Online Information Review

Number 6

Data power
Guest Editors: Ysabel Gerrard and Jo Bates

945  Guest editorial

952  Datification, dataveillance, and the social credit system as China’s new normal
   Claire Seungeun Lee

971  What difference do data make? Data management and social change
   Morgan E. Currie, Britt S. Paris and Joan M. Donovan

986  Ownership and control over publicly accessible platform data
   Teresa Scassa

1003 Open government for all? Co-creating digital public services for older adults
     through data walks
     Juliane Jarke

1021 The Tower of Babel problem: making data make sense with Basic Formal Ontology
     Andrew Iliadis

1046 “Warning! You’re entering a sick zone”: the construction of risk and privacy implications
     of disease tracking apps
     Scott S.D. Mitchell

1063 The compliant environment: conformity, data processing and increasing inequality
     in UK higher education
     Penny Andrews

ISBN 978-1-83982-002-1

www.emeraldinsight.com/loi/oir
Guest editorial

Introduction to the Data Power Special Issue: tactics, access and shaping

The articles in this *Online Information Review (OIR)* Special Issue were presented at the Data Power Conference 2017[1] (Carleton University, Canada, 22-23 June), organised by local hosts Dr Tracey Lauriault and Dr Merlyna Lim, with support from the wider Data Power Steering Committee comprising Professor Helen Kennedy, Dr Jo Bates and Dr Ysabel Gerrard (Sheffield, UK).

Now approaching its third iteration[2], the Data Power Conference focuses on critical questions about the relationship between data and society, with conference speakers invited to address the social and cultural consequences of data’s pervasiveness in our everyday lives. With this focus on emergent “data relations” (Kennedy, 2016), the Data Power Special Issue brings a different slant to the advance of datafication and algorithmic processing than is commonly seen in regular issues of OIR. Papers were selected by the full conference team for their quality, as well as their relevance to the Information Science Research Community who make up the majority of the OIR readership.

The Data Power Conference 2017, and by extension the seven papers in this Special Issue, addressed three questions:

1. How can we reclaim some form of data-based power and autonomy, and advance data-based technological citizenship, while living in regimes of data power?
2. Is it possible to regain agency and mobilise data for the common good? To do so, which theories help to interrogate and make sense of the operations of data power?
3. What kind of design frameworks are needed to build and deploy data-based technologies with values and ethics that are equitable and fair? How can big data be mobilised to improve how we live, beyond notions of efficiency and innovation?

These questions broadly emphasise the reclamation of power, retention of agency and ethics of data-based technologies, and they reflect a broader moment in recent data studies scholarship. While early critical research on “big data” – a term that captures the technologies, analytics and mythologies of increasingly large data sets (Boyd and Crawford, 2012) – could only hypothesise the inequalities and deepened forms discrimination that might emerge as data sets grew in volume, many of those predictions have now become real. The articles in this Special Issue ask pressing questions about data power at a time when we have learned that data are too frequently handled in a way that deepens social inequalities and injustices (amongst others, Eubanks, 2018; Noble, 2018).

The papers in this Special Issue approach discussions of inequality and injustice through three broad lenses: the tactics people use to confront unequal distributions of (data) power; the access to data that are most relevant and essential for particular social groups, coupled with the changing and uncertain legalities of data access; and the shaping of social relations by and through data, whether through the demands placed on app users to disclose more personal information, the use of data to construct cultures of compliance or through the very methodologies commonly used to organise and label information. While these three themes do not exhaustively capture the range of topics addressed in this Special Issue, at the Data Power Conferences, or within the field at large, they represent an emphasis within data studies scholarship on shedding light on the most pressing issues confronting our increasingly datafied world.
Part 1: tactics

Two of the papers in this Special Issue – “Datafication, dataveillance, and the social credit system as China’s new normal” (Lee, 2019) and “What difference does data make? Data management and social change (Currie et al., 2019) – offer unique critiques of power relations through the framework of ‘tactics’”. It is worth engaging in a brief discussion of Michel de Certeau’s (1988) The Practice of Everyday Life here to frame these contributions. This book explores what de Certeau calls “making do”: the tactics people use to navigate power structures in their everyday lives. de Certeau (1988) talks about the everyday, commonplace power struggles between two social groups: the producers of culture and their users (ordinary people), and argues that people “conform” to mechanisms of discipline and power “only in order to evade them” (de Certeau, 1988, p. xiv). In other words, it is possible for people to evade/subvert the ruling order by using a set of tactics. But as de Certeau (1988) notes, “Whatever it wins, it does not keep. It must constantly manipulate events in order to turn them into ‘opportunities’” (p. xix). The necessity to constantly evolve one’s tactics is a particularly important consideration for Lee (2019) and Currie et al. (2019), who write about the tactics people are adapting during the current climate of fast-paced data-based changes (indeed, at a pace that de Certeau probably did not foresee).

Opening this Special Issue, Claire Lee’s paper shares novel early insights into how Chinese citizens adopt tactics in the face of the social credit system: a form of societal governance that intends to standardise Chinese citizens’ behaviour and reputation by collecting personal information to evaluate citizens and give them a “social credit score”. As Lee (2019) explains:

With a high score, one can easily acquire a cash advance, obtain expedited access to vital services including medical insurance and education, as well as enjoy faster processing at customs, in applying for visas and securing animal adoptions. On the other hand, individuals who have lower scores will be restricted from services (pp. 952-970).

The social credit system is still in the early phases of its development, but the plan has been a long-term goal for the Chinese government and citizens are becoming more aware of its steady implementation. Lee collected personal narratives from Chinese citizens to learn their views on what some refer to as “the new normal” in Chinese society. Lee’s main research finding is that the social credit system has heightened citizens’ practices of self-surveillance (see also Lupton and Williamson, 2017): Lee’s (2019) participants feel as though they have begun to monitor themselves more closely since they learned about the social credit system and its consequences. Lee concludes the paper by raising a point of discussion, asking how Chinese citizens might “disrupt the system from the inside” (pp. 952-970), and wondering which citizens will be disproportionately affected by the social credit system. Lee puts herself in conversation with authors whose work has recurred across this Special Issue and who focus primarily on the consequences of data power, such as Boyd and Crawford (2012), Lyon (2014) and O’Neil (2016), amongst many others.

Morgan Currie, Britt Paris and and Joan Donovan then turn to a discussion of the data management practices undertaken by activist groups and grassroots organisations. The authors expand on emerging data activism literature to draw distinctions between the data infrastructures used by groups that organise in response to data collection by corporations and the state. For example, they explore how Fatal Encounters used a collective database to produce missing data about police homicides in the USA, offering a critique of the transparency of publicly available data sets. They examine how Making Sense created a new data set to disclose information about the air quality around Kosovo, an issue that had been concealed by their government; and, how DataRescue – led by the Environmental Data Governance Initiative – archived data created by US federal scientists that documented evidence of climate change and human-induced ecological violence. Literature on data
activism typically focuses on generating new data, but the case studies shared by Currie et al. (2019) demonstrate how activist groups use missing or already-existing data to highlight contentious political issues. Data management systems are thus a crucial part of political mobilisation for these organisations: without proper management, activist groups would simply be unable to do this work. The authors argue that the results activists produce are only a small part of the work they do: “Behind the visualisations or public-facing databases are a suite of data management infrastructures and organisational norms that form a considerable part of activists’ mundane practice” (Currie et al., 2019, pp. 971-985). As Currie et al. (2019) note, data infrastructures are academically under-addressed and yet are integral to “shaping the tactics and political formation of data activists” pp. 971-985). While Lee (2019) and Currie et al.’s (2019) focus is on the tactics citizens use to respond to different contexts of datafication, our next two papers draw attention to issues around citizens’ access to data relevant to their needs.

**Part 2: access**

Two of the papers in this Special Issue – “Ownership and control over publicly accessible platform data” (Scassa, 2019) and “Open government for all? Co-creating digital public services for older adults through data walks” (Jarke, 2019) – offer critiques on the availability and scope of online data sets. Although all of the papers in this Special Issue deal in some way with data and inequality, the papers in this section address issues of data access for social groups and actors whose data needs are often marginalised within discourses and practices dominated by powerful institutions. Readers are likely familiar with such struggles in the context of the increasingly restricted access to social media platforms’ Application Programming Interfaces used by researchers to collect data and produce knowledge about the social world. Our authors examine similar issues in the context of the legalities of access to Airbnb data, and in the development of methodological approaches to make open government data-driven services more relevant to the needs and experiences of older citizens.

Using Airbnb as a case study, Teresa Scassa explores the legalities of access to publicly available data in what Van Dijck et al. (2018) and others have called the “platform society”. In the paper, Scassa (2019) explains that a diverse range of parties make use of publicly available Airbnb data for reasons which often serve the public interest, but existing legal frameworks are not particularly well suited to “our evolving data society generally or to platform data ecosystems in particular” (pp. 986-1002). This creates a risk that users’ perspectives and the public interest will not be well-represented in evolving litigation, if indeed “they are represented at all” (Scassa, 2019, pp. 986-1002). Scassa (2019) argues that Airbnb’s data has significance beyond its immediate user base because we can learn about, for example, “the platform’s effects on the cost and availability of long term accommodation, its impact on incumbent short-term accommodation providers, the incidence of discrimination in Airbnb rentals and pricing” (pp. 986-1002). Although there is a strong public need for access to data by companies like Airbnb, there remain legal uncertainties in relation to the ownership and rights of access to publicly accessible data. Scassa reminds readers that the legitimacy of data scraping activities are likely to be decided by litigation between large, wealthy commercial competitors because, simply put, litigation is expensive. Perhaps the biggest risk is that access to data will be resolved by litigation between business competitors, and will therefore not bear wider interests in mind. This risks squeezing out the voices and interests of non-commercial users, along with non-profit organisations and smaller companies. While we might not all agree on which kinds of data serve the public interest, Scassa reminds us that stark inequalities will emerge if data’s accessibility is determined only by private interests.

Juliane Jarke’s article offers an example of data-related discrimination through the lens of Open Government Data initiatives. As Jarke (2019) explains, Open Government
Data initiatives promote the ideals of “citizen collaboration and participation in the planning, design and delivery of public services” (pp. 1003-1020):

The idea of using open government data for new public services is simple: Governments provide their data for free, online and under open licences; civil society actors or private companies may re-use the data and develop services according to their needs or expected demand.

One of the main espoused benefits of Open Government Data is that it can foster the development of user-centred services by third parties without incurring additional costs on the state. Ideally, this means citizens should receive better services; however, Jarke observes that the needs of older citizens are often marginalised. They are not usually the target user group of services based on use of Open Government Data, and even if they are, the type of data opened by public bodies may not be relevant to their needs. Jarke (2019) argues that there is a real need to “bring together city administrations as data owners, technology developers and older citizens as knowledgeable individuals and prospective users in order to co-create relevant and meaningful public services based on open data” (pp. 1003-1020). In the paper, Jarke presents an evaluation of the innovative “data walks” methodology that she used as a way to engage older citizens in the co-creation of open-data-based digital services. With particular attention paid to the issues of inclusion and efficacy in engaging with the needs and interest of participants, Jarke (2019) argues that data walk workshops are one way in which “older adults cease to be subjects of digital innovation and become co-designers” (pp. 1003-1020). They are a step towards the development of “effective and relevant services for older adults […] based on the needs and requirements of the target audience” (pp. 1003-1020), rather than being driven by the data that is made available under Open Government Data initiatives.

