subject to the processing of the sensitive personal data, the
data being made “manifestly” public by the data subject, or when processing the sensitive personal data is necessary for providing medical care (Article 9, Section 2).

Even if records contain personal – or even sensitive personal – data, the GDPR might not be applicable. The GDPR only regulates data processing activities that fall within both the material scope and territorial scope of the regulation. Data processing activities outside of either scope are per se beyond the reach of the GDPR. Article 2, Section 1 of the GDPR defines the material scope of the regulation:

This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

Article 2, Section 2 carves out four significant exceptions to the above language:

(1) activities outside of the scope of EU law;
(2) activities falling within Chapter 2, Title V of the Treaty of the European Union (foreign and security policy within member states);
(3) data processing by “a natural person in the course of a purely personal or household activity; and
(4) data processing for law enforcement purposes.

“Processing” is further defined within the GDPR as:

[... ] any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction (Article 4 (2)).

The extensive definition of “processing” means that almost any activity involving “personal data” is within the material scope of the GDPR.

However, even if a data processing activity is within the material scope of the GDPR, it will not be regulated thereunder unless the activity and/or the data processor/controller is also within the territorial scope of the GDPR. The GDPR establishes two different ways by which a data processor or controller could be found to be within the territorial scope of the regulation. The first clause of Article 3 of the GDPR holds that:

This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not (Article 3, Section 1).

“Establishment” is not defined in the statutory language, however, the courts have held previously that the concept of “establishment”, within the meaning of Directive 95/46, extends to any real and effective activity – even a minimal one – exercised through stable arrangements (Case C230/14 Weltimmo v NAIH [2015] ECLI:EU:C:2015:639). This broad definition makes it clear that even minimal ties to Europe will likely be sufficient to bring an organization (and therefore its data practices) within the scope of the GDPR.

However, a data processor/controller need not be established within the EU for its data processing to be subject to the GDPR. The second clause of Article 3 holds that GDPR:

[... ] applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:
1. the offering of goods or services, irrespective of whether a payment of the data subject is
required, to such data subjects in the Union; or 2. the monitoring of their behaviour as far as their
description takes place within the Union (Article 3, Section 2).

The breadth of this language should be noted: “data subjects who are in the [EU].” The
citizenship of the data subjects is immaterial to the applicability of the GDPR; if the data
processor/controller is offering goods or services to, or monitoring the behavior of, natural
persons within the EU, that processor/controller is likely within the scope of the GDPR and
must comply therewith.

Privacy by design and by default
In addition to setting forth numerous substantive requirements for data controllers and
processors, GDPR also enshrines “data protection by design and by default” (Article 25).
Privacy by design, originally developed by Ann Cavoukian in the 1990s, encompasses: “IT
systems, accountable business practices; and physical design and networked infrastructure”
(Cavoukian, 2011), an integrated approach that will ring familiar to IG professionals.
Privacy by design encompasses seven principles, of which privacy by default is one, along
with a proactive, preventative approach, privacy embedded into the design of systems (both
IT and business), as a positive-sum, with full lifecycle protection, visibility and
transparency, and a user-centric orientation (Cavoukian, 2011). While much of the GDPR
provides mandatory standards – a compliance floor, as it were – privacy by design and by
default embodies more of an aspirational standard, a vision of data protection as an integral
part of practices and processes. However, because this aspirational standard is given the
force of regulation through GDPR, organizations must work to make data protection an
inherent, ongoing, integrated part of their information governance.

A particular problem: the “right to be forgotten”
Finally, the “right to be forgotten,” or the right to erasure, adds a new urgency to
information governance for organizations that control or process data that falls within the
scope of the GDPR.

The right to erasure, Article 17, provides that:

[a] data subject shall have the right to obtain from the controller the erasure of personal data
concerning him or her without undue delay and the controller shall have the obligation to erase
personal data without undue delay where [one of the legislative] grounds applies (Article 17,
Section 1).

This right is not absolute; the data subject may apply to have his/her/their data erased only
when one of the six legislative grounds outlined in Article 17 applies. A data controller/
processor may deny the application if, for example, there is a legal requirement to keep the
information. Furthermore, GDPR specifically exempts data processing “for archiving
purposes in the public interest, scientific or historical research purposes” from the right to
erasure. Despite these limitations, a number of circumstances exist wherein the right to
erasure might well apply to a blockchain information solution. Consider this from an
information governance perspective: the controller has to be able to identify the subject’s
personal data in its control, be able to examine its processing (as unlawful processing is a
ground for erasure), and to erase that data from the controller’s records. The controller must
also be able to prove when one of the exceptions to the right to erasure applies (Article 17,
Section 3). Unless the controller has very strong information governance in place, complying
with the right to erasure could prove to be an extremely expensive, time-consuming process –
and possibly even impossible, subjecting the controller to penalties for non-compliance.
What is blockchain technology?
It can be challenging to define “blockchain technology,” in part because there is no consensus as to which of the many distributed ledger technologies falls within (or without) the blockchain universe. While there is no universally agreed upon definition of blockchain technology (used interchangeably in this paper with “blockchain”), it can be understood as “a distributed ledger that maintains a continually growing list of publicly accessible records cryptographically secured from tampering and revision” (Lemieux, 2016, p. 5). Part of the definitional challenge arises from the fact that there exists a diversity of blockchain technologies. At a fundamental level, all blockchain technologies distribute a ledger of transactions over numerous computers (nodes); each node runs software that continuously verifies and replicates the most recent copy of the ledger. Each transaction must be validated according to the blockchain’s consensus mechanism. A validated transaction is then hashed; its hash is then put with the hashes of other transactions to form a “block.” These blocks are added to the blockchain, with the “block hash” (the hash of the hashes of the previous block) becoming the first hash in the next block. This prevents the contents of previous blocks being changed, making for a tamper-resistant, tamper-evident ledger of transactions. It is these features of blockchain that cause it to be characterized as an “immutable” ledger. Essentially, once information is written to a blockchain, it is not meant to be altered or removed, but should, in theory, remain immutably intact in perpetuity[2]. Because blocks are time-stamped and redundancy is built into the system, blockchains are also highly auditable. Their design makes blockchains an excellent option for ensuring the integrity of records.

While there exist different kinds of consensus mechanisms, the concept of the consensus mechanism is central to the disruptive potential of blockchain technology. Blockchain transactions are not authenticated by a trusted authority; in fact, no authority, legal or otherwise, validates the blockchain. Instead, trust is placed in the algorithms underlying the consensus mechanisms. This is the basis for the characterization of blockchain as a “trustless system which, theoretically, could offer an automated, hyperefficient means of executing and documenting transactions without the error prone, cost-inducing interference of trusted authorities, individual or institutional. Although a purely “trustless” system, beyond the need for third parties such as courts to mediate claims and resolve disputes is unlikely, a growing number of sectors are capitalising on blockchain’s tamper-resistance, disintermediation, and auditability, including financial services, health care, and supply chain management. These blockchains are generating and/or securing countless records which must be included in organizations’ broader information governance frameworks to “ensure the effective and efficient use of [that] information in enabling [the] organization to achieve its goals” (Logan, 2010).

What are the information governance implications of blockchain technology?
Gartner, in its Hype Cycle for Emerging Technologies in 2018, found that blockchain is part of a broader trend of “digitalized ecosystems,” which are “ecosystem enabling platforms […] laying the foundation for entirely new business models that are forming the bridge between humans and technologies” (Panetta, 2018). Managing these new models, however, will require adapting – or even developing new – models of information governance. Based on North’s suggestion that blockchain is a trust technology for retention, let us consider blockchain solutions, as currently built, vis-a-vis records retention. A standard tool to maximize the asset value of records (and minimize the risks of retaining records through defensible disposition) is a retention schedule. Retention schedules are as variable as the organizations that use them, but, whether they use big buckets or small, they all rely on
some form of records classification to identify the appropriate retention period for given records. Classifying blockchain records is extremely challenging in part because the archival bond[3] is not natively instantiated on the blockchain. Significant metadata must be added to blockchains to relate transactions to the procedures in which they participate; without knowing the identity of a record, it is difficult, if not impossible, to determine the appropriate retention period (a draft contract is a very different matter from an effective contract). Lemieux and Sporny explain the centrality of the archival bond to the identity of records:

[... ] the identities of the documents as records (i.e., evidence of facts about acts or transactions) are completely different by virtue of the different procedures of which they form a part (as represented by the archival bond). In the case of digital records, it would be impossible to prove that a record was an authentic representation (i.e., a copy) of another record, unless both items (the one to be proven authentic and the one that was reproduced) have unique identities. [... ] the archival bond must be made explicit and interpretable in order to ascertain the unique identity of each document as a record of the procedurally bound facts contained within it (Lemieux and Sporny, 2017).

Gartner describes blockchain as sliding from the pinnacle of the Hype Cycle towards the “Trough of Disillusionment,” a point in a technology’s development wherein “interest wanes as experiments and implementations fail to deliver [... ] and [i]nvestments continue only if the surviving providers improve their products to the satisfaction of early adopters” (Gartner Hype Cycle, 2018). A significant number of the improvements that must be made to blockchain solutions have to do with the fundamental RIM function that blockchains serve; to meet ongoing organizational needs in those cases where blockchain solutions are implemented, much more must be understood about blockchain records from an IG perspective. This understanding will require examining the complex, integrated, social, data and technical layers of blockchain technologies.

Blockchain solutions offer a number of appealing aspects from an information governance perspective. They offer disintermediation, which can be invaluable for shared records in situations of low trust (such as between financial institutions). They generate and validate transactions automatically, without human intervention, which can reduce the work necessary to create records and increase compliance. They offer technical transparency, the ability of a technical solution to make information available and/or accessible, which can support process transparency and even organizational transparency. They are also tamper-resistant and tamper-evident, which can increase records’ security and auditability.

However, blockchain technology was originally designed, not as a recordkeeping solution (or even a database) writ large, despite many assertions that blockchain can function as a recordkeeping system or archives, but to support exchange of the cryptocurrency Bitcoin. If blockchain technologies are to become a central part of our records’ infrastructure, their IG challenges must also be addressed. For example, in cases where a blockchain is used to ensure the integrity of records generated outside the blockchain, there is nothing about a blockchain which guarantees such records are accurate or reliable (Lemieux, 2016). As noted above, the archival bond is not natively instantiated on the blockchain, making records identification and classification challenging. The tamper-resistance of the blockchain makes it difficult, if not impossible, to correct, redact and/or destroy records. And, as will be discussed infra, the transjurisdictional, distributed nature of the blockchain can pose significant compliance challenges when blockchains are used to manage organizations’ information assets. Moreover, as blockchain solution providers have sought to assert the blockchain’s place as a recordkeeping system, they have placed ever growing amounts of
data, some personally identifiable, on the blockchain. In many cases, they have written this information in clear text, rather than the cipher text of a hash, causing such information to be immutably recorded in an open public ledger. Such shortcomings in the technical design and use of blockchain from an IG perspective raise serious questions about whether the technology can ever meet GDPR requirements.

Findings from the literature: a novel challenge

A search of the literature revealed a very small number of articles and some grey literature which address either blockchain and GDPR or blockchain and information governance. A greater amount of literature, particularly grey literature, addresses GDPR and information governance. No literature was found which addresses the intersection of blockchain and GDPR from an information governance perspective. All three of these keywords appeared in Lomas and McLeod (2017); however, their study was focused on ICT professionals’ view of the challenges attendant to the Brexit vote. Their mention of blockchain is largely outside the scope of the article, but it does nicely frame the breadth of the challenge of blockchain in a GDPR world from an IG perspective:

Technological change has played a leading role in global transformation, impacting on the economy, trade, warfare, political mobilization and identity formation . . . ] In addition, ICT has been claimed to operate across and even transcend borders and legislative regimes (Lomas and McLeod, 2017).