Part 3: shaping

The third and final theme to emerge through this special issue is “shaping”. Three papers in this Special Issue – “The tower of Babel problem: making data make sense with Basic Formal Ontology” (Iliadis, 2019), “Warning! You’re entering a sick zone: the construction of risk and privacy implications of disease tracking apps” (Mitchell, 2019) and “The compliant environment: Conformity, data processing and increasing inequality in UK Higher Education” (Andrews, 2019) – approach their contributions by accounting for the relationship between data power and the social. As Baym (2010) reminds us, “accounts like these locate causality not with technologies themselves or with the people who use them but in the “middle ground” (p. 44): an approach called the “social shaping of technology”. The final three contributions to our Special Issue emphasise the intricate interplay between new forms of data (and their systems, management and so on) and the social world. As Baym (2010) notes, perspectives like these tell us that: “the consequences of technologies arise from a mix of “affordances” – the social capabilities technological qualities enable – and the unexpected and emergent ways that people make use of those affordances” (p. 44).

Andrew Iliadis’ (2019) research engages with the social shaping and implications of what he calls “Applied Computational Ontologies” – the “largely invisible” (pp. 1021-1045) standardised metadata vocabularies increasingly used to structure data through organising and labelling, often in an effort to facilitate data integration and interoperability. With a focus on Basic Formal Ontology (BFO) and its various applications, Iliadis adopts a data assemblage approach to illuminate ACOs as “products of human-centred communication” (p. 6). Iliadis’ research proposes and puts into practice a methodological approach that combines digital ethnography and digital methods to interrogate critically processes of data labelling and organisation that are underexplored across many contexts of application. Examining the ontological realism of such vocabularies, Iliadis (2019) argues:

If the ontological realism endorsed by BFO is dependent on the universal laws and structures of science, social ontology is dependent on the invisible rules and laws that society follows [...] BFO
follows social ontology and has continued the practice by describing institutional systems to which documents belong, positional roles within such systems, and the production of documents [...] Yet, social kinds are said to be [...] subjective and dependent on mental attitudes [...] interactive and malleable. It is here where social ontology gets tricky (pp. 1021-1045).

Through consideration of applications such as the BFO-powered Military Ontology, Iliadis argues that this raises significant concerns about the material impacts of ACOs, concluding with a call for ethical analysis of the BFO methodology when applied in social contexts, and for more research about the interactions between data scientists and ontologists.

Scott Mitchell’s (2019) article examines the privacy and surveillance implications of digital disease tracking apps, like SickWeather and HealthMap. These apps use data mining, analytics and crowd-sourced data to predict disease outbreaks, and have been called the “Facebook for hypochondriacs” (pp. 1046-1062). The apps work by collecting information from social media and across the wider Web, paired with self-reports from those who use the app to allow users to see who is sick in their neighbourhood. HealthMap, for example, was hailed as a “big data success story” for picking up references to the 2014 Ebola outbreak in Guinea a week before its government notified the World Health Organization (Mitchell, 2019). Mitchell (2019) explores the discursive dimensions of the apps, noting that disease tracking apps like the above “construct disease threat as omnipresent and urgent, compelling users to submit personal information – including sensitive health data – with little oversight or regulation” (pp. 1046-1063). SickWeather, for example, urges its users to help the app to work better – and therefore to raise broader awareness of sickness – by reporting illnesses, which in turn generates data and, eventually, profit for the platform. Influenced by the app walkthrough method (Light et al., 2016), Mitchell found that SickWeather uses smartphone notifications and alerts to create a sense of urgency, discursively compelling users to check the app and add personal information. As Mitchell (2019) explains:

SickWeather works to discursively construct disease threat as an omnipresent, inescapable reality, placing contagion fear in users’ pocket or the palm of their hand; alerted by a sound from their phone, at any moment their supposed disease risk can change and instantly make itself known (pp. 1046-1063).

Mitchell hypothesises that the apps’ dominant discourses might shape data disclosure. This paper presents important findings about the implications of a set of under-explored apps (disease trackers) to contribute to broader discussions about social and technical relations.

Penny Andrews’ article on the role of data processing in the enforcing of the “Compliant Environment” in UK Higher Education (HE) concludes this Special Issue. The “Compliant Environment” is a UK Home Office approach to managing immigration, which in part depends upon the reuse and processing of data from a variety of sources. Andrews argues that such a form of “Compliant environment” is also shaping data practices within the UK’s HE system, which is heavily dependent upon data processing for the production of compliance and conformity amongst staff and students. Taking aim at data-driven research metrics, university rankings, student monitoring and evaluation processes, Andrews (2019) critically examines the political economy of the data systems that have become commonplace in HE settings, observing it is no longer the case that “if you are not paying, you are the product”; rather what we are seeing is “part-payment via data” (pp. 1063-1079) as the business model for many of the data-driven HE systems. Andrews goes on to illuminate the disproportionate impacts of data-driven compliance within HE for marginalised students and staff, including those impacts that result from what can become normalised as a result of HE institutions obligation to monitor students and staff to ensure compliance with immigration authorities. Andrews concludes by calling for resistance to damaging uses of data that serve other agendas, advocating a “civic hygiene” (Schneier, 2007) approach to data management within the HE sector, bringing us back to the question of “tactics” discussed in earlier papers (Lee, 2019 and Currie et al., 2019).
Data Power: diversifying the field

The papers in this Special Issue address how different forms of online information systems that enable data collection, processing, sharing and use are embedded within, and have implications for, the future development of organisations, cultures and societies. The authors in this special issue approach the topic from a variety of theoretical and methodological angles — some that will be more, and some less, familiar to readers of OIR. Our efforts to bring together these papers in a single issue are not only aimed at emphasising a shared focus within the emergent multi-disciplinary critical data studies literature on understanding and resisting data-related injustices, but also to reflect the growing diversity within the field. Among the papers in this issue, readers will find variety in terms of research methods (action research, story completion methods, digital methods, data visualisation, interviews and document analysis), geographical reach (Canada, China, Germany, Kosovo, UK and USA) and cases (China’s social credit system, activists’ data management systems, disease tracking apps, publicly available Airbnb data, Open Government Data), a diversity that suggests a field that is broadening in scope and depth in an effort to address the pressing societal challenge of widespread datafication.

Ysabel Gerrard
Department of Sociological Studies, University of Sheffield, Sheffield, UK, and
Jo Bates
Information School, University of Sheffield, Sheffield, UK

Notes
1. The conference was supported by the following funders: The Social Sciences and Humanities Research Council of Canada Connection Programme (2017); Faculty of Public Affairs, Carleton University; School of Journalism and Communication Carleton University; MacOdrum Library, Carleton University; Carleton Institute for Data Science (CUIDS); Carleton Institute of Criminology and Criminal Justice; Individual Research Grant contributions from Tracey P. Lauriault and Jeffrey Monahan, Carleton University; and Merlyna Lim’s Canada Research Chair Grant.
2. The next Data Power Conference will be held at the University of Bremen, 12-13 September 2019.

References


Datafication, dataveillance, and the social credit system as China’s new normal

Claire Seungeun Lee
Inha University, Incheon, South Korea

Abstract

Purpose – The purpose of this paper is twofold: first, to explore how China uses a social credit system as part of its “data-driven authoritarianism” policy; and second, to investigate how datafication, which is a method to legitimize data collection, and dataveillance, which is continuous surveillance through the use of data, offer the Chinese state a legitimate method of monitoring, surveilling and controlling citizens, businesses and society. Taken together, China’s social credit system is analyzed as an integrated tool for datafication, dataveillance and data-driven authoritarianism.

Design/methodology/approach – This study combines the personal narratives of 22 Chinese citizens with policy analyses, online discussions and media reports. The stories were collected using a scenario-based story completion method to understand the participants’ perceptions of the recently introduced social credit system in China.

Findings – China’s new social credit system, which turns both online and offline behaviors into a credit score through smartphone apps, creates a “new normal” way of life for Chinese citizens. This data-driven authoritarianism uses data and technology to enhance citizen surveillance. Interactions between individuals, technologies and information emerge from understanding the system as one that provides social goods, using technologies, and raising concerns of privacy, security and collectivity. An integrated critical perspective that incorporates the concepts of datafication and dataveillance enhances a general understanding of how data-driven authoritarianism develops through the social credit system.

Originality/value – This study builds upon an ongoing debate and an emerging body of literature on datafication, dataveillance and digital sociology while filling empirical gaps in the study of the global South. The Chinese social credit system has growing recognition and importance as both a governing tool and a part of everyday datafication and dataveillance processes. Thus, these phenomena necessitate discussion of its consequences for, and applications by, the Chinese state and businesses, as well as affected individuals’ efforts to adapt to the system.

Keywords China, Deviance, Dataveillance, Data-driven authoritarianism, Datafication, Social credit score system, Digital sociology, Critical data studies, Digital space

Paper type Research paper

1. Introduction

We live in an age where data are both abundant and powerful. In this data-driven society, every online interaction or post can be stored and retrieved elsewhere. The process of securing citizens’ information and storing it in computerized databases already has a long history; however, what is unique to China’s context is its publicly known long-term plan. Governments are taking advantage of stored data in a more sophisticated way than before, and China is no exception. In fact, China’s Government is a new pioneer in utilizing data and technology as tools for governing society. It has invested capital and resources into a new IT-backed authoritarianism, turning technology into the tool for power (Browne, 2017). The country’s government has realized that technology is an important tool for maintaining its desired status-quo via the surveillance of its population and cyberspace.

On the other side of this relationship, China’s population has strived to adapt the introduction of public and private surveillance tools to their existing code of social etiquette. “Lacie wears contact lenses, which are full of information. Her behaviors are captured and...
monitored by apps. Lacie’s rating was affected by how others rate her and her behaviors ruined her life and relationship with her best friend.” When one’s social rating with others greatly influences one’s life, a woman tries to improve her own rating to balance the scores of her colleagues, drivers, (and) friends. Although this quote is derived from an episode of the television series *Black Mirror* that aired in 2016[1], such sentiments and social controlling are increasingly echoed by Chinese people when speaking about their everyday lives. In 2014, a new system called the social credit system (*shehui xinyong tixi*), similarly portrayed in the *Black Mirror*, was introduced. The system links personal financial data to every part of an individual’s social life for the ostensible purpose of supporting economic development, social management and problem solving (Hoffman, 2018).