One theme which emerges in the literature is the use of blockchain for automated data protection management. Ibáñez et al. capture much of the work currently being done with regard to blockchain and data protection both within and without Europe when they posit fairly sophisticated technical solutions for data protection, a model they call “Consent 2.0” wherein data subject consents and a “structured description of what processing the data subject] allows for her data” are captured on the blockchain (Ibáñez et al., 2018). Although it relies on technologies that are still nascent, such as secure multi-party computation, homomorphic encryption and ontologies and controlled vocabularies to capture consent (Ibáñez et al., 2018), blockchain data protection management emerges as a solution throughout the literature. Wirth and Kolain assert that “Web 3.0, in combination with blockchain technology and modern cryptography, can bring personal data management to a level of privacy and security that prioritizes individual sovereignty and shared transparency” (Wirth and Kolain, 2018, p. 1); they, too, propose “a blockchain-enabled-architecture that builds upon the idea of Privacy by Design [. . .] to protect personal information in the digital world” (Wirth and Kolain, 2018, p. 2). A number of other privacy-protecting technical solutions are being developed, including ring confidential transactions, which obscure sender, receiver, and amount of a transactions, and zero-knowledge proofs, a cryptographic method by which a party can prove that they know a particular secret value \( x \) without revealing the secret. These techniques are currently immature, however (Ibáñez et al., 2018).

Perhaps unsurprisingly, a second theme that arises in the literature is the challenges of blockchain vis-à-vis GDPR. The GDPR largely arose in the context of an internet supported by centralized cloud technologies; blockchain, by contrast, relies upon a distributed architecture (Lima, 2018). This poses a particular problem when it comes to determine who is a data controller or processor within the scope of GDPR when personal data is processed on a blockchain (Ibáñez et al., 2018; Lima, 2018; Maxwell and Salmon, 2017; van Geelkerken and Konings, 2017). Theoretically, every miner on a permissionless public Blockchain could be a controller within the meaning of GDPR. In addition, the right to be forgotten, discussed
supra, is identified as a particular problem with regard to a technology which boasts immutable records as one of its primary strengths. As Lima notes, “the immutability of data transactions that are imprinted in the fabric of [blockchains] implies that one of the key principles of GDPR, Art. 17 right to erasure […] is not met by Blockchain” (Lima, 2018, p. 2). As Maxwell and Salmon note, the right to erasure will prove a particularly interesting question because, as it stands, “[what] constitutes “erasure” is still open to debate” (Maxwell and Salmon, 2017, p. 15).

A third theme which emerges in the literature – both the GDPR/blockchain and the GDPR/information governance literature – is the importance of strategic concerns in building and implementing solutions. As Blair points out, GDPR is:

[…] only the latest example of the myriad ways that the collection, use, storage, and governance of information is being regulated […] these laws and regulations share a singular theme: organizations need to understand and govern their data (Blair, 2018, p. 45).

Ibáñez et al. point to the very human questions in the interplay between GDPR and blockchain:

In the GDPR scenario, data subjects do not completely trust data controllers and are now entitled to more control on how their data is processed […] blockchain may turn out to be a powerful tool to implement [privacy by design and default] (Ibáñez et al., 2018).

**GDPR does not work with blockchain […] Or does it?**

There is a dominant narrative that blockchain and GDPR cannot play well together. As Lima puts it, “most of the initial reaction regarding Blockchain is that this new technology is not compatible at all with the new GDPR directives” (Lima, 2018, p. 5). Our research, however, points away from this dominant narrative; this observation by Lima seems more accurate:

Blockchain can be considered as technology that can not only improve the fundamental aspect of data privacy and security, as specified in GDPR […] and can also be carefully studied, architected and implemented with GDPR-compliance intent for data privacy, using some unique techniques. These alternatives are not simple to implement, and they require deep understanding of how Blockchain works and how the technology ecosystem is interrelated, to create GDPR-Blockchain compatible architectures (Lima, 2018, p. 5).

The problems identified in the literature above – right to erasure, defining data controllers, finding and identifying personal data on blockchains – are being actively researched for solutions (Figure 2). For example, the most commonly proposed solution to “erase” data from the blockchain is irreversible encryption (i.e. revoking access rights to data to render it inaccessible), but it remains to be seen if such a solution will receive the law’s approval (Maxwell and Salmon, 2017; van Geelkerken and Konings, 2017; Wirth and Kolain, 2018). Another proposed solution – one that is commonly implemented now – is simply to store personal data off-chain, with pointers held on chain (Lima, 2018).

We found three blockchain-based GDPR compliance products being offered on the market[4], indicating that blockchain technology is viewed by some as helping, rather than hindering GDPR compliance. VOLTA is an application developed by Guardtime to provide organizations with a solution for GDPR compliance and is designed to support governance and compliance processes for managing personally identifiable information (PII) identified by the GDPR. VOLTA integrates disparate systems and workflows (e.g. applications, processes and services) to track how PII is used. VOLTA accomplishes integration by supporting “light-touch interfaces such as CSV and REST” and by “enabling user-defined
policies to be applied on all transactions associated with personal data handling.” PikcioChain, by contrast, has more of a “data mart” approach. PikcioChain is a distributed permission-based platform developed by Pikcio AG, which focuses on the collection, certification, verification and exchange of personal data. PikcioChain enables businesses to trade and exchange personal data, while giving individuals control over their own personal data and the chance to be compensated for its use. Finally, GDPR Edge is an enterprise-oriented compliance solution which combines a blockchain with a data lake. Each of these solutions targets a different segment of needs in the post-GDPR era, showing the diverse applications that people are imagining for using blockchains in a manner that supports a GDPR compliant-world.

Significance of design

One of the central findings of this work is the importance of design in blockchain systems. As noted in the opening of this paper, defining blockchain technology is challenging in part because of the diversity of blockchain solutions that exist. Ensuring that a blockchain solution meets information governance needs, including compliance with legislation such as GDPR, requires thoughtful design up front; the design must address a range of issues, including data and records flows and architectures and the impact of those flows and architectures on data protection and (non-) compliance. Blockchain technologies, as noted supra, are sociotechnical systems with interdependent social, data/records and technical layers. Ensuring compliance at the social layer requires a holistic consideration of all the layers of the system and their interactions:

For example, Lima finds that, with regard to GDPR compliance:

The main challenges are related to public permissionless Blockchain technologies where, due to how the blocks and Blockchain transactions are built, all information and records that enter the distributed ledgers [...] are publically visible, tamper-proof and immutable, which means that the data added to the public permissionless Blockchain is there forever (Lima, 2018).

Even private, permissioned blockchains, however, could easily fall afoul of the law if not correctly designed and implemented; a blockchain that is not built in such a way as to facilitate finding and making available all of a data subject’s data, for example, poses a problem when the subject asserts his/her/their rights under GDPR.
Discussion

Obligations, rights and the “Transparency paradox”

At the heart of GDPR is the idea of empowering data subjects by acknowledging data protection as a fundamental right and providing individuals with greater power to know and control who has their data and what is being done with it. At the core of this idea is informed consent on the part of the data subject. One common assertion is that blockchain can improve and even automate the management of data protection consents by increasing transparency. As van Geelkerken and Konings state, [...]. Blockchain greatly increases transparency amongst its participants. Seeing as any participant to the Blockchain [...] can access all contents of the Blockchain, the exchange of data or information is transparent (van Geelkerken and Konings, 2017).

However, it is a longstanding problem in privacy scholarship that the mere availability of information is not enough to make consent informed. Nissenbaum terms this:

[...] the transparency paradox [...] If notice (in the form of a privacy policy) finely details every flow, condition, qualification, and exception, we know that it is unlikely to be understood, let alone read. [...] An abbreviated, plain-language policy would be quick and easy to read, but it is the hidden details that carry the significance (Nissenbaum, 2011, p. 36).

Even if Nissenbaum’s transparency paradox were to be overcome, there exist real questions as to what – if any – choice data subjects truly have when we consent to opt-in/opt-out “clickwrap,” when opting out can effectively marginalize or exclude an individual from the life of society. This is particularly pernicious in the case of government records when it comes to information shared with the government – in the incredible reams of vital records, property records, voting records, court records – any “consent” given to the collection, use, and sharing of personal information is, in reality, pro forma (Solove, 2002).

It remains to be seen whether or not blockchain solutions can help solve the transparency paradox and make informed consent to the use of personal data easier and/or more meaningful. As noted supra, the use of blockchain for informed consent management is being tested heavily in the medical domain, to “[reimagine] consent from, a one-time event [to a process that] is ongoing, dynamic, and granular, allowing participants to change their mind” (Hofman et al., 2018, p. 1651, citing Kirby et al., 2013). However, while medical data are sensitive personal data, the challenges of informed consent transcend medical data. Whether blockchain, GDPR, or both can actually resolve the data protection challenge remains to be seen. However, because of the increased data subject rights under GDPR, it is critical that organizations be aware of and use all the tools at their disposal to enable compliance.

To capitalize on the strengths of blockchain technologies for GDPR compliance, a much richer understanding of their role in RIM and IG is necessary. The technical understanding of blockchain technologies is perhaps the best understood, as blockchains are built on the integration of technologies such as cryptography and hashing that have rich bodies of research. Some aspects of the social layer of blockchain solutions, such as law and business procedures, are also well understood. Much less well understood is the data layer, and how it serves as an interface between the social and the technical in a sociotechnical system like blockchain. In addition to a need for more research about the data/records layer of blockchains and compliance, there is a need for more information governance professionals who can provide input on this layer, both to their organizations and other stakeholders. Given the central importance of design to the effectiveness and compliance of these solutions, information
governance professionals must be at the table when their organizations are designing and implementing such solutions to advise on data/records requirements, such as GDPR compliance, data/records architectures and flows.

**Blockchain and the ability of “technology neutral” law to regulate novel technologies**

GDPR is meant to protect rights in a way that is “technologically neutral and should not depend on the techniques used” (Recital 15). This is not an uncommon statement in ICT regulation. However, it is a problematic one. Invocations of “technology neutrality” can serve several different purposes within regulations. Koops finds that claims that an ICT regulation is “technology neutral” have a number of different meanings and purposes, including:

1. **Addressing the purpose of the regulation:**
   - (A1) The “technology neutral” law regulates functions and effects rather than means; and/or
   - (A2) Being “technology neutral” dictates that what holds offline should also hold online;

2. **Addressing the consequences of regulation:**
   - (B1) The regulation should not discriminate against certain technologies; and/or
   - (B2) The regulation should not hinder the development of ICT;

3. **Serve as a legislative technique:**
   - (C1) The law should be sustainable in the face of further technological development; and/or
   - (C2) The regulation should be subsidiary and proportionate; and/or even
   - (C3) The law should be transparent (Koops, 2006).

These requirements are broad, distinctive, and sometimes contradictory. “[The] requirement of sustainability (C1), on the one hand, and subsidiarity, proportionality and transparency (C2 and C3), on the other, are contradictory to a certain extent. That is, legislation that is too much focused on sustainability and hence abstracts very much away from technology will result in vague laws that provide little legal certainty” (Koops, 2006). Koops comes down in favor of “technology-neutral” being a legislative technique (C), attempting to find a balance between the need for certainty in the law and the heightened risk of obsolescence when regulation aimed at ICT is tied to a specific technology (Koops, 2006). However, he also highlights that from this sustainability/certainty starting point, a number of trade-offs must be made and explicitly considered to achieve useful legislation.

The significant uncertainty surrounding how blockchain will be regulated under GDPR stems, in part, from the fact that GDPR is a “technology neutral” in the broad, contradictory undefined sense. The GDPR does clarify that it explicitly intends to be technology neutral in the (A2) sense, in that paper-based systems containing personal data are also subject to regulation under GDPR. However, because the GDPR intends to sweep any data- and record keeping technology that could include personal data into its purview, the balance between sustainability and certainty swing heavily toward sustainability. A number of questions – is unbreakable encryption erasure? Is every miner a data controller? Are there compliant ways to store personal data on-chain? – will have to be answered moving forward.

**Conclusion**

Managing personal data will continue to be one of the most challenging, fraught issues for information governance moving forward; given the fairly broad scope of the GDPR,
many organizations, including those outside of the EU, will have to manage personal data in compliance with the GDPR. Blockchain technology could play an important role in ensuring organizations have easily auditable, tamper-resistant, tamper-evident records to meet broader organizational needs and to comply with the GDPR. Because it is information – the data/records layer – that serves as the interface between social systems, such as the law and technical systems such as blockchain, IG and RIM professionals must be at the table in the development and integration of blockchain and GDPR. Ultimately, blockchain and GDPR are both “trust technologies,” although their impacts on IG thus far have been substantially different. GDPR seems to have awakened many organizations to the importance of IG; blockchain discussions typically focus on the technical to such an extent that the technology’s RIM/IG implications are forgotten. IG professionals must bridge the two conversations, helping lead their organizations in using the technical tools – such as blockchain – to achieve their goals, including compliance. In the complex intersection of blockchain, GDPR and information governance, as it turns out, there is little margin between the edge of the world and infinite possibility’ (Naylor, 1993).

Notes

1. A terminology note: the term “privacy” in the USA (where Schoch is based) and Canada aligns more closely with the European concept of “data protection.” When the term “privacy” is used in this paper, it is in the US/Canadian sense of a liberty based right to control information about oneself, as opposed to the dignity-based European sense of “privacy.”

2. The shortcomings of blockchain technology vis-a-vis any archival notions of immutability, or long-term preservation of authentic records are discussed in Lemieux 2016.

3. The archival bond is “the network of relationships that each record has with the records belonging in the same aggregation. The archival bond is originary, because it comes into existence when a record is created […] necessary, because it exists for every record […] and determined, because it is qualified by the function of the record in the documentary aggregation in which it belongs” (Duranti, 1997).

4. Nothing herein is meant as an endorsement of any of these products. We include them simply to illustrate that, despite the frequent cry that blockchain cannot work with GDPR, some in both industry and research are looking at blockchain as a solution to GDPR compliance.

References


Gartner Hype Cycle (2018), *Gartner*.


Rom, G. (2018), “Use the EU general data protection regulation (GDPR) as an opportunity to promote the importance of information governance”, ARMA International Swiss Chapter News, pp. 2-4.


**Corresponding author**
Victoria Louise Lemieux can be contacted at: vlemieux@mail.ubc.ca

For instructions on how to order reprints of this article, please visit our website: www.emeraldgrouppublishing.com/licensing/reprints.htm
Or contact us for further details: permissions@emeraldinsight.com
The monistic diversity of continuum informatics

A method for analysing the relationships between recordkeeping informatics, ethics and information governance

Frank Upward
Centre for Organisational and Social Informatics, Monash University, Melbourne, Australia

Abstract

Purpose – The Information Age during the transition from the paper era to the digital one saw the fracturing and fragmenting of the information-based specialisations. More recently, professional norms for governance have been swept aside within new business models based on information based business applications. This paper aims to support an advance towards networked cohesion based on informatics, regenerating professionalism for the complex networked age.

Design/methodology/approach – New regulatory approaches will have to manage monistic diversity, connecting the deeper logic of continuum thinking in which information governance exists as part of a simple whole (the monistic component) with a recognition that the parts of information governance are much more complex than the whole (the expanding diversity). A continuum approach of this type involves studying things in motion as part of evolutionary processes.

Findings – The production of information is galloping ahead of its authoritative management, and this is at the heart of many of the failings of the post-truth information era. Informatics with its emphasis upon the joint operation of technologies, social processes and knowledge forming and its ability to be an umbrella term for many specialisations can be a cohering force.

Practical implications – The alignment of thought, action and ethical information governance across inter-connected practices for individuals, groups and organisations can be supported by the deeper logic and grounded experience of continuum thinking.

Originality/value – This paper will look to expand the army of sympathisers who wish to get more in touch with studying things in motion, including those trying to cope with the need to develop more adequate ways for managing nanosecond archiving processes.

Keywords Records management, Archiving, Informatics, Continuum thinking

Nanosecond archiving and monistic diversity

A century ago, the spacetime multiverse was a major topic of innovative studies and had its creative disrupter in Einstein’s discovery that $E = MC^2$, a discovery that went out of control and resulted in weapons of mass destruction that have needed regulation. Today, the expanding continuum of recorded information, the archival multiverse, is undergoing creative disruption of the like that has never been seen before in the way societies form knowledge or create, manage and use evidence. Indeed, the expansion in the continuum of recorded information is giving us a new form of mass destruction, cyber-warfare. The critiques of information governance have also been growing exponentially, including within the Internet Plus business environment that is the concern of this article.
Apart from the internet’s powers of creative destruction, criticisms of it have ranged from the way organisations have been held back from that power by dependence on programming within our application platform interfaces, the way the internet has reflected and entrenched inequality and the way it is having a detrimental effect on our cognitive skills. The internet has given us an Information Age beyond imagining, but in relation to governance, it is failing to support difference, creating pockets of one-talking groups, disrupting notions of privacy and identity, generating a post-truth world and because of its technocratic nature, disrupting the development and breadth of professionalism[1].

At the heart of the creative destruction has been disruption to the way archives have been formed. We have moved from the slow-moving archival pace of the paper era, through the clunkiness of leviathan information systems with gnat-like lifecycles, into an archivally ungoverned world of cloud computing that has less to do with computing as we once knew it and a lot to do with smart applications and remote storage of information on servers controlled by someone else. New technologies that are dependent upon the quality of nanosecond archiving processes during communication and action processes have become a mixed blessing as uncertainty spreads across cyber-security issues, artificial intelligence and the control of new business models. More than a century ago, the spacetime continuum drew a prophetic critique from the philosopher William James. Without an ethical perspective, it was plastic and morally indifferent (Upward, 2017). The same goes for the expanding continuum of recorded information and the apparatus that is producing it. The plasticity and moral indifference of social media, hacking, leaking and big data, for example, were all demonstrated very clearly in the US presidential election in 2016. When it comes to continuum thinking, James was right. Ethical conduct should not be an add on; it should be a starting point.

Information has always been manipulated but the difference in this century is the scale and power of such manipulation. The quick-fire nanosecond archiving processes of today and the production of information within an expanding continuum of recorded information is galloping ahead of its authoritative management. Governance processes have not kept pace with the change, and this is at the heart of the failure of internet technologies to deliver maximum benefits. The technologies are magnificent by any historical criteria, but they have not been fulfilling their potential.

Recently, an archives and records management critique has been published in a book on recordkeeping informatics which deals with the relative neglect of basic archives and records management informatics as one cause of failures in governance (Upward et al., 2018):

- information cultures do not adequately support evidence and knowledge;
- business process analysis and business models often lack an understanding of what is involved in authoritatively managing the expanding cascade of inscriptions in today’s smart Internet Plus business environment;
- access to recorded information is in an unqualified mess; and
- ethical recordkeeping functionality sitting underneath business applications is often inadequate.

It is easy to produce such critiques. More importantly, what can be done to mediate the disruption and produce transformations in authoritative information resource management? As a reviewer of the book noted:
Whilst we all know that we need to move away from archaic paper-based thinking and into the world of nanosecond archiving, the way forward is not a well-known path (Davern, 2018).

Fortunately, the reviewer then drew attention to ways of using the book that can enable its reader to explore the new world pragmatically with results in mind. This article, similarly, will try to clarify and condense the way continuum thinking and recordkeeping informatics can be used to begin to address information governance issues. In essence, they can be connected to a program of action providing you work out from the concept of monistic diversity and its relationship with information governance. In the book, monistic diversity is called simplexity, a neologism that combines the singularity of the continuum with the expanding complexity of its parts. The monism is the archival multiverse, a laterally interconnected universe of recorded information that is in a state of exponential expansion. Information governance exists as part of this simple whole but any simple solutions to deal with it are sure to be wrong. They will be confounded by the fact that the diversity of the parts are much more complex than the whole and are in motion, expanding in their complexity.

The continuum of recorded information is becoming more difficult to govern, partly as a consequence of innovations in the nature and use of the different apparatus for producing and communicating information and data. Whilst everything seems to be converging on to a single digital media-based storage format, if you see that as a solution you do not understand monistic diversity. It is precisely the convergence and the new connections that are forming that is the cause of much of the archival disruption. The action and storage points for all of our inscriptions are becoming increasingly chaotic in the face of cloud computing, leaking, hacking, post-truth intrusions on the operation of the apparatus and the growing arsenal of cyber-warfare techniques. If the monism points to the need for lateral integration, the diversity points to how difficult it will be to achieve vertical integration of many different specialised forms of information management and systems development. In short, the monism might give us mental images of what order might be produced, but the diversity induces disorder which for records management includes the sort of creative disruption within many modern business models.

The rest of this article will open up ideas about how to manage monistic diversity by looking at what it can mean to say “all is archive” as a base for developing continuum informatics as an integration tool. It will look at how the connections made by things in motion expand the complexity of information governance before looking at the evolution of un-governance. It will argue that there is a need to develop disciplinary integration that can spread the stress of holding new governance structures together again. The conclusion will briefly point to the significance of project work and agile forms of networking, with the goal of producing renewed forms of information professionalism operating across an expanding web of relationships. This is not an article on networking, professionalism or project methods, but it is an article on an archival philosophy that can underpin them in this century.

**All is archive**

The archival philosophising in this article is based on the deeply logical idea that all is archive, a notion that can be given different forms of expression. In the age of science in which continuum thinking flourished more than a century ago, the notion was relatable to any things we could study. Everything is in motion, moving from many different pasts into many different futures via the present moment. Philosophers such as Gabriel Tarde in France advised us to face up to the complexity of the connections within this simple whole. Alfred North Whitehead in Britain agreed and fought hard but unsuccessfully against the
accelerating trend to split science off from the arts. Both studied the formation of things, and Albert Einstein explored aspects of the complexity of the formation of the universe itself.

Another contemporary, Henri Bergson looked at the formation of things from the viewpoint of creative evolution. His view of monistic diversity created what Gilles Deleuze later described as a flicker, comparing it with the cinematic flicker that at the time was changing the way people viewed the world (Deleuze, 1988). The flicker was that instant when the past reconstituted itself as the future over and over again in place upon place. The flicker of the archive can be mediative, mitigating against or delaying change or transformative. The archive is the instrument of change, or represses it. T.S. Eliot gave poetic expression to the flicker in his poem *Burnt Norton*:

> At the still point of the turning world. Neither flesh nor fleshless;
>
> Neither from nor towards; at the still point, there the dance is,
>
> But neither arrest nor movement. And do not call it fixity,
>
> Where past and future are gathered. Neither movement from nor towards,
>
> Neither ascent nor decline. Except for the point, the still point,
>
> There would be no dance, and there is only the dance.

T.S. Eliot, “Burnt Norton”, II.

For many archivists, as the century progressed the archive became the still point. They ignored Eliot’s injunction and called it fixity. For a continuum archivist, it is the dance and there is only the dance.

For Australians, the expression of the archive as continuum was shaped by the influence of one of Britain’s great continuum philosophers, Samuel Alexander, an expatriate Australian who left his homeland for postgraduate study in England. He never returned, but in the 1920s and 1930s, his patronage-dominated appointments made to chairs of philosophy at Sydney and Melbourne University. If Aristotelian philosophy focuses on things, the study of *being qua being*, Alexander’s philosophy focused on the study of things in motion, the study of *becoming qua becoming* (the formation of things as they are forming). Einstein studied the formation of the universe; Alexander, in much the same philosophical vein, advised his students to study things in motion such as chemicals combining or ants after their nest had been poked with a stick.