Using a unique case study of the social credit system introduced in 2014[2], this research examines how datafication and dataveillance provide the Chinese state with a legitimate way of monitoring, surveilling and controlling citizens. Utilizing van Dijck’s (2014, p. 198) definition, this paper defines datafication as “a legitimate means to access, understand and monitor people’s behavior with data.” Dataveillance is defined continuous surveillance through the use of data (Raley, 2013; van Dijck, 2014). “Data-driven authoritarianism,” or the collection of personal data by the state apparatus as part of a social credit system, is processed by means of datafication, and as a part of a dataveillance program. This signifies how state-initiated datafication becomes a powerful tool for conducting dataveillance in effort to monitor individual people, social networks, finances, work productivity and social security. The social credit system in China is a unique case study for understanding how datafication shapes dataveillance, and vice versa, in an age of data-driven authoritarianism.

This study uses an innovative approach to connect the personal narratives of research participants with two complementary primary sources: policy documents from central and local governments, and relevant media reports. As the social credit system’s development is still in the early stages, this paper also draws on empirical research in order to examine how people respond to this system’s integration. Specifically, a story completion method, or a scenario-based method, was used. This method, in which participants were invited to complete a story using their own words within 10 min, is popularly used in psychology to elicit candid participant reactions to sensitive topics and to tap into participants’ imaginations or perceptions (Amundson, 1985; Clarke *et al.*, 2017; Gray *et al.*, 2017; Kitzinger, 1995; Lansky, 1968). Specifically, 22 Chinese participants were invited to create a story based on a possible future scenario of the social credit system, to explore how people perceive the social credit system. There are multiple reasons for using this method: first, the nascent stage of the social credit system at the time of this study limits the pool of potential subjects who have experienced living under such a system. Furthermore, revealing a great number of details about the system to participants could lead to the development of subjective prejudices about the system, which could then skew the study’s results. Finally, due to the political nature of this issue in China, it is a difficult prospect not only for participants but also the researcher to openly discuss it. The story completion method is, therefore, a viable method to address the issues relevant to the study.

This paper first contextualizes this study, introducing the debate around datafication and dataveillance through scholarship, policy and media sources, while simultaneously illuminating the limited presence of these sources in the non-western world. This paper then provides a detailed overview of existing policies for examining the emergence and development of the social credit system in China. The next section introduces the research methods used in the study, and the following section analyzes and discusses participants’ firsthand interaction with the social credit system. By utilizing the ideas of datafication, dataveillance and data-driven authoritarianism as analytical lenses, this paper argues that the social credit system leverages datafication in tandem with dataveillance, and by using it the Chinese state legitimizes the monitoring, surveilling, and enacting of
social control upon people, business and societies. In other words, China’s social credit system is analyzed as an integrated tool of datafication, dataveillance and data-driven authoritarianism. In closing, this paper offers implications and reflections on various dimensions of data-driven authoritarianism.

2. Data, datafication, dataveillance

2.1 Datafication and dataveillance
Over the past decade, with the advancement of technology and big data, researchers in the fields of sociology, media and communication studies, science and technological studies, and criminology, among others, have examined the intensified interplay between new technologies, (big) data, and social control (e.g. Boyd and Crawford, 2012; Cukier and Mayer-Schoenberger, 2013; Qiu, 2015; Yeo, 2016). Some of these works focus on technology, cyberspace and digital media. Yet, another strand of research has taken a critical approach to these recent developments – namely, what datafication does to our society (Birchall, 2016; Flyverbom, 2017; Hintz et al., 2017; Lupton, 2015; Lupton and Williamson, 2017; van Dijck, 2014) and ethical dimensions and data justice (Dencik et al., 2016; Friedewald et al., 2017; Taylor, 2017). Past studies have examined how different stakeholders, such as the state, companies and individuals, use data. Others analyze how and what (big) datafication does to different modes of surveillance, and what its explicit and implicit consequences are (Andrejevic and Gates, 2014; Boyd and Crawford, 2012; Kitchin, 2014; Lyon, 2001, 2004, 2010, 2014; Mann et al., 2003; O’Neil, 2016; Qiu, 2015).

Diverse modes of surveillance have emerged, including a new form of surveillance called dataveillance. Dataveillance, a type of surveillance due to the existence and emergence of data, is defined as the ways in which information is collected as different forms of data, and the consequences of such programs (Lupton and Williamson, 2017; Raley, 2013, p. 15; van Dijck, 2014). Dataveillance is augmented by the development and utilization of digital technologies. People may voluntarily participate in self-surveillance by utilizing self-tracking gadgets and software (Albrechtslund and Lauritsen, 2013; Lupton and Williamson, 2017, p. 782).

Depending on the agency and how they exercise power, there are different modes and practices of datafication and dataveillance. Both state and private sectors can be agents of datafication and dataveillance. The recent cases of Edward Snowden’s dismissal from the National Security Agency (Fidler, 2015; Hintz and Brown, 2017; Lyon, 2014) and the Cambridge Analytica/Facebook scandal reveal how and to what extent the government and private companies store, use and abuse individuals’ personal data (Laterza, 2018; Manokha, 2018). Technologies play an important role for these agencies in the process of datafication and dataveillance. Currently, these new methods of dataveillance, aided by technological development, are intertwined with computational propaganda algorithms. Regardless of who the actors are and what techniques they use, critical issues such as privacy need to be taken into account.

2.2 Cyberspace, datafication and dataveillance in China: from IT-backed authoritarianism to data-driven authoritarianism
This section illustrates the aforementioned literature in the Chinese context through a critical examination of contemporary Chinese society. The internet and cyberspace in China are emerging research topics; in particular, discussion around how to govern the internet, its platforms and its virtual space have gained traction. Studies of authoritarian deliberation (He, 2006; Jiang, 2010), internet sovereignty (Jiang, 2014), internet governance and cybergovernance (Creemers, 2017), control and regulation on the internet (Pan, 2010; Tsui, 2003), and activism (Yang, 2009; Qiu, 2016) have been conducted among many others. With the explosive growth of the internet and social media in China, the government
has successfully managed to control information, disinformation, and misinformation (Huang, 2017; Lee, 2018) and establish censorship using algorithms and mechanisms (Creemers, 2017; King et al., 2013, 2014). China has effectively turned the potentially precarious situation that technology and open internet might have brought to the society into a more manageable situation. Likewise, much of the earlier discussion around the Chinese internet focuses on how the state and the people utilize technology for political or cultural surveillance, and to control social dissidents and counterculture movements. How these spaces and technologies become embedded in and store data do not appear in existing debates. By putting data-driven literature in conversation with the internet and cyberspace, I show how the social credit system in China, as well as how the concepts and processes of datafication and dataveillance, are more complex.

In the Xi Jinping era, strategies for managing and policing society became integral to Chinese governmental policy and gained much scholarly attention (Lee, 2017a). In this light, the government’s use of technology in enhancing its governance and social management work, as well as surveillance capacities in both online and offline spaces, are increasingly prevalent. This demonstrates how China’s authoritarian style has strengthened in the age of the internet and technology. This unique governmental model is often called “IT-backed authoritarianism” (Browne, 2017; Meissner, 2017), and refers to “the Chinese government’s capacity to enforce and fine-tune its market regulations and industrial policies [...] through new incentive mechanisms” (Meissner, 2017, p. 9). “Digital Leninism,” or “networked authoritarianism” (McKinnon, 2011), refers to an authoritarian regime that embraces and adjusts to the inevitable changes brought by digital communications. These frameworks highlight how information technology and networked features play an important role in managing society. However, it is not enough to simply depict the situation without capturing the changing nature of governance in China. It can be suggested that these new forms of authoritarianism pave a pathway for a totalitarian Chinese future. Drawing from this critique, but with its changing nature in mind, I use the term “data-driven authoritarianism.” It is defined as a mode of social governance and management using (big) data, datafication and dataveillance in an authoritarian society, and how datafication and dataveillance play critical roles in governing the society’s people.

In data-driven society and data-driven authoritarianism, dataveillance can empower data owners and collectors. For instance, new technologies of surveillance and control of a Chinese Uber-like service, Didi dache, have been employed (Chen, 2018). If the right to collect consumer data lies with the government, this app-based service can be a highly powerful tool. Datafication and dataveillance offer the Chinese state a legitimate way of monitoring, surveilling and social controlling people, business and society. Likewise, the Chinese state has initiated this data-driven strategy as a “legitimate” source of surveillance and a way to transform every aspect of social life into data.

This paper explores how datafication and dataveillance fit into China’s credit score system through responses from citizens. In particular, it explores China’s emerging data-driven authoritarianism. This research ultimately hopes to contribute to the interdisciplinary literature on digital sociology and critical data studies by shedding light on the nature, practice, and reality of the Chinese social credit system that is programmed with the government’s distinctive use of datafication and dataveillance.

3. The social credit system as a “new normal”

The implementation of a social credit system has slowly changed the dynamics in academic, public, and media discussions on state surveillance and social control. With respect to datafication and dataveillance, studies have addressed mass surveillance and the digital totalitarian state (Maurtvedt, 2017), as well as the datafication of China’s social credit system (Diab, 2017). This allows us to think of the Chinese platform as not restricted to only
The Chinese Central Government promulgated a formal policy – The Planning Outline for the Construction of a Social Credit System (2014–2020) – with the aim of total national expansion by 2020 (State Council, 2016) following careful planning vis-à-vis enhanced technology and systematic control. The system had already expanded to the local governments of Taiyuan in Shandong in December 2014, Chengdu, Hangzhou, Hefei, Nanjing, Qingdao, Shenyang, Suqian, Wenzhou, Wuxi and Yiwu in August 2015. In September 2016, Qingdao became an official pilot city for the social credit system. Some of these pilot cities are located in Anhui, Beijing, Fujian, Guangdong, Hebei, Heilongjiang, Hubei, Inner Mongolia, Jiangsu, Liaoning, Shandong, Sichuan and Zhejiang (Credit China, 2018a)[4]. These places have already started collecting personal information to evaluate and save “credit scores” based on Chinese citizens’ financial, social and civic activities.

A social credit system spans both the public and the private spheres. The government aims to build a trustworthy social credit system with a role model development, and civil service integrity management and education enhancement, as well as law enforcement credibility and faith in public safety. The social credit system is being constructed also for the social sector (e.g. the medical, cultural and environmental sectors), as well as the private sector in the areas of production, distribution, finance, taxation, transportation, e-commerce, service. The system is being built to create profiles and a database of individuals who work in areas are related to credit registration in industry, commerce, service and the public sectors (State Council, 2016; Lee, 2017b) (Figure 1).

With collected and datafied information, evaluation is an integral part of the social credit system. All data are arranged into a large-scale database and analyzed, creating an individual score. A total of 30 specific criteria are regularly assessed, including records of money-related exchanges, tax records, traffic offenses, social networking and internet activities, among others. With a high score, one can easily acquire a cash advance, obtain expedited access to vital services including medical insurance and education, as well as enjoy faster processing at customs, in applying for visas and securing animal adoptions. On the other hand, individuals who have lower scores will be restricted from services[5]. These people are considered by the administration to be hurtful to others, untrustworthy, and may be labeled as scapegoats for the spread of false data and disinformation on the web.