In Australia, a consequence of viewing things in motion was communicated in the middle of last century in an introductory text on philosophy by Quentin Gibson, a member of a family of philosophers that had benefited from Alexander’s patronage. Remember that problems are not static. No matter how much you think you have resolved them, they are always likely to break out in new idioms (Gibson, 1961). Today, we call such problems wicked. They are complex, and their complexity is always expanding. The American continuum philosopher, Richard Rorty, points to why this is the case:

> There is nothing to be known about anything except an initially large, and forever expandable, web of relations to other things. Everything that can serve as a term of relation can be dissolved into another set of relations, and so on for ever. There are, so to speak, relations all the way down,
all the way up, and all the way out in every direction: you never reach something which is not just one more nexus of relations (Rorty, 1999).

November, Camacho-Huber and Latour express the concept of the significance of relationships within a continuum as something which provides meaning:

An isolated image has no scientific referent – but it generates, of course, like all images, a virtual image, the “what” that it is said to be the representation “of”. Taken in isolation, an electron microscopic image of a virus, a photograph of a galaxy, and the drawing of a skeleton in a natural history museum, has no specific value (even though they might have powerful aesthetic, pedagogical, or rhetorical strength). If you want to understand what an isolated inscription means in science, you have to reinsert it inside the cascade of other inscriptions out of which it has been extracted (November et al., 2010).

Within this cascading and relational complexity, however, there are patterns. If recordkeeping informatics, for example, is to have a strong future, it is likely to be built on managing business applications as fractals, as recurrent patterns of activity in which nanosecond archiving processes can be internalised and modules can distributed in tailorable form from an application store for use in an organisation's recordkeeping architecture. The module has to be dance-ready, and as the dance changes, it needs to be amendable or replaceable often without losing its capacity to represent a virtual image of those moments “where past and future are gathered” within business transactions or its place in the cascade, a place that gives it meaning.

Logic, experience and things in motion
The archive, as it is discussed in the previous section, can be innovative, making connections within the complexity of its parts that can be different from those parts. Gilles Deleuze called this process machinic connectivity, an expansionary relationship between ideas that produces something new. Unfortunately for information governance, the paper and the digital era are so different that new connections in information governance have proved difficult to make. Alexander's advocacy of the need to study the formation of things as they were forming, for example, influenced archives and records management practices whilst they were dominated by paper because Australians understood the business environments that gave rise to their records continuum practices. In the middle of last century in Australia, the Commonwealth Government’s archival authority and its Public Service Board (PSB) jointly studied the formation of the archive. The PSB wanted to govern recordkeeping processes during transactions to ensure that accurate and reliable records of transactions were formed. Ian Maclean, Australia’s chief archivist, focused his attention on how to produce reliable records by studying their characteristics, by examining the records classification processes that enabled the archive to be built out coherently from transactions in the first place and by designing authoritative recordkeeping systems. He had been taught to know, however, that things would move on. As he noted.

I am well aware that, even if its main principles continue to stand up to professional criticism, it needs much clarification and adjustment, not only in terms of logical argument but also in the light of the practical experience of archivists and records managers (Maclean, 1959).

Unfortunately for the governance of individual public servants and the formation of an archive of their actions, the paper era was coming to a close, and for the next 50 years, much of the change to archival formation processes occurred outside of the ongoing immediate practical experiences of archivists and records managers. A sharp archival turn has been taking the archive away from slow linear formation processes towards dependence upon
nanosecond-based systems and applications. As a student of the turn within feminism, Eichorn (2008):

The archive and desktop are already synonymous. Once denoting a material repository of documents governed by an established institution (e.g., a state archive), definitions of the archive continue to loosen. For a new generation of readers and writers, the archive may be known only as a site of virtual storage (Eichorn, 2008).

Already Eichorn’s statement needs revision in the light of the experience it captures. The site of virtual storage even in 2008 was beginning to be connected to many devices other than the desktop computer. It also needs to be expressed more adequately in terms of deeper archival logic. Only in some times and places has the notion of an archive been so specific. There is a much deeper logic to the idea that all is archive. And, in relation to information governance, is it too optimistic? The new archival sites built out of nanosecond archiving processes are always likely to be a source of fleeting virtual images rather than of meaningfully connected cascades of related inscriptions using, for example, hypertext connections or the new blockchain technological developments.

Maclean’s original approach to the records continuum foundered on the differences in experiences between the paper era and the emerging electronic one in which archives were being formed outside of the conventional location of archival experiences. To address this disjunction and as a way of uncovering logical patterns for archival formation processes across both paper and electronic experiences, a records continuum model emerged from Monash University in 1996 with which some readers might be familiar (Upward, 1960). It attempted to depict a topology [a logical shape] for the archive by which the experiences of archival formation processes in different times and places could be read dimensionally. The first dimension was the creation of an inscription, a term covering any form of document or data which in the original model was called an archival document. The inscription acquires its meaning through its relationships with other inscriptions in the archives. Accordingly, the subsequent dimensions involved its capture as a record, its formation as part of an archive and its pluralisation with other archives. The dimensions as thresholds for the cascade might or might not all be crossed in particular instances, or might get uncrossed at a later date.

The model was not an implementation model nor a guide for how to form archives. It provided a logical shape for readings of the formation of archives in any era. To further guide such readings, four vectors that have a tendency to shape the nature of archives were depicted dimensionally as axes on the model. The vectors were:

1. transactionality (the nature of the business);
2. evidentiality (whether adequate evidence of the transactions was being formed);
3. memory and evidence (the ability of the archive to function as useful and usable memory); and
4. storage (the recordkeeping containers).

These are the major vectors of a professional recordkeeping archivist or records manager, and the model has been used in many teaching and training programmes globally to help explain the evidence base for their professional activity.

The survival or otherwise of any human activity today depends upon how successful we are going to be in bringing ethical governance to nanosecond archiving processes that support the formation and use of evidence. Accordingly, the original model as a way of analysing the formation of evidence has continuing relevance, but it was obvious even in
1996 that the formation of archives was moving beyond the scope of the single recordkeeping mind it depicted. A number of other models were developed covering information management, information systems development, publishing, digital forensics and cultural heritage management, all of which have some bearing on archive formation today. The models were based on the same four dimensions but set out different vectors. In terms of monistic diversity, the dimensions represent the monism, the logic of formation that can be found across all forms of information in any time and place. The vectors represent the forces that can connect machinically, producing different results in particular times and places and expanding the archival multiverse[2].

The goal of the modelling was to carry the emphasis upon deep logic and grounded experience in continuum thinking about things in motion across the paper and digital divide. This was achieved, but as usual, just when you think a problem has been resolved, it breaks out in a new and more wicked idiom. Maclean had worked in an era that placed a lot of value on information governance. We live in one where information governance has been in decay. Will the twenty-first-century re-learn how to form useful and usable archives because that is the way authoritative information resource management can begin to keep pace with the expanding productive power of our technologies?

The evolution of information un-governance
Since 2016 and Brexit and the election of Donald Trump, there has been a torrent of books and articles explaining how we have got to a post-truth stage in which there is widespread distrust of politicians and/or suspicion about the technocratic drive to disrupt existing business models. Widespread awareness that there is a crisis in governance might be recent, but it has been a long time in the making. In Australia, for example, the strengthening of authoritative information resource management in the 1950s began to shrivel up in the 1980s after the PSB had been abolished, and the archival authority focused its greatest efforts on storing permanent records that were at least 30 years old.

The problem for the formation of archives globally and in Australia was that archival formation processes have been progressively disrupted by new management approaches, changing values in information management, large-scale information systems development and data management techniques, all of which were outside of the immediate experiences of archivists from the paper era. The Information Age in the last half of the twentieth century saw the fracturing and fragmenting of the information based specialisations, and most archivists and records managers found themselves relegated to back rooms managing the growing quantity of paper records on shelves. They had to look after the end products of the expanding continuum of recorded information, even if it took them further away from the activity base that was producing inscriptions in an increasingly wide variety of formats and media. Professionals who were close to the centre of the expanding continuum of recorded information were now on its periphery, and those amateurs closest to the expanding technical powers of production were at the centre of the storm. A few noticed the absence of archivists or records managers, but not many. For many technocrats and managers, archival formation processes were increasingly identified with repositories that were cost centres divorced from direct engagement in business processes.

That is an over-simplification of course. The recordkeeping strand of information governance is crucial to regulating and ordering the formation of a reliable archive, and this has always piqued the interest of some technocrats and managers, whilst the importance of recordkeeping is beginning to be noticed by more professionals within the “Internet Plus” business environment. The plus component has been expanding exponentially within the development of new business models all dependent upon nanosecond archiving processes.
combined with innovative smart devices and artificial intelligence. An awareness is growing again that all is archive, but what often can go missing is a practical emphasis upon the relationship between any form of governance, recordkeeping processes and our management of things over spacetime, our mutual associations and the connection between the formation of an archive and our life chances. These relationships do not go away just because too many people who are at the forefront of technical and managerial change ignore them or because no-one is providing reliable and stable advice on how to form an archive as a thing in motion.

In part the problem for information professionals is that, as the twentieth century progressed, there have been splits between archives and records management, information management and information systems development and between all these pursuits and the formation of the archive. Yet, paradoxically, one of the things to carry forward to address regulatory control of the formation of archives is the expansion of the specialisations. Their inability to integrate laterally or carry that integration down vertically into the complexity of archive formation might have been a problem in the past but that was during a period of fragmentation followed by current over-simplified views of convergence. Monistic diversity as a logical concept and driver of new practices can help remedy the blind spots in top-down approaches promoting both lateral and vertical integration. Specialisations can continue to expand within shared understandings of the need to address the galloping expansion in the continuum of recorded information by jointly studying things in motion whilst not neglecting their own skill and knowledge bases.

The popular study of the formation of things is beginning to bounce back from its promising start a century ago when in Britain, many people, influenced by Samuel Alexander, went out and bought microscopes to study things like the cheese they bought as it changed composition over spacetime. As more and more people understand that managing cascading inscriptions in this century creates nanosecond archiving problems that are changing the archival game forever, becoming qua becoming will open up a new front for discovery. Whether you are an auditor, a lawyer, a businessman or a scientist, you need to monitor the formation of information objects within an archive and work collaboratively with others. This forecast of a widespread and deeply logical archival turn might sound too optimistic, but scratch below the surface of the many fractured and fragmented disciplines and there are rich studies of things in motion to be found. If you are an architect, you will have been taught continuum mechanics to counter the effect of movement in your structures; sociologists have their structuration theories in which structure and action are in constant motion producing new idioms; mathematicians have their theories of patterns and expanding relationships; archivists and records managers have their records continuum practices.

In English language literature, continuum thinking of this type tends to be constructivist directed at building a structure including, in records continuum thinking, building an archive. However, we live in an era of deconstruction in which much of the modern energy in technological innovation is openly directed at creative destruction. All is still archive; it is just that, for ideas that have explored the disruptive power of the flicker of spacetime, it has been more useful to trawl over Bergsonism and French literary philosophers. In the 1990s, American academic literature, for example, was rife with studies of Michel Foucault’s theories of recommencement as ideas from the past emerged from defeat in new idioms, with Deleuze’s rhizoid thinking in which blocks of becoming representing tendencies for things to form in particular ways gather force, with Derrida’s deconstruction of ideas as a way of freeing the archive from its own past, with Lacan’s topologies for reshaping the mind and
with Lyotard’s postmodernity in which the future exists as an unknown variation of many small stories from the past.

Lyotard presented what might at first glance seem to be a pessimistic view of those in the vanguard of dealing with things in motion:

The artist and the writer, then, are working without rules in order to formulate the rules of what will have been done. Hence the fact that work and text have the characters of an event; hence also, they always come too late for their author, or, what amounts to the same thing, their being put into work, their realisation (mise en œuvre) always begins too soon (Lyotard, 1984).