Credit China (Xinyong Zhongguo), a website established in June 2015, offers access to credit information and the credit scores of individuals, companies and organizations for free. The scope of this research extends only to individuals’ scores, which can be accessed via four search systems: China’s People’s Bank (Renmin Yinhang); credit service organizations[6]; local credit scores: Suzhou (gulhufen), Suqian (xichufen); and telecom company credit scores: China Unicom’s Wo credit scores (wo xinyongfen) and China Mobile’s Shijinshi credit (xinyong) (Shijinshi Xinyong, 2018.) From these four main stakeholders, one can see that this social credit system is managed by both banks and private credit score services, in addition to local governments. In addition, telecom companies were also involved in pilot program cities. In July 2018, Fuzhou’s “molifen” can also be searched through the “eFuzhou” smartphone application (Fuzhou Wanbao, 2018).

Figure 1.
Social credit’s search system

Source: Credit China (2018b)
The accomplishment of such a program rests upon the government’s collaboration with private companies. Social credit companies are assigned an essential role in this process. To create a social credit framework, the Chinese Government had approved companies, including Alibaba and Tencent, to obtain individual web history records in October 2015 (Silverman, 2015). My Financial Sesame Credit is calculated using information from credit history, behaviors, performance liability, sociodemographics and social networks (Minnanwang, 2018). In Sesame Credit, internet records and personal credit ratings are obtained through the cooperation of strategic partners like Alipay and Didi Dache. Credit rating companies then evaluate individuals and assign differential advantages in light of the collected information. If one’s credit score is above 600, one can get a quick cash loan of up to RMB5,000 (US$740).

Given the increasing awareness of China’s social credit system both in and outside of China, the objective of this paper is to examine the social credit system in the realm of individuals functions as datafication, dataveillance and data-driven authoritarianism.

4. Data and research methods
4.1 Data collection
In the early stages of the system’s development, more policy and media reports were published than academic studies on the system’s policies and concerns (Browne, 2017; Hoffman, 2018; Lee, 2017b; Meissner, 2017). At the beginning of this study’s data collection process in April 2017, not many Chinese people who were initially contacted for interviews knew about the social credit system. In addition, it is important to note that keywords such as “(social) credit (system)” are not allowed to appear in the largest Bulletin Board Systems (BBS) on the Chinese internet, Baidu Tieba. Figure 2 illustrates what appears when those words are searched, “according to relevant laws and policies, the page is temporarily closed.” This message is often received as a result of search censorship, meaning that certain keywords are not searchable (Bamman et al., 2012). This response highlights the potential difficulties of conducting empirical research, which implies also that research participants may feel sensitive about the social credit system. From these, the subject of the social credit

4. Data and research methods
4.1 Data collection
In the early stages of the system’s development, more policy and media reports were published than academic studies on the system’s policies and concerns (Browne, 2017; Hoffman, 2018; Lee, 2017b; Meissner, 2017). At the beginning of this study’s data collection process in April 2017, not many Chinese people who were initially contacted for interviews knew about the social credit system. In addition, it is important to note that keywords such as “(social) credit (system)” are not allowed to appear in the largest Bulletin Board Systems (BBS) on the Chinese internet, Baidu Tieba. Figure 2 illustrates what appears when those words are searched, “according to relevant laws and policies, the page is temporarily closed.” This message is often received as a result of search censorship, meaning that certain keywords are not searchable (Bamman et al., 2012). This response highlights the potential difficulties of conducting empirical research, which implies also that research participants may feel sensitive about the social credit system. From these, the subject of the social credit

4. Data and research methods
4.1 Data collection
In the early stages of the system’s development, more policy and media reports were published than academic studies on the system’s policies and concerns (Browne, 2017; Hoffman, 2018; Lee, 2017b; Meissner, 2017). At the beginning of this study’s data collection process in April 2017, not many Chinese people who were initially contacted for interviews knew about the social credit system. In addition, it is important to note that keywords such as “(social) credit (system)” are not allowed to appear in the largest Bulletin Board Systems (BBS) on the Chinese internet, Baidu Tieba. Figure 2 illustrates what appears when those words are searched, “according to relevant laws and policies, the page is temporarily closed.” This message is often received as a result of search censorship, meaning that certain keywords are not searchable (Bamman et al., 2012). This response highlights the potential difficulties of conducting empirical research, which implies also that research participants may feel sensitive about the social credit system. From these, the subject of the social credit

4. Data and research methods
4.1 Data collection
In the early stages of the system’s development, more policy and media reports were published than academic studies on the system’s policies and concerns (Browne, 2017; Hoffman, 2018; Lee, 2017b; Meissner, 2017). At the beginning of this study’s data collection process in April 2017, not many Chinese people who were initially contacted for interviews knew about the social credit system. In addition, it is important to note that keywords such as “(social) credit (system)” are not allowed to appear in the largest Bulletin Board Systems (BBS) on the Chinese internet, Baidu Tieba. Figure 2 illustrates what appears when those words are searched, “according to relevant laws and policies, the page is temporarily closed.” This message is often received as a result of search censorship, meaning that certain keywords are not searchable (Bamman et al., 2012). This response highlights the potential difficulties of conducting empirical research, which implies also that research participants may feel sensitive about the social credit system. From these, the subject of the social credit

4. Data and research methods
4.1 Data collection
In the early stages of the system’s development, more policy and media reports were published than academic studies on the system’s policies and concerns (Browne, 2017; Hoffman, 2018; Lee, 2017b; Meissner, 2017). At the beginning of this study’s data collection process in April 2017, not many Chinese people who were initially contacted for interviews knew about the social credit system. In addition, it is important to note that keywords such as “(social) credit (system)” are not allowed to appear in the largest Bulletin Board Systems (BBS) on the Chinese internet, Baidu Tieba. Figure 2 illustrates what appears when those words are searched, “according to relevant laws and policies, the page is temporarily closed.” This message is often received as a result of search censorship, meaning that certain keywords are not searchable (Bamman et al., 2012). This response highlights the potential difficulties of conducting empirical research, which implies also that research participants may feel sensitive about the social credit system. From these, the subject of the social credit
system is not an easy one for Chinese citizens, particularly those who reside in the country and may already be subject to internet censorship.

In recognition of the aforementioned issue and the implications of not being able to search for "social credit" on the Chinese internet, I utilized a story completion strategy, created by psychologists and sociologists to inspect how investigate participants’ creative impulses emerge through stories (Clarke et al., 2017; Gibson, 2017; Giles, 2017; Gray et al., 2017; Kitzinger, 1995; Terry and Braun, 2017). This strategy has been utilized to research the fundamental implications and outcomes in the covert settings of social connections. It was chosen for this investigation to maximize informants’ creative energy as a means of gathering information.

Regarding the feasibility of the story completion strategy as a method of gathering information to assess for this project, I deliberately refrained from explicitly naming the credit system in the process of the story completion method, in order to preserve participants’ objectivity. Some subjects may live in places where the “social credit system” has just been implemented, while others do not know the details of the arranged establishment of the framework. In the event that this method revealed to participants the official name of the system, biases might have formed, as well. Subsequently, the strategy of secrecy was carried out throughout the entire information gathering stage. With that said, withholding such information may also have put limits upon informants’ creative impulses and eventually edited the substance of their data. Nonetheless, the potential affectability of the social credit framework in China situated the story creation technique as the most viable method of creating information for additional content examination.

4.2 Story completion method: study design and sampling strategy
From August to November 2017, two Chinese research assistants were procured for this portion of the task. The criteria for the study were Chinese citizens over the age of 19. At the time of the data collection, one of the research assistants, who was in China, recruited participants through his social and school networks. Another research assistant primarily focused on contacting potential participants who were outside of China. From the participants who initially participated in this research project, another round of data collection was conducted through a snowball sampling strategy. A total of 22 stories were gathered through this approach. The participants composed a half-page reaction to a given story prompt and finished the story to the best of their abilities. Participants also completed their story consummation within 10 min:

1) Study guide: prompt:
- Story.
   In Beijing, Wang is looking at his cell phone to determine his hongli score (bonus, dividend), which is a smartphone app that is provided by a collaboration between the Chinese Central Government and a company. He accessed his friend’s score and his friend’s score looks fine. He can also get his brother’s score, but his brother’s score seemed to have some problems because of a ticket he had received for speeding. Because of this, Wang could not get the RMB500 quick loan he needed immediately. The reason for him downloading this app is because he recently learned of this new experimental system in China. The government plans to use technology to gather information about all people and use that information to measure people’s performance and behavior, including financial credit and personal conduct.
- Questions.
   What do you think? What happens next for Wang and his friends and family? (Please take at least 10 min to write a story and complete the “About you” section form below.)
All research participants were of Han ethnicity\(^7\). Among them, 12 members (54.6 percent) were female and ten members (45.5 percent) were male. A total of 16 members (72.7 percent) live in China, while 6 members (27.3 percent) live abroad. The participants are relatively young, with 17 members being born in the 1990s. Geographically, participants were concentrated in Shandong, which is one of the pilot cities for the credit system and makes up 63.6 percent of the member pool. The rest were from Chongqing (4.5 percent), Hebei (4.5 percent), Henan (4.5 percent), Jiangsu (4.5 percent), Jilin (4.5 percent), Ningxia (4.5 percent), Shanxi (4.5 percent) and Tianjin (4.5 percent).

The nature of qualitative research means that this project does not aim to generalize its results. However, it is worth noting that participants include highly educated and elite Chinese citizens (only 13.6 percent of the sample have no higher education background). Yet, it is also important to mention that the participants’ educational level does not always correspond with the perceptions of their expected social class. In the demographic survey at the end of each story-completion questionnaire, only 13.6 percent of the participants identified as middle-class, the rest were identified themselves as laborers.

Once the data were collected, I carefully translated each story into English while paying attention to cross-cultural and conceptual equivalences (Lee et al., 2009). A Chinese–English bilingual researcher double-checked the translated stories. The stories were then slightly modified and saved to TAMS Analyzer (a Macintosh qualitative analysis software) for further analysis. Then, with a careful reading and a primary analysis of the data, codes and themes were identified and annotated. A content analysis was conducted to look into the meanings behind the stories, in relation to the social credit system. After that, participants’ opinions about China’s social credit system were examined to better understand the system’s covert datafication and dataveillance and how the Chinese state uses both. Finally, we considered the implications of the social credit system \textit{vis-à-vis} data-driven authoritarianism in China and elsewhere (Table I).