Managing things in motion within information governance is, indeed, going to be a hopeless task this century if you focus on end products rather than the cascade of recorded information of which they are part. Managing nanosecond archival formation processes requires monitory responses probing the too soon/too late conundrum by paying attention to the flicker and things in motion. In recordkeeping informatics, for example, it is highly unlikely, if not impossible, that modern problems with leaking, hacking, criminality, corruption, accountability and information transparency will be solved by firewalls, encryption and other techniques for protecting end products. They are too late to protect the formation processes and too soon to counter the next wave of technical sophistication. There is a need to monitor the ongoing cascades, and in the process to monitor, the integrity and ethics of the recordkeeping processes, rules, and resources underpinning the formation of an archive.

Continuum thinking might not be rocket science; it just looks like it. In the 1990s, in Australia, for example, it was argued that archivists, including records managers, should be auditors not undertakers (Acland, 1991), but the problem then was that traditional audits started out from end products. It was an activity based on shutting stable doors after the horse had bolted. It is also true that governors have always had a preference for watching others over watching themselves. That means they can avoid facing up to the complexity of the flicker, but not to monitor the formation of your own archive is to risk placing yourself in a hopeless position when it comes to information governance, minimising criminality or corruption in your own or your outsourced ranks or successfully implementing transparency and accountability programs. When things go wrong in a world of nanosecond archiving, they can involve unprecedented cascades of inscriptions and extremely costly fraudulent acts. If we are to manage the ethical and creative evolution of today’s expanding continuum of recorded information, there is an obvious need to keep archival formation processes under constant scrutiny. It is monitoring the cascade that is feasible these days, not a traditional audit relying on expensive and often futile searches for virtual images of smoking guns within that cascade.

**Continuum informatics and the spreading of the ethical stress of building an archive**

Unless mediative factors are introduced, the transformative impact of the digital technologies and the archival disruption of new business models will continue to extend chaos, accelerating the growth of a lack of confidence in information governance in particular and governance in general. Monitoring on its own, as suggested above, probably means monitoring the archival mess, whereas building a stable archive these days is much more complex than identifying the areas of chaos. Arguably, like more conventional forms of architecture, a form of continuum mechanics will be needed to spread the stress of forming the archive as a thing in motion.
The archival architects of this century will need an ethical compass. The expanding continuum of recorded information is proving itself to be as plastic and morally indifferent as its parent, the spacetime continuum. Anyone can enjoy this period of creative archival buckling and go along for a productive rollercoaster ride to what might prove to be an unsustainable future, or they can strive to be a new archivist, looking to generate mediative forms of authoritative information resource management that are equally innovative. So far, the new archivist has been lagging a long way behind the power of the technology. The aforementioned Jean-François Lyotard predicted this dilemma 40 years ago in a polemic advising that, flicker fashion, we either opened up our information and data banks giving innovative problem-solvers information-based parity or we faced a future of accelerating terror (Lyotard, 1984). His metaprescription for us all was to direct information at justice and the unknown, and that can be part of the new idiom for forming archives in the face of a deconstructive flicker, along with the more traditional constructive emphasis upon evidence and its role in authoritative information resource management.

In some places, the development of innovative approaches to mediative practices for this century has begun under an informatics banner. At Monash University, for example, the Centre for Organisational and Social Informatics (COSI) has been at the leading edge of a worldwide trend to use informatics within research programmes designed to increase societal and organisational trust in technology. Within the Internet Plus environment, technical innovations are regularly running out of control by their creators. The most obvious examples in the post 2016 era of studies of the mess we have been getting into in our governance processes have been Facebook and Twitter. Organisations like COSI and others have a longer history in encouraging research into how to accommodate diversity whilst promoting healthier information cultures, but the front has not been broad enough to spread the stress of forming ethical archives. Informatics is not yet specifically focussed on playing the role it can in promoting the monistic diversity needed to manage the expanding continuum of recorded information. The potential for the growth of continuum informatics is there, however, in a number of existing features that can be used to encourage the necessary lateral and vertical integration of different professional approaches.

For a start, informatics offers a way of approaching the modern need for the convergence of disciplines without interfering with the continued development of specialisations. As mentioned above within the brief reference to the modelling of the continuum of recorded information, the common dimensions of create, capture, organisation and pluralisation can give some coherence to the vectors of specialisations that in the twentieth century broke off from each other and then fractured within the pieces they had formed. A host of blocks of becoming, tendencies to form the archive in different ways, developed. They can, however, be brought together coherently using the creation, capture, organisation and/or pluralisation needs of particular cascades of recorded information as thresholds that might or might not get crossed or uncrossed within particular applications, thereby spreading the stress of archival formation processes across any or all disciplines involved in designing and implementing them.

The single word informatics also offers a form of coherence that does not interfere with expanding diversity. For example, in the recent book on recordkeeping informatics, the many meanings that can be given to the word in particular times and places are over-ridden by the deeper logic of its coverage of technical, social and cognitive issues. The expanding diversity within the word comes from the way it encompasses galloping expansion in the development of information and communication technologies, the social changes being wrought by the technologies and new business models based on them and the fact that both knowledge construction processes and ways of forming and managing evidence are in flux.
To get down into managing the complexity without losing contact with the whole, all you have to do is add another word in front of informatics as a qualifier. Add continuum and you get the monism, continuum informatics, which is the whole thing in motion. Add particular areas for studies of things in motion and it becomes a specialisation whether it is large like medical, health, legal, data or recordkeeping informatics or a more specific area of study such as food informatics.

As part of the development of an archival science of continuum informatics, it might help to think in terms of the internal and external mechanics of archival formation processes. Within a recordkeeping informatics strategy, for example, the internal mechanics can be compared with the ongoing monitoring of the materials used in building a bridge. What recordkeeping functionality supporting nanosecond archiving needs to be included during the design stages and operation of an application that manages cascading inscriptions? Are any of the modular parts in the overall recordkeeping architecture showing signs of fatigue? How will fatigued parts be upgraded and/or replaced without damaging the integrity of the whole or losing valued or required information? How have information governance processes been internalised within an application using multiple input integrated laterally (across the whole) and vertically (within the complexity of the application)? Has this internalised functionality been based on adequate analyses of information cultures, business processes and access requirements?

The external mechanics relate to recordkeeping architectures and their operation in a particular situated context, as well as over time and in other places. Organisations need to gain control over their recordkeeping architectures to make sure they meet their business needs and ensure that they are tailored and modified to meet their access and storage requirements. The technologies provide many options, but many of those marketing them want to keep the options as skinny as possible, putting their own commercial benefits and profits ahead of the interests of their clients. Archival institutions, as an external authority, can play a role in appraising fractals, those applications in stores which when drawn down can be tailored for use within organisational architectures and be modified or replaced when outdated. Such applications should be capable of being monitored for their ethical operation by approved auditing arrangements. Both organisational and external authorities need to develop joint monitoring methods for assessing “becoming as becoming”, i.e. how the applications are performing whilst they are in action. Authorities can also advise on controlled processes for updating and replacing the applications.

There is still a long way to go in terms of the evolution of control mechanisms, but at last, using smart applications innovative forms of authoritative information resource management are emerging or can be envisaged. As an example, blockchain technological developments show that the idea of recordkeeping informatics operating within the simple whole whilst managing the expanding complexity of the parts is not fanciful. Blockchain is the sort of tool for tracking source and transmission information from which innovative forms of governance of cascading and related inscriptions can evolve (e.g. the provenance of food in supermarkets). It can be internalised within business applications and promoted externally across fractals. The external appraisal and monitoring of its use within applications can keep it developing as both a ledger mechanism and as a more general provenance tracking tool, rather than stagnating as an old technology. It might have started out within the dubious parameters of bitcoin as part of an attempt to disrupt the archive that is the modern approach to currencies, but removed from these origins blockchain could be the beginnings of many innovations related to the management and control of the nanosecond archiving of cascading communications. Its future, of course, depends upon what is going to be carried forward in the flicker.
Archival networks, projects and intellectual sympathisers

Cyber-maturity has often been a euphemism for information governance when used by those marketing solutions, a substitute for lifecycle thinking. All will be well because the technology is maturing. In fact, it is not, and there is no good reason to think it ever will. The technological advances over the last 30 years have been remarkable but if modernity is any guide only ever offer a prelude for a new wave of immature but even more remarkable technologies. So much birth and so few clear paths maturing towards a timely death! Maturity, from a governance viewpoint, is not just a technical issue. Indeed using the clunky leviathan style information systems and architectures of the 1990s and the lifecycle concepts of the time upgrading authoritative information resource management could not be done.

The Internet plus business environment, however, is starting to provide an approach to the archival multiverse in which an application jigsaw suit an organisation’s needs can be assembled, updated and replaced in agile fashion within perennial start-up processes. Business and its governance are becoming the embodiment of Henri Bergson’s flicker. Fitting the jigsaw of complex pieces together in timely fashion in our organisations can help them retain contact with things in motion. To remain in contact, the business environment will need to be constantly monitored and innovative responses produced using archival networking and a project focus.

For a continuum thinker, cyber-maturity will only have started to arrive when we can hold easy yet sophisticated informatics-based discussions on the management of what can be carried forward for authoritative information resource management purposes within this flicker of newness. The technology matters, but maturity will come from the social and cognitive capacities we have to study and manage things in motion. We need continuum informaticians who can spread the stress of systematically building and implementing rules and resources for applications that deliver orderly spacetime management, mutual association, life chances, justice and perhaps above all else, help individuals, groups, organisations and societies to cope with the flickering of time and the constant expansion of the web of relationships in which everything exists.

The archival networks that are needed to manage the web of relationships can be modelled on those described in the actor-network theory (ANT), at least as it has been described more recently by Bruno Latour. He helped build the theory, but in French philosophical fashion is quite happy to point out it is not about actors, networks or theory[3]. It will be evolutionary and will take many shapes. For information governance, it can be about actants. An actant can be a relationship, an instrument, a person or a thing involved in an action. As a network, ANT can be more like a rhizome, spreading and making machinic connections. It can be about flexible and agile teams of like-minded but differently skilled people who can be assembled within projects. They are like-minded not as one-talks but as lovers of diversity who enjoy explorations of deep logic across varied experiences and as sharers of the ethical purposes underneath authoritative information resource management. And, they are not theorists preferring to tie together academia and workplaces in ways that creatively connect authoritative information resource management with the powerful evolution of information production.

Ethics must drive any archival form of ANT. The complexity of archival formation processes connected to evidence, authoritative information resource management, justice and the unknown have to be respected if we are to move beyond the continued cascading of sludge and deceit. Monitoring the unknown that is evolving in the flicker is something that individuals, groups and societies do not yet know how to do adequately – but learning to do so quickly using flexible teams brought together within a host of possible projects is not an impossibility. Any application of artificial intelligence, for example, can benefit from
absorbing continuum informatics as can the development of regulatory controls or the direct
monitory auditing of the operation of our business applications, and thus the rhizome can
spread. The development of organisationally exploitable common fractals, projects that
deliver bang for their developmental buck at low cost to our businesses, would also be a
priority within a rhizome-based continuum informatics program.

Team members will need to consist of those who are sympathetic to and understand
the challenges of monistic diversity. They will welcome explorations of ethics and
justice because they like exploring the unknown and finding new idioms for addressing
problems. They cannot afford to ignore the expanding productive power of
technologies, but they should want to find mediative rules and resources for the
ordering of archival formation processes. (There are already enough teams out there
disrupting the archive.)

Cyber-maturity, then, would involve discussions about flickering change and how to
monitor and study things in motion. Modern Silicon Valley forms of innovation focus
on disruption. Continuum informatics will focus on the disruptions and strive to be just
as innovative but with an appreciation of the importance of mutual reciprocity and
association, with an understanding of what things can be disrupted and what we want
to carry forward, and with meaningful assessments of how the changes can improve
individual, group, organisational, and societal life chances. Governance is in trouble
unless those promoting it learn to be as creative and as evolutionary as the forces and
people that are deconstructing it.

Notes
1. Criticisms in the opening paragraph are crudely drawn from the works of Joseph Schumpeter,
   Jaron Lanier, Astra Taylor, Nicholas Carr, Anthony Appiah, Aleks Krotski and Andrew
   Keen.
2. See Chapter 7 of Recordkeeping Informatics for a Networked Age, cited above.
3. Bruno Latour was one of the developers of the ANT which is succinctly described in its
   Wikipedia entry in ways which overlap with many ideas in this article (viewed September 2018).

References
pp. 91-95.
association”, February, 11.
Manchester, p. 81.
Maclean, I. (1959), “Australian experience in records and archives management”, American Archivist,
Vol. 22 No. 4, p. 399.


Upward, F., Reed, B., Oliver, G. and Evans, J. (2018), Recordkeeping Informatics for a Networked Age, Monash University Press, Clayton.

About the author
Dr Frank Upward was a senior lecturer at Monash University before he retired in 2006. He developed the universities first postgraduate archives and records management programs at the end of the 1980s, and subsequently taught in many of the School of Information Management and Systems programs. Before joining Monash University, he had extensive workplace experience in archives and records management, information management and data management. He is currently a principal researcher at Monash’s Center for Social and Organizational Informatics. Frank Upward can be contacted at: frank.upward@bigpond.com

For instructions on how to order reprints of this article, please visit our website:
www.emeraldgrouppublishing.com/licensing/reprints.htm
Or contact us for further details: permissions@emeraldinsight.com
Situating trust challenges of online trade

Tove Engvall
Faculty of Science, Technology and Media, Sundsvall, Sweden

Abstract
Purpose – This paper aims to offer an improved understanding of trust challenges in online trade, providing examples of issues that should be addressed for a trustworthy online environment. It also aims to illustrate how records and recordkeeping can contribute in terms of enabling trust and accountability.

Design/methodology/approach – The paper is based on results from a self-ethnographic study of online trade (Engvall, 2017); the results are analyzed further. Kelton, Fleischmann and Wallace’s (2008) model for trust is used to gain a better understanding of the characteristics of the challenges and where they should be addressed.

Findings – This paper recognizes that there are different types of trust challenges at different levels – individual, between clients and businesses and at a societal level – that should be addressed at these levels in different ways.

Originality/value – This paper provides an understanding of trust challenges in the online environment.

Keywords Sustainability, Trust, Accountability, Online trade

Paper type Conceptual paper

Introduction

Trust is an important part of social structures; it is a requirement for everyday life and activities. People have to trust processes to engage in them (Larsson and Runeson, 2014). Records have a central role in these interactions, which is why it is important to ensure their trustworthiness (Rogers and Tennis, 2013).

This is also related to accountability; records have an important role in serving as evidence of human acts (Duranti, 1989) and social and organizational activities (McKemmish, 2001). With the development of information technology, activities, businesses and processes can take place in a digital context online. Activities which often takes place in an international setting, crossing national jurisdictions, beyond physical places involving different actors with complex relationships. In this evolving landscape, it is important to look at how this infrastructure corresponds to societal concerns and targets. The online environment raises challenges in terms of ownership, liability, jurisdiction and records’ trustworthiness, which is also addressed in the international research project, InterPARES Trust (Duranti and Jansen, 2013). If records processes supporting trust, transparency and accountability have mainly been built on the structures within the frames of nation states, there is a need to consider how to guarantee these mechanisms in a globalized digital environment to promote social and economic fairness. It is necessary to be more aware of how the landscape evolves to develop something that serves its purpose. In a study of online trade in the financial market, severe challenges have been identified. A complex business environment, scam companies, dishonest brokers and firms, manipulation to increase clients’ investments and fear and greed, being factors in the decisions people make, have led to frequent money losses and a lack of trust in brokers and the business domain. The way
technology is used increases the risk of losing large amounts of money fast, as well as
the establishment of unequal power relationships between companies and clients
(Engvall, 2017). This raises the question: who and what information can you trust in the
online environment?

Objectives
In the study on online trade (Engvall, 2017), trust challenges were identified that appeared to
address very different aspects. To bring clarity, the challenges are analyzed further in this
article. The aim is to develop a better understanding of the contextual online environment
and to relate records management objectives to contemporary challenges, primarily
focusing on trust and accountability.

The first part of the article discusses literature on the subject, highlighting the role of
records in relation to trust and accountability. This is followed by a section where the
challenges found in the study are placed into a model for trust (Kelton et al., 2008) and
related to records management objectives expressed in ISO 15489. The article ends with a
discussion of the findings.

Online trade
Online trade means that a client can open an account with a brokerage company at a website
and access an online trading platform where buy and sell positions can be placed (Roca et al.,
2008, p. 97; Investopedia, 2016). It is often possible to trade in forex, shares, indexes and
commodities, and the trade is done on the fluctuations of the market, which is why profit or
loss can be made when the market goes up or down. The client often works together with a
personal broker, whose role is to provide guidance, market analysis and assist the client
(Engvall, 2017).

Methodology
With rapid global economic, social, cultural and technological changes, there is a need to
develop understanding, unravel complexities and uncover social injustices. Interpretive
ethnographic research with “critical reflexivity” can contribute to this (Lincoln and Denzin,
2013). This article is based on a self-ethnographic study and adopts an interpretivist and
constructivist approach, which is based on the idea that reality is interpreted and
constructed by people, on both personal and social levels (Williamson, 2013a).
Interpretivism and ethnography are used in studies aiming to understand, interpret and
describe values, behaviors and relationships, as well as how reality is constructed
(Williamson, 2013b; Pickard, 2013). It includes firsthand experience through participation
and observation and relies on the researcher’s interpretation of meanings of phenomena
(Collins and Gallinat, 2010). The researcher can take different roles, with different degrees of
involvement in the field, as a peripheral member, active participant or complete member
(Brannick and Coghlan, 2007; Adler and Adler, 1987).

The study included one year of fieldwork with observations, interviews and personal
experience. Results from the study have been presented in an article (Engvall, 2017), and this
article uses the results for further analysis. Respondents were primarily brokers in online
trading. Unstructured interviews were undertaken with seven brokers and the owner of an
online trading academy, and 75-100 oral conversations were had with brokers.
Conversations were performed over phone or Skype, with some information shared via
e-mail. The study also included experience from online trade with six different brokerage
companies and an educational course.
Self-ethnography and reflexivity

Self-ethnography can be described as a study where the researcher:

[...] is an active participant, more or less on equal terms with other participants. The researcher (…) works and/or lives in the setting and then uses the experiences, knowledge and access to empirical material for research purposes. This research is, however, not a major preoccupation, apart from at a particular time when the empirical material is targeted for close scrutiny and writing (Alvesson, 2003, p. 174).

According to Adler and Adler (1987), being one among the group makes it easier to understand how people in the field interpret and make their social world meaningful. An important reason for carrying out a self-ethnographic study was that it provided a means of access to the field, and throughout the process, it was a way to get in contact with people, experience the systems, ask more informed questions, understand the field and see how it worked in practice.

A central part of the fieldwork and analysis is reflexivity, which is used to develop insights and understanding. It is applied to the interpretation of empirical material and to reflect on the process and the relation between researcher and what is researched (Finlay and Gough, 2003; Alvesson and Sköldberg, 2009). There is no single definition of “reflexivity,” and it is understood and applied in different ways. Finlay and Gough (2003) has outlined a typology of five different approaches: introspection, intersubjective reflection, mutual collaboration, social critique and ironic deconstruction. In this study, introspection, mutual collaboration and social critique have been applied. Both self-dialog around personal experiences and ongoing collaboration with brokers, including reflexive dialog (Finlay and Gough, 2003), were used to develop understanding, identify questions for further exploration and conversations and analyze the empirical material. Triangulation was supported by personal experiences and reflections, conversations with participants in the field and interviews. A bit into the research process, a critical approach was applied because of the experiences and problems that were raised by participants. Central areas for reflection in this study were about trust, expressed in attitudes, values, behaviors and practices in interactions between actors and were related to the institutional setting. The researcher’s role and perspectives were continuously reviewed, as was how to handle any bias in interpretation and presentation.

The model for trust, developed by Kelton et al. (2008), is used in this article to situate the trust challenges for a better understanding and to find out where they should be addressed. Once determined, this is related to objectives for records management. Records management practice and frameworks were not the focus in the empirical part of the study, but is discussed on an idea level of possible applications.

Records, trust and accountability

For a long time, records have been used as impartial evidence of acts for juridical purposes (Duranti, 1989), evidences of agreements, transactions and events that can be used for purposes of accountability and transparency (Hurley, 2005; Iacovino, 2005; Ketelaar, 2005; McKemmish, 2001), to support or deny actions (Reed, 2005) and to claim rights and responsibilities (Jimerson, 2009). A record can be defined as “information created, received and maintained as evidence and as an asset by an organization or person, in pursuit of legal obligations or in the transaction of business” (International Organisation for Standardization, 2016). They also support social justice and responsibility and can be used as tools for control and power in different processes and relationships (Jimerson, 2009). Records also contribute to trust in different parts of society. “Records are a kind of inanimate
object that we trust” (Yeo, 2013, p. 215). It is a “socially accepted form for ensuring accuracy and resolving disputes” (Jimerson, 2009, p. 28). To function as trustworthy evidence, records’ authenticity, reliability and integrity have to be guaranteed (Rogers and Tennis, 2013).

Accountability and trust
Records and recordkeeping are crucial for good governance by enabling transparency, accountability, efficiency, predictability and protection of human rights (Dikopoulou and Mihiotis, 2012; Cunningham and Philips, 2005; Lemieux, 2001). The purpose of accountability is to ensure “honest, responsible, upright and transparent conduct of human affairs” (Hurley, 2005, p. 226). This means that someone is accountable for something to someone and there are methods for how this is applied. Accountability makes human activities visible and enable evaluation and control, which, for example, can prevent fraud. It is also a way for an organization to become aware of its own processes (Lemieux, 2001). In cases of corruption or failure of accountability, part of the reason is mostly also a failure of recordkeeping practices (Hurley, 2005). Long-term preservation of records enables accountability over both distance and time (Cunningham and Philips, 2005). Keeping records is not enough though; it has to be connected to rules and mandates to carry out accountability processes.

There is a connection and balance between accountability and trust. Accountability is based on the need for control of behaviors. Trust, however, does not require continual proof of legitimate intentions and the behaviors of others (Ammetra et al., 2000). Accountability helps to constrain behaviors, while trust is based on the belief in the motives of others, for example, social norms, common values and a person’s propensity to trust. Predictability, dependability and faith are central indicators of trust. Trust implies both competence and properties related to values, ethics and motives. Many online problems can be explained by the lack of trust and accountability (Bechtold and Perrig, 2014). The internet raises challenges regarding misinformation and manipulation because of “the way in which internet technology allows fraudsters to operate with relative ease and to disseminate their scams widely at minimal cost to themselves” (Yeo, 2013, p. 216). Previous centralized authority structures where trustworthy people were responsible for controlling the trustworthiness of the information are no longer effective (Yeo, 2013). There is a need for a shared regulatory and procedural framework for the management of digital objects in the online environment (Duranti and Jansen, 2013), technical solutions (Larsson and Runeson, 2014) and help for users to assess potential risks and harm to facilitate goodwill within communities and improve communication (Friedman and Thomas, 1999).