<table>
<thead>
<tr>
<th>ID</th>
<th>Pseudonym</th>
<th>Gender</th>
<th>Birthyear</th>
<th>Birthplace</th>
<th>Occupation</th>
<th>Current location</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Zhimei An</td>
<td>F</td>
<td>1995</td>
<td>Chongqing</td>
<td>Company worker</td>
<td>China</td>
</tr>
<tr>
<td>2</td>
<td>Juncai Chen</td>
<td>M</td>
<td>1992</td>
<td>Qingdao, Shandong</td>
<td>Undergraduate student</td>
<td>China</td>
</tr>
<tr>
<td>3</td>
<td>Liwen Chen</td>
<td>F</td>
<td>1995</td>
<td>Qingdao, Shandong</td>
<td>Company worker</td>
<td>China</td>
</tr>
<tr>
<td>4</td>
<td>Shulan Jin</td>
<td>F</td>
<td>1990</td>
<td>Zibo, Shandong</td>
<td>Student</td>
<td>China</td>
</tr>
<tr>
<td>5</td>
<td>Na Li</td>
<td>F</td>
<td>1994</td>
<td>Weihai, Shandong</td>
<td>Undergraduate student</td>
<td>Abroad</td>
</tr>
<tr>
<td>6</td>
<td>Wei Li</td>
<td>M</td>
<td>1979</td>
<td>Qingdao, Shandong</td>
<td>Company worker</td>
<td>China</td>
</tr>
<tr>
<td>7</td>
<td>Xiuying Li</td>
<td>F</td>
<td>1995</td>
<td>Tai’an, Shandong</td>
<td>Undergraduate student</td>
<td>China</td>
</tr>
<tr>
<td>8</td>
<td>Xinran Min</td>
<td>F</td>
<td>1994</td>
<td>Yangquan, Shanxi</td>
<td>Undergraduate student</td>
<td>China</td>
</tr>
<tr>
<td>9</td>
<td>Yixun Rong</td>
<td>F</td>
<td>1995</td>
<td>Qingdao, Shandong</td>
<td>Undergraduate student</td>
<td>China</td>
</tr>
<tr>
<td>10</td>
<td>Lina Sun</td>
<td>F</td>
<td>1994</td>
<td>Tianjin</td>
<td>Teacher</td>
<td>China</td>
</tr>
<tr>
<td>11</td>
<td>Gaojie Lu</td>
<td>M</td>
<td>1996</td>
<td>Kaifeng, Henan</td>
<td>Undergraduate student</td>
<td>Abroad</td>
</tr>
<tr>
<td>12</td>
<td>Yongjun Wu</td>
<td>M</td>
<td>1992</td>
<td>Yanji, Jilin</td>
<td>Undergraduate student</td>
<td>Abroad</td>
</tr>
<tr>
<td>13</td>
<td>Fang Wang</td>
<td>F</td>
<td>1989</td>
<td>Qingdao, Shandong</td>
<td>Graduate student</td>
<td>China</td>
</tr>
<tr>
<td>14</td>
<td>Shuwei Wang</td>
<td>M</td>
<td>1991</td>
<td>Qingdao, Shandong</td>
<td>Undergraduate student</td>
<td>China</td>
</tr>
<tr>
<td>15</td>
<td>Xiuying Wang</td>
<td>F</td>
<td>1987</td>
<td>Qingdao, Shandong</td>
<td>Graduate student</td>
<td>China</td>
</tr>
<tr>
<td>16</td>
<td>Feiyang Zhang</td>
<td>F</td>
<td>1996</td>
<td>Yantai, Shandong</td>
<td>Interpreter</td>
<td>China</td>
</tr>
<tr>
<td>17</td>
<td>Min Zhang</td>
<td>M</td>
<td>1992</td>
<td>Qingdao, Shandong</td>
<td>Undergraduate student</td>
<td>China</td>
</tr>
<tr>
<td>18</td>
<td>Wei Zhang</td>
<td>M</td>
<td>1965</td>
<td>Qingdao, Shandong</td>
<td>Teacher</td>
<td>China</td>
</tr>
<tr>
<td>19</td>
<td>Ying Zhang</td>
<td>M</td>
<td>1990</td>
<td>Qingdao, Shandong</td>
<td>Graduate student</td>
<td>China</td>
</tr>
<tr>
<td>20</td>
<td>Feiyu Zhao</td>
<td>M</td>
<td>1990</td>
<td>Baoding, Hebei</td>
<td>Graduate student</td>
<td>Abroad</td>
</tr>
<tr>
<td>21</td>
<td>Shengjie Zheng</td>
<td>M</td>
<td>1988</td>
<td>Nantong, Jiangsu</td>
<td>Company worker</td>
<td>Abroad</td>
</tr>
<tr>
<td>22</td>
<td>Haoying Zhong</td>
<td>M</td>
<td>1993</td>
<td>Yinchuan, Ningxia</td>
<td>Undergraduate student</td>
<td>Abroad</td>
</tr>
</tbody>
</table>

\textbf{Note:} Columns in gray are participants from a pilot city at the time of this research.

Datafication, dataveillance, and the social credit system

\textit{Table I.} Research participants’ demographic information
5. Analysis: everyday datafication and dataveillance

In this age of data-driven authoritarianism, Chinese citizens must co-exist with the social credit system (People’s Daily, 2018). Living with the system is becoming a “new normal”[8] way of life in China. In what follows, the Chinese social credit system can be understood as a sophisticated model that integrates datafication and dataveillance, modes or practices, technologies and concerns or threats.

5.1 Credit scores as a double-edge sword

5.1.1 Credit scores as public goods. The social credit system, which collects individuals’ and companies’ social credit scores, provides social goods. Credit scores collection can extend to daily activities, such as bike sharing (Xinhuanet, 2018), and commercial and public services as well as financial services (Qingdao Municipal Government, 2017). The bike-share system (gongxiang danche) was part of the first comprehensive social credit system plan published in 2014, along with e-commerce (dianzi shangwu), finance (shejinrong) and loans (xiaoyuan jiekuan) (Credit China, 2018b). Similar to the Chinese Government’s economic policy that emphasizes the nature of “sharing” (gongxiang) (Lan et al., 2017; Zhu et al., 2017), the act of sharing bikes, as a privilege in which social credits are officially applied for (Credit China, 2018b), can produce social goods for those who do not have personal goods to use.

Shengjie highlights the benefits of the social credit system by suggesting that Chinese citizens’ behaviors are associated more with creating social goods than before: “[…] Xiao Wang compared his driving speed to the time when there was no such a software for social credit scores. Now his speed is much slower than before. To improve the scores, Xiao Wang used his vacation period to do charitable activities and worked hard in public welfare activities without asking for rewards, in order to make his scores better” (No. 21, Shengjie Zheng, born in 1988, male, company worker, Jiangsu, China). Shengjie further emphasized that, “the government’s development of software is often used for collecting citizen data and using these data to evaluate an individual’s personal performance and behavior and create benign social behaviors.” Shengjie understood that the datafied information via the social credit system has a face value and that can be used for common goods.

Another participant, Wei, who shared a similar opinion stated that, “the country began to collect everyone’s scores, everyone began to pay attention to their own conduct, social ethics getting better and better. […] Wang’s family was affected by the scores, and he began to participate in social volunteer activities to improve their scores” (No. 6, Wei Li, born in 1979, male, company worker, Shandong, China). Wei conveys the idea that credit scores can enhance a society’s ethical standards and provide public goods, leveraging the system’s datafication and dataveillance process.

Similar to data, credit scores can be datafied, and datafied information can function as a means of obtaining social goods. In this system, many Chinese citizens think that the social credit system can bring stability and serve as a basis for a harmonious, socially managed society. Coupled with the sharing economy, datafied information gains higher value when tied to other’s information. What this tells us is that in data-driven authoritarianism, the government’s intentions can be considered as positive and negative, and those Chinese citizens who decode the underlying meanings behind the social credit system value the state’s positive intentions to build the system. Monitoring illegal behaviors can, in turn, provide social goods for others who cannot distinguish whom to trust.

5.1.2 Promises and perils of technologies. Surveillance is one form of social sorting and categorizing individuals and groups. It has already become a permanent feature of people’s lives and societies (Lyon, 2001). Along these lines, surveillance is closely coupled with technology and data. Together, these factors create a more complex mode of surveilling. In an era when social credit scores have become characteristic of the new normal way of life,
dataveillance – the new and augmented form of surveillance via technology – by the state can be used to conduct social sorting, monitoring and the controlling of citizens. Specifically, smartphone apps, software and online platforms play a vital role in maintaining and developing the social credit system. With the Chinese state’s partnership, Sesame Credit uses apps to inform users of their credit scores (Lee, 2017b). These technologies enable credit scores to be integrated, saved into databases and used for dataveillance. In this regard, technology facilitates the social control aspect of dataveillance in online and offline spaces, as Shulan communicates:

[...] subsequent to returning home from work, Xiao Wang told his family about this high-tech system and said that the system can watch his relatives. If a relative has committed an illegal act, it will affect the entire family, so always remaining law-abiding is the only way to benefit the family. He then contacted his friends, as well, and told them that this magical system exists, but also to remind friends to be careful everywhere. He also hoped that his friends would convey this to more friends, to remind everyone to be careful and well-behaved. (No. 4, Shulan Jin, born in 1990, female, Student, Shandong, China)

The development and use of technology within the social credit system is certainly a proactive and mundane way of disseminating dataveillance through technology. It also illustrates how datafication and dataveillance are intertwined with technology. This was also captured in the USA’s credit score, CreditScoreDating, job markets among others (O’Neil, 2016) and echoes Hoffman’s (2018) argument that the system is not bound to the nation of China. In other words, in this globalized world, one’s experiences can also be tracked across borders as part of his or her social credit score because scores are stored in a database – perhaps in the “cloud” of a private company that is linked to China or another country. These data, which were collected through the system, are not only useful for Chinese citizens and businesses but are also valuable for individuals and companies beyond national boundaries. Due to their relations with foreign entities and individuals, participants in this study clearly imagined their own overseas futures and, more importantly, how China’s social credit system could extend to other countries in the long run. Along these lines, datafication serves as a basis for dataveillance and serves China’s “invented” social credit system well.

At the same time, Shulan also noted the consequences of the social credit system, such as privacy infringement. Her scenario continued: “In the wake of using this new experimental system, Xiao Wang laments the rapid development of high technology and the disappearance of his privacy. This situation also makes Wang aware of the importance of law-abiding, cautious work” (No. 4, Shulan Jin, born in 1990, female, student, Shandong, China). The infringement of privacy is a potential consequence of the scenario and the social credit system.

Another participant also sheds light on the privacy issue in the following story: “Although Wang got the loan of 500 yuan, he has always felt that he is on the radar. Sometimes, people around him know the record of Wang through the app. Xiao Wang believes that using this software to invades personal privacy to some extent. Everyone has their own information, have their own privacy rights, and some people do not want their privacy to be leaked. Everyone’s financial credit is their personal information. Xiao Wang and his friends may face the risk of information being leaked in the future. Later on, they decided to file a protest request with the government” (No. 3, Liwen Chen, born in 1995, female, Qingdao, China). Liwen’s comment of “everyone’s financial credit is their personal information” encapsulates the social credit system’s nature regarding dataveillance, which increases individuals’ privacy concerns, which echoes Taylor’s (2017) work.

In the process of the state’s utilization of a social credit system to mine and store data, citizens largely remain unaware, but increasingly equip themselves with ways to work
around the technology inside the social credit system. Na Li has recommended creating a strategy to use technology in relation to datafication and dataveillance:

This experimental system now seems to be working very well and has become a part of everyday life for Chinese citizens. Everyone who has been evaluated will be able to borrow only a certain amount of money that can be borrowed, just as any bank or loan service organizations needs to measure individuals. However, no one expected that, after just ten years, this measurement system would spread across all aspects of life. It’s not just about lending money, even what kind of work a person can find, how high they can be promoted, and what level of service they can receive in a restaurant or other service area in life is affected. (No. 6, Na Li, born in 1994, female, student, Weihai, China)

Na understood the potential expansion of the social credit score system as well as the dangers and hazards of the system, which are tightly combined with technologies and smartphone platforms. Like other technologically propelled systems, this score system could be hacked. This demonstrates the vulnerabilities of the system, and the data and information that the system potentially holds.

Some participants realize that the social credit system gives them no privacy at all. This is well depicted by Feiyu’s scenario. He laments that “in the future, due to the continuous upgrading of state surveillance, people’s lives are closely monitored and have no privacy. Wang was on a business trip to Shanghai because of her work, but his scores were deducted because the day before the garbage collection day, the waste was not properly thrown to the designated place. He arrived in Shanghai, ready to stay in a hotel, but because his scores did not reach full marks, the hotel refused to give him a room. Wang could only call his Shanghai friend, but he had been expelled by the company because his score plummeted” (No. 20, Feiyu Zhao, born in 1990, male, student, Hebei, abroad). This story illustrates not only how dataveillance functions, but it also alludes to the ways in which the system and apps permeate people’s lives. Privacy is not guaranteed and becomes an important part of the concerns brought forth by the participants in this study.

Recently, individuals are increasingly concerned about the potential threats that datafication and dataveillance might pose to them. Citizens’ rights, civil liberties and social justice issues related to datafication are becoming a part of the awareness for scholars (Dencik et al., 2016; Kennedy and Bates, 2017; Taylor, 2017), as well.

Dataveillance via technology plays an important role in China’s data-driven social credit system. The proliferation of digital technologies impacts datafication and dataveillance, especially of young people (Lupton and Williamson, 2017). While a proactive, technology-based approach to dataveillance is beneficial to the state, such a system regularly faces issues regarding technological, cybersecurity and privacy concerns. With the further development of the credit system, it is important for us to pay attention to an involuntary aspect of datafication and dataveillance via technology that might increase technological perils – cybersecurity and privacy – for Chinese citizens.

As discussed above, the social credit system is a double-edged sword. On one side, it may elevate societal levels of honesty and trust on the whole. Individuals and companies who follow the system’s guidelines receive special treatment and speedy administrative services. Nonetheless, mistakes potentially extend even beyond those who do not follow the credit system. Subsequent blacklists serve as a mechanism that will weed out “unqualified” individuals and companies, as the current Credit China website outlines. It also increases levels of government supervision and develops a revealing framework for extended social control.

5.2 Collective punishment of the social credit system
While credit scores are determined by one’s own behavior, there is a potential for scores to be computed and influenced by people within one’s social network. Like the US financial
credit score system, the Chinese social credit system also leverages individual liability. What makes the Chinese social credit system unique and punitive, however, is the “social” part of this system. This comes from China’s long-time collective punishment (lianzuo) practices, inherited from the Qin dynasty (Lau and Stacck, 2016). The policy of guilt-by-association has been commonly practiced in China to control people, protesters and unrest (see Deng and O’Brien, 2013). The chain effect, generated by one’s social network, might result in opportunities for subjects to subconsciously police each other.

Zhimei discussed the chain effect in her scenario:

When Wang watched his friend’s score go bad, he began to fear that it would affect him to get a loan from a bank quickly. So, he thought of substituting his friend’s score for his brother’s score and waiting for the loan before switching the scores back. This is what he did, but when he selected his friend’s score and wanted to exchange it with his brother’s score, the app displayed a red alert and he panicked. One fears that one’s own behavior will have a bad influence on one’s friends, but one is also afraid that one will be affected. (No. 1, Zhimei An, born in 1995, female, company worker, Sichuan, China)

In this scenario, Wang’s unemployment was due to his brother’s deviant behavior. This situation illustrates how important it is for Chinese citizens to manage their social networks’ social credit scores in the era of the social credit system. This collective punishment method has preventative measures in place to keep one’s social credit scores from falling perilously low by tying it to those of close social network members.

In connection with this, scholars voice their concerns about the consequences of the system (Chin and Wong, 2016; Hintz et al., 2017). Social networks can be personally harmful and affect others’ lives when an individual engages in inappropriate behavior and generates a low social credit score. With such effects in mind, Gaojie introduces a credit score exchange mechanism in her scenario:

Wang began to carefully maintain his own score, and he knew that not long afterwards, the score would not only be the voucher for the loan but would also be the standard for friends to evaluate each other.

This app has quickly become popular, but also more and more powerful. The app not only collects people’s financial and life conditions, even people’s private life. First work late, leave early, work performance, and then every time you say dirty words, every time you visit bad pages it is recorded. The government has created a super-algorithm that comprehensively analyzes the data to give everyone a score. High marks tend to receive more respect. So everyone is careful about what you say.

Later, Wang through hard work, got a very, very high score, because of the high score, he found a new and better job and began to go on blind dates. (No. 11, Gaojie Lu, born in 1996, male, student, Henan, China)

Gaojie’s scenario was crafted with the expectation that individuals’ scores could be “traded” with those of others in their social network. Trading as an exchange for economy is synthesized with who the individuals know and what kind of relationship they have. Such an expectation is not necessarily inaccurate, because China’s credit system is moving toward that direction. While collected data are used for systematic dataveillance, the “social” part of the system is particularly strengthened by the punitive aspect of dataveillance.

Xiuying imagined the following scenario, which is linked to the previous participant’s story:

Xiao Wang first seeks opinions from friends about whether or not he could transfer his friend’s scores to his younger brother. He hopes to get help from his friends for further loan services. Then, he contacted his brother to ask if he could pay a speeding ticket as soon as possible, but the younger brother said that he has no money now and there is no way to pay the ticket. Xiao Wang couldn’t get a loan, and he learned that this was because of his brother’s wrongdoing. He had a big fight with his brother, and because he didn’t score a friend, Xiao Wang stop seeing his friends. (No. 15, Xiuying Wang, born in 1987, female, student, Qingdao, China).
Credit-scores trading is a unique way of utilizing the chain effect and social network into reality. Such trading is possible because the participant is aware of the collective connection of the system. This awareness indicates that, in the future, the credit system is likely to be taken advantage of by some Chinese citizens who will loopholes to obtain new benefits or utilize the existing system with new functions.

We identify complementary spheres within the everyday dataveillance mechanism: family-oriented and social network-oriented circles on the one hand, and dataveillance via technology and its advantages and perils on the other. Each trajectory and mechanism entail specific tactics for datafication and dataveillance and, in particular, deviant behaviors within society, but all are embedded within the web of state and social control in Chinese society.

6. Discussion and conclusion

This paper demonstrates how China uses its social credit system as an apparatus of datafication and dataveillance by combining a qualitative content analysis of 22 stories and through analyses of policy and media reports. This research contends that China’s social credit system is an important case study for investigating data-driven authoritarianism, wherein a state’s social control tactic has translated into citizens’ own practice of self-surveillance (Lupton and Williamson, 2017). At one end, the social credit system institutionalizes dataveillance via datafication, and enacts social control upon its subjects. At another, how citizens respond to the system on a daily basis demonstrates adaptive self-surveillance, and how data-driven authoritarianism becomes deeply embedded and programmed into individuals.

Methodologically, this paper was able to examine and understand Chinese citizens’ perceptions of the social credit system utilizing the stories that study participants created. This data revealed that China’s social credit system can be understood through the concept of public goods, technology, privacy and collective punishment. These elements factor in how the social credit system is embedded within and supports data-driven authoritarianism. Social credits collected across different government and private platforms are datafied (Lee, 2017b). The social credits are then prepared for further evaluation by individuals and companies who involuntarily “opted in” to the social credit score-awarding program run by the government. These datafied social credits serve as a critical basis for Chinese dataveillance. What is also important is the government’s ongoing efforts to link individuality with collectiveness. The essential premise of this system is the persuade citizens to control themselves, in addition to policing their interpersonal networks. This outlined framework focuses on the China context, but it is also plausible that this particular governmental model applies to other societies, as well.

Technologies, smartphone applications and platforms play a significant role as facilitators and actors by highlighting the presence of dataveillance in China’s social credit system. With an expanding level of mindfulness, critical views on the social credit system, and the potential for disrupting the system from the inside, are points of discourse on this subject. By demonstrating how the social credit system rewards and programs citizens through the utilization of big data and technological innovation, this study offers implications for how China’s data-driven authoritarianism will continue to develop.

In addition, it is advantageous to consider the discoveries of this exploratory research to Chinese citizens’ reactions in this time of a social credit system as the “new normal.” The system is still just beginning to spread across the country. Existing frameworks in comparative studies, for example, understand that the USA’s credit score system in the private sector is different from the Chinese social credit system (O’Neil, 2016), and that public–private partnership might illuminate countermeasures and future developments in China’s social credit system. The social credit system is unique to connect financial, social and behavioral scores into the system and take into account of social networks into scores; however, its manifestation exists in different forms and contexts. It is also important to further investigate the situations and actors would be more affected by the social credit system.
For instance, whether different online lifestyles would lead to larger exposure to the social credit system’s disadvantages should be studied with a large-scale survey of Chinese citizens. In addition, with data mining and web analysis of Chinese online discussions from news media, BBS and social media, the connection between online and offline spaces, in relation to the social credit system, could also be a part of future research agendas.

As the social credit system is still a new topic in scholarly research, this study marks an initial, yet important, addition to the emerging body of literature. This research demonstrates the importance of assessing the social credit system with Chinese citizens’ narratives, and how the state’s governmental model of data-driven authoritarianism is carried out through the social credit system. In addition, it also reveals how citizens are coping with, and imagine adapting to, this new system. The present research offers clarifications for how the social credit system uses datafication and dataveillance. Similar to trends in cybercrime victim demographics, less educated and more elderly individuals who are typically less tech-savvy might become targeted more heavily by this system. The social credit system might have broader socio-political implications such as prejudice, structural social inequality, privacy and data justice in the near future. Critical examination of the implementation and development of the social credit system are necessary.