Accountability in the financial sector
Good records management promotes good financial governance and financial stability (Lemieux, 2010). It enables transparency, accountability, risk management and response to crises, regulation of the financial system and supervision and asserts legal and financial claims. Accountability in turn supports internal control and effective decision-making, which is also crucial to acquire competitive viability (Lemieux, 2001). Financial crises are not only the result of market events but also the operation of information management and organizational issues (Lemieux, 2011). Research has shown that poor records management is highly connected to instability in the global financial system and is also often a reason why data breaches in financial firms can occur (Lemieux, 2010). Research has shown that deficiencies in records and insufficient records management led to weak internal control and contributed to a build-up risk in the global financial system, which, in turn, led to its collapse in 2008 (Lemieux and Limonad, 2011). An efficient risk management is important to have a
trustworthy management of the financial system, and for this, records management is central (Lemieux, 2010). The emergence of more complex financial instruments makes it more difficult to assess the risks involved, increasing the risks in the financial system further (Lemieux, 2010). There is also an increasing volume of data in the financial system, which makes monitoring complex. It requires more attention to networks and collaborations than is usually applied in accounting or supervisory techniques and specialized techniques for data capture, risk analysis and risk management (Flood et al., 2012).

A model for trust
For an improved understanding of the trust challenges in online trade, the Kelton et al. (2008) model of trust will be used. This model has integrated research on trust from behavioral and social sciences, with research on information quality and human–computer interaction. The authors see trust as both a social and psychological phenomenon, arguing that trust is a key mediating variable between information quality and information usage. They address four socio/psychological levels to conceptualize trust: the individual, interpersonal, relational and societal levels.

Individual trust is seen as a psychological attribute, a person’s expectations of others. It is primarily connected to personality and experiences, but the social context also has an impact. Interpersonal trust is understood as a social tie and an attitude the trustor holds toward the trustee. For this, competence, goodwill, ethical behavior and actions are considered important factors. The relational perspective is a property of a mutual relationship and an attribute in the relationship as a whole. It can be seen as an ongoing practice and emerges over time from the involved actors’ interactions. The societal level deals with how a society functions and its social and functional mechanisms. With many interactions between strangers, there has to be a level of trust that is not dependent on interpersonal relations. Rather, it is a trust in the systems where certain behaviors are expected, which also function as a social order (Kelton et al., 2008, p. 364). Figure 1 shows the model for trust and its various attributes, followed by an explanation of said model and its attributes.

**Figure 1.** An integrated model of trust

*Source: Kelton et al. (2008, p. 366)*
Preconditions for trust
Kelton et al. (2008) argue that trust only arises under conditions of uncertainty and vulnerability; there has to be a risk involved and a dependence between trustor and trustee. One function of trust is to decrease uncertainty. In addition, trust matters only if the actors are willing to put themselves in a vulnerable position. Dependency refers to the trustee possessing the potential to satisfy a trustor’s need (Kelton et al., 2008).

Development processes. Mechanisms for creating trust through different processes are identified as prediction (referring to past behavior and development of predictability), attribution (underlying motivations and intentions based on words, actions or trustworthy information, assessing other’s competence, ethics and intentions), bonding (the development and strengthening of emotional bonds in a relationship), reputation (awarding of trust based on recommendations from others) and identification (including goal congruence, the extent to which both parties share a common identity, goals and values). The outcomes in the process affects the perceived trustworthiness of the trustee and social trust (Kelton et al., 2008).

Trustworthiness. Trustworthiness is described as “the perceived likelihood that a particular trustee will uphold one’s trust” (Kelton et al., 2008, p. 367). It includes attributes such as competence (knowledge, expertise, skills and credibility, as well as whether the information provided can be trusted), ethics (can include moral principles, integrity, honesty, fairness, fiduciary obligation and commitment), predictability (reliability, consistency and behaving as expected, and can be based on experience or expectations of a social role or function) and positive intentions (benevolence, goodwill, loyalty and motivation, which are central to effective dimensions of trust). The effect is an increased confidence in the trustee fulfilling the trust (Kelton et al., 2008, p. 367). It should also be mentioned that the above depend on culture and people’s priorities and values.

Influences on trust. Several factors affect perceived trustworthiness and the development of trust. These are identified in the model as propensity to trust, the context and the level of social trust in the recipient. Propensity to trust is explained as a person’s psychological traits and personality influencing the willingness to trust in a specific situation. Context implies that trust is influenced by the contextual situation and is not generalizable. Social trust refers to whether the trustee is trusted by others, for example, through reputation (Kelton et al., 2008).

Elements of trust. Kelton, Fleischmann and Wallace argue that trust is an attitude composed of two parts: “confidence in positive outcomes, and a willingness to modify one’s behavior in expectation of those outcomes” (Kelton et al., 2008, p. 368). The elements of trust are also related to risk and information behavior, i.e. how people perceive risk and act on information. A person that trusts is confident that the outcome will be positive, and has a willingness to act on that confidence.

Kelton, Fleischmann and Wallace go on to develop the model by connecting the elements of trust in the model to trust in digital information, where it becomes a model for trust in digital information. This article will not expand on this perspective, but rather use the model to situate the challenges that have been identified.

Results
In this section, challenges identified in the study are presented and situated in the model for trust, with comments on how they relate to different aspects of the model. The challenges that are highlighted are: corporate structure, relationships between brokers and clients, risk management, regulatory environment, information management and greed and fear. The model for trust focuses on the interpersonal level of trust, but in this article other levels will
also be addressed. The results are presented for records management professionals to consider how records management can be included as an influence on trust to mitigate the risks associated with these challenges. The benefits of records management that are expressed in ISO 15489-1:2016 are considered to contribute to trust and will be used as a theoretical underpinning of arguments. In the standard, records management is said to enable: “a) improved transparency and accountability; b) effective policy formation; c) informed decision-making; d) management of business risks; e) continuity in the event of disaster; f) the protection of rights and obligations of organizations and individuals; g) protection and support in litigation; h) compliance with legislation and regulations; i) improved ability to demonstrate corporate responsibility, including meeting sustainability goals; j) reduction of costs through greater business efficiency; k) protection of intellectual property; l) evidence-based research and development activities; m) the formation of business, personal and cultural identity; n) the protection of corporate, personal and collective memory” (ISO 15489-1:2016, p. 6).

Challenges analyzed with the model for trust relating to records management objectives
In the following, the challenges are presented one by one, and connected to the model for trust and objectives for records management.

Challenge: Corporate structures and accountability mechanisms
The corporate structures in the online environment can be unclear, difficult to understand and lead to confusion. Several companies can be involved, carrying out different tasks for a client, and functions within a company can be located in different parts of the world. Roles and responsibilities can be unclear and communication can be a challenge. According to one of the respondents, these conditions makes it easy for companies to avoid accountability, as well as the means for accountability are weak. It is also easy for companies to disappear and reappear under a different name in the online environment.

Model for trust:
- Level of trust: This mainly refers to the systemic level, but it also affects interpersonal trust, depending on how the broker manages these issues in relation to the client and how the company acts.
- Preconditions for trust: The complexity creates a high degree of uncertainty, vulnerability and also dependence. A client who has low understanding of how things work, becomes dependent on the broker. The complexities challenge conditions for accountability, creating a high degree of vulnerability for clients.
- Trustworthiness: Company ethics affect trustworthiness, whether it means taking advantage of a situation or not. Competence is also relevant, that the company and broker are able to provide processes that are client oriented.
- Influences on trust: The context and social trust influence the degree of trust, but the propensity to trust in a complex environment is also relevant.
- Comment: Depending on whether a company has regulations, and what these regulations are, processes for accountability could either be in place or missing.
- Recordkeeping aspect: Here, records could have both an informative role to increase transparency, and an accountability role. Records can be used to state the companies’ tasks, collaboration with others, responsible persons and explicitly explain where to address questions regarding rights and obligations. Records of different actors’ activities, and an efficient records management with access for supervising
authorities, are crucial to provide means for accountability processes and to assess compliance with regulations. These aspects could lead to more informed decisions from clients (ISO 15489:1, p. 6, section “Benefits”, points a, c, f, h, i).

**Challenge: The relationship between broker and client**

According to interviewees, there are brokers who work for the clients, and brokers who intentionally make people lose money, as well as scam companies involved in fraud. Some use aggressive marketing strategies, and pressure people into investing large sums of money. Lies and manipulation seem to be frequently used. Misconduct has resulted in a lack of trust in brokers and a bad reputation for the profession. This has complicated the work for serious brokers and companies. Bad experiences are also a source of concern for clients. It is difficult to know who and what to trust.

**Model for trust:**

- **Level of trust:** This applies to the interpersonal level. Trust in a broker is a requirement for a person to make an investment; the relational trust will develop over time. A client’s experience will affect the individual level, while a bad reputation affects the societal level. Challenges in the online context relate to the societal level.
- **Preconditions for trust:** There is a high degree of uncertainty about who can be trusted. Clients are in a vulnerable position in relation to brokers, upon whom they rely and are dependent to a lesser or greater extent.
- **Trustworthiness:** The ethics of the brokers and companies influence their trustworthiness; if they have positive intentions and their clients’ best in mind, as well as the broker’s predictability and reliability, e.g. if s/he keeps promises and delivers according to agreement.
- **Influences on trust:** The contextual environment makes it difficult to know who can be trusted. The broker profession’s bad reputation relates to social trust. A transparent environment, well-functioning mechanisms for accountability and capacity to deal with fraud could decrease the number of scam companies. Bad experience affects clients’ propensity to trust. Broken agreements and lack of action leads to distrust, just like bad ethics, dishonorable intentions, and lack of predictability and competence.
- **Recordkeeping aspect:** Several brokers mentioned that there are stricter processes for recording phone calls between brokers and clients. However, a challenge is to capture all communication between broker and client, as multiple communication channels are used. Brokers are acting in a corporate context, which is why connecting it to a broader recordkeeping framework within the firm is also necessary. It is important for clients to know which companies are regulated and which are not to make informed decisions. Records of agreements and acts by different parties enable accountability and protection of rights and obligations, as well as means for control of compliance with regulations (ISO 15489:1, p. 6, section “Benefits”, points a, f and h).

**Challenge: Clients lack trust in themselves**

Something that was highlighted by respondents was that many people lack trust in themselves, which leads to clients who do whatever the broker tells them, which, in turn, makes them easy prey. In addition, this means that to a greater extent they are driven by fear and greed.
Model for trust:

- **Level of trust**: This refers to the individual level, but a bad experience can also influence personal trust and trust for others, which is why interpersonal and relational trust is also important.

- **Preconditions for trust**: Lack of trust in oneself leads to a high level of dependency and a feeling of uncertainty, and puts the person in a vulnerable position.

- **Trustworthiness**: When clients lack personal trust, a high level of responsibility is placed on the companies and brokers and their behavior. All elements of trustworthiness (competence, positive intentions, ethics and predictability) are relevant. It is important to not take advantage of clients that trust others more than themselves.

- **Influences on trust**: This affects the propensity to trust, as well as willingness, confidence and taking action. Contextually, a trustworthy environment will probably increase a client’s willingness to trust. For a person that lacks personal trust, social trust is important.

- **Recordkeeping aspect**: It is important for clients to have control of their money and to have tools for planning out their investments and risk levels to not overdraw their accounts and get into troublesome situations. Personal records management for clients’ economy and trading are crucial for a person to succeed.

**Challenge: Insufficient risk management**

According to respondents, clients lacking proper risk management take too big risks and lack understanding of risk and risk management and how to calculate it. This leads to uninformed decisions, often a result of fear and greed, and loss of money. Risk management is about managing not only external risks on the market but also personal and psychological risks, as well as managing pressure from brokers, which can lead to rash decisions. Risk can also be seen as an opportunity, but it has to be managed.

Model for trust:

- **Level of trust**: This refers to the individual level, a person’s risk awareness and competence. It deals with the interpersonal and relational level, depending on the risk management approach the broker applies and how it is managed during the trading process. It also addresses the societal level, depending on regulations and situations on the market.

- **Preconditions for trust**: There is a high degree of risk in trading and often a high degree of vulnerability and dependence on those with whom the client works.

- **Trustworthiness**: All four elements are relevant. The broker’s competence, skills, reliability and information, the broker’s intentions and approach to risk, ethical perspectives on how risks are managed and risk management. All of these contribute to predictability.