Currently, one can use an API on the CreditScore website to access the credit scores of individuals and companies with approval. This relative transparency, however, means that citizens should also be cautious of the consequences of datafication and dataveillance. If Credit China’s database were to be hacked and used unlawfully, the results could be wide-spread. The 2017-enacted Chinese Cybersecurity Law increases awareness of potential cybersecurity threats, but at the same time enables the government and law enforcement agencies to create loopholes and evade the law.

This study presented empirical results based on the voices of different stakeholders, from the state, to the media, to individuals. However, this study is not without limitations. We hope that this research will further the understanding of datafication and dataveillance as it is connected to cyberspace, and how data-driven authoritarianism will continue to develop.

Notes
1. *Black Mirror* is a British television series. The quotation was from “Nosedive” (Episode 1, Series 3), which was initially aired in October 21, 2016.
2. The scope of this paper is limited to individual credit scores only.
3. Boyd and Crawford (2012), for example, call for a critical understanding of big data in terms of definitions, scopes, uses and applications in social mediascape. Qiu (2015) brings us to the debate about accessibility and ethical concerns of big data, which has vast volume, veracity, velocity.
4. At the time of the research, pilot cities include Anqing, Hefei, Huaihai and Wuhu (in Anhui), Futian, Fuzhou and Xiamen (in Fujian), Shantou, Shenzhen and Zhuhai (in Guangdong), Suifenhe (in Heilongjiang), Nanyang and Zhengzhou (in Henan), Huangshi, Wuhan, Xiamen and Yichang (in Hubei), Suqian, Suzhou, Nanjing and Wuxi (in Jiangsu), Anshan, Dalian and Shenyang (in Liaoning), Dezhou, Qingdao, Rongcheng, Weifang and Weihai (in Shandong), Chengdu (in Sichuan) and Hangzhou, Huzhou, Taizhou, Wenzhou and Yiwu (in Zhejiang).
5. In June 2018, the National Public Credit Information Center (*Guojia Gonggong Xinyong Xinxi Zhongxin*) published the first Black List Monthly Report covering May 2018. The report offers a comprehensive information on “black list” (heimingdan) companies that are currently being penalized.
6. The organizations include agencies like Baidu Credit Scores, Tianxia Credit Scores with *Pengyuan Zhengxin*, Sesame Credit Scores with Sesame credit, Tengxun Credit Scores, Qianhai Credit (haoxinfen), Zhongchengxin Credit (wuxiangfen), Kaola Credit (kaola xinyongfen), Jingdong Zhengxin (xiaobai xinyongfen), Wanda Credit (feifan xinyongfen), Huadao Credit (xinyong wendu), and Zhongqing Credit (younifen).
7. Han Chinese account for about 92 percent of the whole population in China.

8. A “new normal” (xin changtai) is a newly established standard for China’s economic growth as opposed to the previous decades when China’s exponential and unprecedented two-digit economic growth was maintained. In the Chinese context, Xi Jinping’s administration coined the idea of a “new normal” economy in 2015. It is also used in academic papers and media in English as well.

References


Datafication, dataveillance, and the social credit system


Lau, U. and Stacck, T. (2016), Legal Practice in the Formative Stages of the Chinese Empire: An Annotated Translation of the Exemplary Qin Criminal Cases from the Yuelu Academy Collection, Brill, Leiden and Boston, MA.


Further reading


About the author
Claire Seungeun Lee is an incoming Assistant Professor at the School of Criminology and Justice Studies at the University of Massachusetts Lowell, USA and is Affiliated Researcher at Boston University’s Cybercrime Investigation & Cybersecurity Lab. Trained as a sociologist, her research interests include the movement of technology, people, deviance and crime, and social implications of digital technologies and platforms. Claire Seungeun Lee can be contacted at: drclaireselee@gmail.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
What difference do data make? Data management and social change

Morgan E. Currie
*University of Edinburgh, Edinburgh, UK, and*
Britt S. Paris and Joan M. Donovan
*Data and Society Research Institute, New York, New York, USA*

Abstract

**Purpose** – The purpose of this paper is to expand on emergent data activism literature to draw distinctions between different types of data management practices undertaken by groups of data activists.

**Design/methodology/approach** – The authors offer three case studies that illuminate the data management strategies of these groups. Each group discussed in the case studies is devoted to representing a contentious political issue through data, but their data management practices differ in meaningful ways. The project Making Sense produces their own data on pollution in Kosovo. Fatal Encounters collects “missing data” on police homicides in the USA. The Environmental Data Governance Initiative hopes to keep vulnerable US data on climate change and environmental injustices in the public domain.

**Findings** – In analysing the three case studies, the authors surface how temporal dimensions, geographic scale and sociotechnical politics influence their differing data management strategies.

**Originality/value** – The authors build upon extant literature on data management infrastructure, which primarily discusses how these practices manifest in scientific and institutional research settings, to analyse how data management infrastructure is often crucial to social movements that rely on data to surface political issues.

**Keywords** Civic data, Data activism, Data infrastructure, Police data, Statactivism

**Paper type** Research paper

Introduction

What difference do data make? Over the last decade, scholars have struggled to understand the rapid informationalization of society, as the data that drive this trend grow larger by the moment, are increasingly commodified for private profit and are used to control populations through both finely targeted advertisements and surveillance architectures that link corporate and government data streams. A rigorous set of scholarship now addresses this issue of data quantity by focussing on the sociotechnical dimensions of data infrastructures – how “big data” is collected, categorised, analysed, stored, controlled and accessed, and how these practices produce widely uneven distributions of political and economic power (Eubanks, 2018; Bates et al., 2016; Ribes and Jackson, 2013).

Simultaneously, a growing set of literature examines social and activist movements that organise in response to data collection by corporations and the state (Milan and Van der Velden, 2016; Liboiron, 2015; Currie et al., 2016; Bruno et al., 2014; Dalton and Stallmann, 2018; Dalton and Thatcher, 2014; Gieseking, 2018). In some cases, these political activists achieve some agency by avoiding data capture through the use of encryption devices or by designing alternative, non-commercial and collectively owned platforms. Other activists respond by creating their own representations and framings of an issue through community data collection, visualisation and analysis. An example of the latter are data activist projects that collect and publish data on policing in the USA. Here, the best data generated from the Federal Bureau of

The authors specially thank volunteers from the Environmental Data and Governance Initiative, Fatal Encounters and Making Sense.
Investigation consistently underestimate the body count of those killed by police, so activists and journalists approached the issue through various methodologies to improve accuracy. Whether working with data to make an issue more visible or to contest its “official” representations, the results are often only a small part of these activists’ actual work. Behind the visualisations or public-facing databases are a suite of data management infrastructures and organisational norms that form a considerable part of activists’ mundane practice. For activists who rely on data to represent and politicise an issue, the acts of standardising data, anonymising it and making it robust over time are essential group strategies. In many cases, groups will be concerned to keep track of who contributes and accesses data, to guarantee they remain safe from tampering, and to ensure their longevity in electronic storage media. Yet, these broader infrastructural practices of data activists are an often-underappreciated area of scholarly attention in literature on these projects.

This paper’s central focus is on the data management practices of data activists; it argues for more research devoted to the infrastructural needs of social movements that rely on data to politicise issues. To make this argument, we begin by defining data activism, drawing on a rich and growing set of literature on the topic; through this research, we make some conceptual distinctions between types of data activists that we draw on for our case study selection. In the second section, we examine literature on data management infrastructure, most of which we find focusses on large institutional projects generally within government or research universities; less research is devoted to projects arising from the level of grassroots social movements.

In the third section of the paper, we offer three case studies that provide a window into the data management strategies of groups devoted to representing a contentious political issue through data, either by producing their own data, collecting “missing data” or keeping vulnerable data in the public domain. Methodologically, evidence for our three case studies is drawn primarily from personal interviews with a member from each organisation, selected because he or she played a relevant role in some aspect of these projects’ data infrastructural work, whether selection, design, implementation, governance or use, or a combination of several of these activities. We combined these interviews with news reports about issues of concern to these activists, media coverage of the activist projects and several primary documents in the form of procedural reports and press releases produced by these projects. Finally, in our conclusion, we discuss some of the implications revealed in the case study analysis. In particular, we find lessons to be learned regarding the role that data management plays in shaping the governance structures of data activist projects, as well as the need to attend to the political-economic dimensions of information infrastructure itself.

The nuances of data activism
In the past decade, scholars within Information Studies, Geography and Science and Technology Studies (STS) have sought new terms to describe data practices as novel forms of activism and resistance. These scholars, and the activists they analyse, understand that data are not benign, neutral information resources underpinning our representations of the world, but are a major source of political power and social critique. While in some instances the practices that fall under the term “data activism” may not be new, the literature largely positions data activism as a response to several forces specific to the past several decades: the use of indexes and benchmarking indicators by the modern nation state, numbers that are so routine that they produce reality “through an irreversible ratchet-effect” (Desrosieres, 2008, p. 12); the capturing and monetisation of online user data and the consequent rise of finely tuned microtargeting that sways commercial consumption and political votes alike (Smicik, 2016; Tufekci, 2014a); the often covert exchange of data between powerful commercial platforms and government surveillance apparatuses; and the fact that online
surveys, digital mapping and digital sensors are now widely accessible and relatively affordable to lay publics.

Given this backdrop, literature on data activism documents examples of citizens who use data to address the vast informational asymmetry in democratic societies. Scholars of citizen science, for instance, offer rich case studies that expose the power imbalance between scientists and laypeople in making scientific claims about climate change, air pollution and the design of urban space (Irwin, 2001). Scientists have at their disposal highly technical “inscription devices”, such as microscopes and lab protocols that make their objects of study stable, authoritative sources of information (Latour, 1987). The general public, in contrast, often has very few and highly unreliable devices with which to make claims (Priest, 2013). Nevertheless, as these scholars have shown, lay publics can use their own data gathering techniques to intervene in scientific debates and enact more democratic forms of environmental policy making as a result. Citizens have used data, for instance, to contest chemical weapons disposal in the USA (Futrell, 2003), map the exposure to toxins and pollutants in buildings (Murphy, 2006) and take lo-fi aerial photographs to document evidence of sewage flow into protected sites (Wylie et al., 2014).

Bruno et al. (2014) use the term “statactivism” to pinpoint more precisely activists who use “numbers, measurements, and indicators as a means of denunciation and criticism” (p. 199). Statactivism acknowledges “the double role of statistics in representing as well as criticizing reality” and of revealing the political and negotiated dimensions of statistical work (p. 200). The authors describe how statactivists can use statistics to make a community, social category or cause more visible; they illustrate the force of a new social category, for instance, when citizens championed the need for the government to recognise a new class, the intellos precaires, or precarious workers, who have higher education degrees but no reliable long-term employment. Once established as a stable category, individuals who fall in this group can start putting forward collective demands. Statactivism can also cast doubt on or rejects official state indicators and benchmarks. Scholars from critical GIS (geographic information systems) similarly call such acts of resistance to institutional and commercial data sets “counter-data actions” (Dalton and Thatcher, 2014, n.p.). The concept of counter-data draws from longstanding work in critical GIS to create alternative cartographies that privilege the geographic knowledge of individuals, such as indigenous groups or LGBTQ communities, often left out of mainstream political discourse, science, industry and technological practice (Dalton and Stallmann, 2018; Gieseking, 2018).