- **Influences on trust**: Contextually, the technical environment can both increase risks and provide means for risk management. Good tools, strategies and awareness of risk management can increase the propensity to trust, as well as social trust. This could decrease fear, increase confidence and the willingness to act and improve outcomes. A good risk management also contributes to trustworthiness.

- **Recordkeeping aspect**: Records management is an important tool in risk management on systemic, business and personal levels. Control of monetary
operations, informed decisions and the use of records to learn from past activities are some of the aspects that are central (ISO 15489:1, p. 6, section ”Benefits”, points c, d, e, l).

**Challenge: Insufficient regulations**

Highlighted in the interviews are the common occurrences of fraud, brokers who manipulate clients, companies who behave badly and operate without any regulation and insufficient regulations and audit mechanisms. Clients lack awareness of regulations and what to look for. Accountability and transparency mechanisms for actors in the internet environment and protection of citizen and consumer rights seem to be insufficient.

**Model for trust:**

- **Level of trust:** This is primarily connected not only to the societal level but also the individual level because of lack of awareness of the risks and regulations and where to turn when rights are violated. Insufficient regulations and challenges because of scams lead to a bad reputation that affects the field as a whole, which in turn affects the interpersonal level.
- **Preconditions for trust:** There is a high degree of uncertainty and vulnerability, as well as a high dependency on the goodwill of people.
- **Trustworthiness:** Because of insufficient regulations, trustworthiness depends on competence, good intentions, ethical behavior and predictability, in addition to the choices people make.
- **Influences on trust:** Social trust is affected by not only what is regulated and what social institutions take responsibility for in relation to its citizens, but also the context based on the conditions in the online environment.
- **Recordkeeping aspect:** Records can be used as evidence in juridical processes and to support rights in disputes. Considerations of regulatory frameworks for global processes and records requirements related to this are relevant. The new regulations, Markets in Financial Instruments Regulation and Markets in Financial Instruments Directive (ESMA, 2018), include requirements on providing data about market transactions that can be used for accountability purposes. This new legislation will increase the need to address recordkeeping tasks regarding market transactions (ISO 15489:1, p. 6, section ”Benefits”, points a, f, h).

**Challenge: An information-intensive and information-sensitive domain**

In online trade, information is crucial for success. It is important to have authentic and reliable information at the right time. Information with high quality is an expensive asset that can give market advantages. Changes are fast and frequent, and multiple sources provide large amounts of information. How information is managed affects control in business processes and quality of market analysis. Records management and communication affects perceived trust. Personal data are bought and sold, which puts clients in a vulnerable position. Clients do not have control over how their personal data is used on the global market. Control of information processes and monetary transaction processes creates power relationships between clients, brokers and companies.

Money is represented by information therefore it can also be seen as management of records.

**Model for trust:**

- **Level of trust:** All levels are affected – the individual level because the client has access and capacity to manage some information, the interpersonal level because
management of information affects the impression, the relational level because it affects the results and communication with clients, the societal level because the informational landscape is global and the business level because of the value of information.

- **Preconditions for trust:** There is a high degree of dependency on information and money to access high-quality information. But there is also an uncertainty about what information to trust, which also implies vulnerability.

- **Trustworthiness:** Aspects that affect trustworthiness are, for example, the company’s and broker’s abilities to manage and interpret information and how they share and manage the information. Ethical aspects, management of personal data and how power relationships are created between companies, brokers and clients, as a result of how information processes are formed, affect trustworthiness. Access to high-quality, reliable information increases predictability for clients, brokers and companies.

- **Influences on trust:** How a person copes with and manages large amounts of information can affect his/her propensity to trust. Contextually, the informational landscape is crucial for the performance of trading. Social trust is affected by, for example, how information, especially personal data, is managed on societal and business levels. Because it affects the perceived competence of corporate and societal institutions, it also affects trustworthiness. Good information management increases the ability to take action and the probability of good results.

- **Recordkeeping aspect:** The financial domain is dependent on authentic, reliable and accurate records, as well as efficient records management, both within firms as well as between different actors. This makes recordkeeping a core aspect of the business domain, even though many seem to be unaware of this fact. Recordkeeping awareness is therefore a crucial question to address. The new **General Data Protection Legislation**, GDPR (EUR-Lex, 2018) pays attention to management of personal data, which has been identified as a concern in the study. In addition, professional ethics could be improved regarding management of records and data. Records processes are part of shaping relations of power and could be addressed in IT design. From a client perspective, it is important that there are easily accessible, trustworthy records to use for informed decision-making (ISO 15489:1, p. 6, section “Benefits”, points. f, J, k).

**Challenge: People are driven by greed and fear**

One of the main reasons why clients lose money, which was highlighted by respondents, was that people act based on fear or greed. This leads to rash decisions where positions are opened and closed at inopportune times. Too high expectations on making profit creates greed, which frequently results in too great risks and financial losses.

**Model for trust:**

- **Level of trust:** This relates to the individual level, but as it can be the result of a bad experience, it also affects the interpersonal and relational level. At the relational level, it can be challenging for brokers with clients that make rushed decisions and stressful for clients with brokers that fuel fear and greed.

- **Preconditions for trust:** A tendency for fear and greed creates a high level of uncertainty and vulnerability on a personal level. An uncertain environment where the client is vulnerable also affects the level of fear.
Trustworthiness: The ability to control greed and fear and the ability to teach clients the same are important. Risk management is important in meeting the challenge; it increases control and gives some level of predictability. Knowledge, competence and predictability could reduce feelings of fear and greed.

Influences on trust: The propensity to trust, context and social trust all affect an individual's level of fear and greed. It is personal but also affected by the context and social norms, as well as societal mechanisms in place to protect consumer rights, which act on fraud and companies' misconduct. Different actors' tendencies to be controlled by greed and fear also affect the context and social trust.

Recordkeeping aspects: Money transactions and trading operations are controlled by records, and practical tools for risk management can reduce the risk of decisions based on fear and greed. Better risk management, use of strategies and, most importantly, increasing knowledge through education can increase confidence and predictability, and thereby reduce fear. Records of trading transactions provide the means for continuous learning, which requires recordkeeping. Additionally, design of IT systems and tools can be considered from a user perspective. Improved means for accountability and systemic trustworthiness are also important parts (ISO 15489:1, p. 6, section “Benefits”, points c, d, l).

Discussion
The problems mentioned here damage trust. Scams, manipulation and unethical behavior, where people and companies take advantage of others, are not sustainable ways of operation. Clients' unawareness about risks, lack of management of risks and lack of knowledge lead to uninformed decisions and loss of money. This, in addition to a high degree of fear and greed, among both brokers and clients is devastating. It is dependent on, and affects, individual, business and societal levels and damages trust between actors and the domain in general. An improved means for transparency, accountability, informed decision-making, risk management and ability to protect and demonstrate rights and obligations, along with corporate responsibilities and having a continuous evidence-based learning from past experiences, are benefits of records and records management, which are expressed in the ISO 15489-1:2016 standards (ISO 15489-1:2016, p. 6). This has also been emphasized by brokers as relevant measures, it would contribute to a greater trustworthiness.

What the model for trust shows is that trust challenges are different in character, refer to different levels (individual, client–business relations and societal) and interact with each other. Different kinds of problems have to be addressed at different levels with appropriate means, and responsibilities for each kind of actor at different levels have to be clear. This article aimed to clarify where to address different challenges, and also to discuss records roles related to that. At the same time, we have to address the entirety and relations between individuals and their contexts. This can be analyzed from the perspective of where formal accountability, in terms of records requirements, could be appropriate in relation to regulations, policies and active shaping of business processes and values. By creating more awareness of different aspects of problems related to trust, they can be managed and changed for the better. Accountability is a tool that can be used to create predictability and to promote fair and honest behavior, which has been shown to be a major challenge in this case and which is enabled by records.

This article aims to create a better understanding of challenges of trust in the online environment, demonstrated by using one example (online trade) from this area and
connecting it to how records and records management can be applied to mitigate those risks. This is important when considering how infrastructure can be designed to support trust and accountability online and in operations beyond national jurisdictions and established processes. What the study also shows is that recordkeeping has to be adapted to the technological conditions and have a proactive approach. This may include to look at how mechanisms for trust and responsibilities can be embedded in the technology. Records roles as a mechanism to steer agreements, enabling foresight, as well as to manage and set restrictions for risk behaviours at a personal client level, is something that would be relevant to explore further.

References


Further reading


Corresponding author
Tove Engvall can be contacted at: tove.engvall@miun.se

For instructions on how to order reprints of this article, please visit our website: www.emeraldgrouppublishing.com/licensing/reprints.htm
Or contact us for further details: permissions@emeraldinsight.com
Preserving over 100 years of management research online

A lifetime investment for your institution, Emerald Backfiles will significantly enhance your library’s offering by providing access to over 125,000 articles from more than 260 journals dating back to 1898.

Visit emeraldinsight.com

Get Backfiles Collections for your library

Recommend Backfiles to your librarian today.
Find out more: emeraldpublishing.com/backfilescollections
eBook Collections

Research at your fingertips

Bringing together over 1,600 eBooks, the Emerald eBook collections are a cost-effective way of instantly expanding library holdings and increasing usage through an award winning platform alongside journals.

Visit emeraldinsight.com

Get eBook Collections for your library

Recommend eBooks to your librarian today. Find out more: emeraldpublishing.com/ebookcollections
Records Management Journal

Number 1/2
Information governance and ethics: information opportunities and challenges in a shifting world
Guest Editors: Elizabeth Lomás, Basma Makhlouf Shabou and Arina Grazhenskaya

1 Editorial advisory board
2 Guest editorial
5 Perspectives on the relationship between records management and information governance
   Julie Brooks
18 The influence of organizational culture on information governance effectiveness
   Ali Daneshmandnia
42 The defensible deletion of government email
   James Lappin, Tom Jackson, Graham Matthews and Ejovwoke Onojeharho
57 A must for agencies or a candidate for deletion: a grounded theory investigation of the relationships between records management and information security
   Sherry Li Xie
86 Theory, regulation and practice in Swedish digital records appraisal
   Elisabeth Klett
103 An integrated framework to elevate information governance to a national level in South Africa
   Paul Anthony Mullon and Mpho Ngoepe
117 Leadership and political will for implementation of the access to information (ATI) Act (2016) in Kenya
   Victor Kabata and Francis Garaba
134 The impact of new public management through outsourcing on the management of government information: the case of Sweden
   Proscovia Svård
152 Open government data: critical information management perspectives
   Elizabeth Shepherd, Jenny Bunn, Andrew Flinn, Elizabeth Lomas, Anna Sexton, Sara Brimble, Katherine Chorley, Emma Harrison, James Lowry and Jessica Page
168 The role of information governance in e-discovery – the case of China
   Guanyan Fan
178 Participatory information governance: transforming recordkeeping for childhood out-of-home Care
   Joanne Evans, Sue McKemmish and Gregory Rolan
194 Balancing information governance obligations when accessing social care data for collaborative research
   Malkiat Thiarai, Sarunkorn Chotvijit and Stephen Jarvis
210 The role of archives and records management legislation after colonialism in Africa: case of Southern Africa
   Nkholezdeni Sidney Netshakhuma
224 The inevitability of digital transfer: how prepared are UK public bodies for the transfer of born-digital records to the archives?
   Lale Özdemir
240 “The margin between the edge of the world and infinite possibility”: Blockchain, GDPR and information governance
   Darra Hofman, Victoria Louise Lemieux, Alysha Joo and Danielle Alves Batista
258 The monistic diversity of continuum informatics: a method for analysing the relationships between recordkeeping informatics, ethics and information governance
   Frank Upward
272 Situating trust challenges of online trade
   Tove Engvall

ISBN 978-1-78973-925-1

www.emeraldinsight.com/loi/rmj