To widen their scope of analysis beyond statistical or numerical representations, Stefania Milan and Lonneke Van der Velden (2016) use the term “data activism”, which includes making use of visual and qualitative data as well as tactics to avoid data capture. What the authors term “pro-active” data activism uses data to create or contest representations of an issue, while “re-active” data activism avoids data collection and surveillance through encryption tools, obfuscation and anonymity. This stark binary can easily fall apart – re-active tactics can also entail very pro-active, creative design strategies that offer alternatives to data extraction platforms – but it does begin to make important analytical distinctions between various types of data activism.

This paper focusses its analysis on what Milan and Van der Velden term the “pro-active” type – those activists who work with data as a tactic to challenge authoritative accounts that are either inadequate, politically vulnerable or misleading, and who must generally consider some form of data management practices to put forward their case. We want to spotlight the practices of political movements devoted to issue visibility specifically through data collection and maintenance. In these cases, the acts of creating and managing data are not ancillary to movement building but are the adhesion that tie activists together and make their political movement cohere.
We also selected examples that further nuance this literature, by showing how representational work can manifest in at least three ways. The first two cases offer examples of counter-data, though responding to slightly different deficiencies of government accountability. In the first case, we describe citizens’ response to data that has not been gathered by the state in any comprehensive manner to fully assess a phenomenon. We use an example of data activism that sought to correct and augment the statistical work of the US Government, which fails to account for all deaths caused by police. For activists opposing police brutality, such as Black Lives Matter, recourse to reliable and accurate statistics on deaths in custody has been a crucial strategy to call for policing reforms. We illustrate how one organisation, Fatal Encounters, uses a collective database to produce this missing data and so critique the data that does exist. In our second case study, we examine activism that produced a new dataset to make visible an issue that was being deliberately obscured by their government. In this case, activists collected air quality data around Kosovo and in its capital city, Prishtina; they used the data within media campaigns to force a public debate around a health crisis that the government had largely kept invisible. Our final example focusses on visibilising an issue by means other than critiquing existing institutional data. In our third case study, we look at activism undertaken to keep politically vulnerable data in the public domain. We look at the DataRescue work led by the Environmental Data Governance Initiative (EDGI), comprised of networks of scholar-activists that formed in reaction to Donald Trump’s election. EDGI’s goal was to archive data created by US federal scientists that documented evidence of climate change and human-induced ecological violence.

Controlling representations entails careful epistemic work. Open, collaborative networks of contributors in particular will want to ensure that the data are reliable and withstand scrutiny in the public sphere. Yet, outside of some more detailed descriptions of civic science and sensing projects (Jalbert et al., 2017; Kinchy et al., 2014; Wylie et al., 2014), literature on data activism has rarely examined data management infrastructures of activists with close scrutiny. Literature on data activism typically describes the project of generating data to create new statistical representations or to challenge official ones, and it often looks at how these representations circulate; it has widely ignored issues of stewardship and the dynamics of data management among the activists themselves. Moreover, the ways in which various groups practicing data activism think about the politics of the infrastructures they engage with to collect and maintain their data is under-represented in this scholarly work. In the following section, we briefly go over scholarship focused on data management infrastructures to clarify some heuristics for examining these practices, before moving on to our case studies.

**Particulars of activist data management**

When we talk about infrastructures of data management, what, exactly, does this encompass and what does it mean in the particular cases of grassroots activists? Just as literature on data activism has devoted less focus on everyday data management infrastructures, so professional literature on data management often has very little to say about its manifestation in grassroots settings outside of government, corporate and scientific contexts. Within archival science and information studies, the concern is almost solely on the design, adoption and use of data repositories in university and government settings (Lauriault et al., 2007; Borgman, 2007; Frost et al., 2015; Borgman, 2015)[1]. For instance, “Elements of a Data Management Plan” is a list provided by the Inter-university Consortium for Political and Social Research, which maintains one of the oldest research data archives in the world[2]. The elements list factors of data maintenance relevant to projects that rely on managing data sets: the need to consider data formatting, back-up, access and sharing rights, ethics and privacy, and quality assurance, among several others.
This list provides a standard rubric or heuristic for thinking about those practices that groups involved in data collection and maintenance for evidence collection may need to consider. However, this professional literature is limited because it is concerned with establishing good practices for institutional settings only.

This professional literature also does not offer a framework for analysing data management practice within broader, sociotechnical relations. Drawing on STS literature, we think of data management not only as a set of best practices but as relational infrastructures. Infrastructures in this sense are not a set of connected technological artifacts programmed to be useful but largely unnoticed; instead, infrastructures emerge through relations of users and within the context of the other social, institutional and economic systems that they are necessarily part of (Star and Ruhleder, 1996; Dodge and Kitchin, 2007; Ruppert, 2012). This framing helps us analyse infrastructures of data management as a non-linear, non-routinised set of relations between people and technologies working in complex organisational contexts. In these settings, difficulties will inevitably emerge; these may not be resolved by gaining more information or skills, such as a new user who learns to onboard a system, but may encompass more complicated cultural dynamics that arise around access privileges, software selection, privacy concerns and economic trade-offs, to name just a few. Infrastructures shape these dynamics as much as they are shaped by them. Yet even this STS literature is largely absent of cases that look at data infrastructures at grassroots levels; instead, it offers rich descriptions of government censuses, scientific data models and systems of corporate data capture and dissemination (Star and Bowker, 1999; Edwards, 2010; Kitchin, 2014; Gillespie, 2018). This literature therefore raises a set of questions about the dynamics of these practices particular to activist projects working outside of institutions.

Take, for instance, that literature on data management in a research context often assumes colleagues who share some institutional, disciplinary or technical knowledge. Data activist projects, on the other hand, coordinate people with widely different backgrounds and skillsets, some of whom may never meet face to face. Many data activist projects will need a structure to manage multiple contributors and low barriers entry for participation while maintaining data integrity. How this coordination takes shape, whether through gatekeeper and hierarchies of access permissions or by more radically decentralised and participatory methods, also shapes the relations among the participants themselves.

A related question concerns storage, back-up and security: does someone take the ultimate responsibility of keeping an electronic data set secure in storage media so that it is reliable over time, or can this role be federated or even outsourced? Who designs the formatting and description protocols of the data set? In university or government settings, the roles regarding data management tasks may be set by traditional institutional hierarchies (senior researchers on down to postdoc and PhD students), but for grassroots activists in the civic sphere, defining these roles may be ad hoc as the data collecting or maintenance unfolds; it can, for instance, fall to the work of one or a few people with technical and professional skills or take shape through more democratic decision-making procedures.

Finally, we can ask about the politics of the technologies used to store and maintain data. Literature on data management does address the wider political economy of software, particularly by arguing for the economic virtues of open source software over closed licences or commercial platforms (Frost et al., 2015; Fry et al., 2008; Strasser, 2013). In the institutional research context, digital data repositories that are not tethered to expensive licensing contracts can have greater longevity and make their content free to users. Yet data management literature has less to say about the activists’ wide use of social media to publicise, galvanise and organise contentious politics. For grassroots projects with little to no business plan or funding, off-the-shelf “free” platforms may be the best tool to get the job done. Activists often use social media to locate each other and narrate their causes to
wide audiences; these platforms boost organisational capacity of people working outside of traditional institutions (Tufekci, 2014b).

Yet in other cases, platforms such as Google or Facebook could pose problems in the long term should the policies of these opaque companies change or if activists want more control over their data, particularly when privacy becomes a concern. Writing in 2011, a year after Facebook went public, Geert Lovink (2011) lamented that “Activists organize transnational campaigns online, and Web 2.0 companies profit from the free labor and attention provided by networks of users” (pp. 167-168). The awareness of “platform capitalism” has only since grown (Srnicek, 2016). As a result of the surveillance and data capture by these corporate platforms, some activists are now building their own alternative communication and networking systems to mobilise and exchange goods and transactions using open source software, platform cooperatives, mesh networks and alternative internet protocols. An analysis of data activists and their management tools, therefore, should look at both the use and repurposing of networked media and at alternative technological platforms created to sustain their work. We can ask whether projects build alternative infrastructures that give owners more control over their data, and we can ask to what extent these technologies might shape the data in terms of formats and automated metadata.

In sum, while literature on data management infrastructure falls short in discussing the practices of grassroots projects operating outside of institutional contexts, it focuses our attention on a few dimensions that we can ask of data activist projects:

(1) How did the coordination of the data management take shape – that is, how does the data’s collection and maintenance become distributed between participants over time?

(2) How are the platforms that collect, store and update the data managed over time – by one or few individuals or collectively?

(3) How are access and sharing privileges across data infrastructures determined and distributed?

(4) Who designs the data formatting and description protocols, and who makes sure these are maintained over time?

(5) How do these data infrastructures play a role, in turn, in shaping the relations among participants?

(6) What software has been chosen to maintain the data, how was it chosen and what is its wider political economy – i.e. open source software vs freemium platforms vs commercial software that must be licensed?

Though these are no means exhaustive, we draw on these six factors now to analyse our three case studies looking at missing data, vulnerable data and data created to make an issue newly visible in the public sphere.

Case study 1: filling in the gaps

The accuracy of statistics on policing is one of the most persistent problems facing activists in the Black Lives Matter Movement. After the death of Michael Brown in 2014, widespread protests across the USA called for increased accountability and oversight of policing practices. Multiple organisations took up the charge of gathering statistics on the number of people killed by law enforcement. Similarly, activists in the early 1990s sought the very same data on policing after the Rodney King trial and the acquittal of officers from the Los Angeles Police Department. In 1994, the Attorney General was mandated to collect data on the “use of excessive force”, and the Bureau of Justice Statistics (BJS) was to issue an annual report on this (McEwen, 1996). However, the law
never required state law agencies to report to BJS. As a result, year after year, the BJS continuously admonished police departments for failing to provide accurate – and, in some cases, any – counts of deaths in custody or provide consistent metadata so that trends could be charted over time (Smith and Austin, 2015; Mumola, 2007). Relying only on police departments for this information, the BJS faced a persistent problem of missing data.

As the public sought ways to hold police accountable, grassroots groups and data journalists built public databases of police killings by sourcing materials across a wide array of public records requests, media reports, obituaries and social media. Many of these databases relied on crowd-work to harvest missing metadata and fill in gaps related to information about the officer and the person who was murdered. Methods of data collection and categorisation vary across all projects (Currie et al., 2016). Here we focus on the group Fatal Encounters. The project was volunteer-run and directed by its founder journalist, Brian Burghart, from its inception until 2014, when it started to receive grants. Until 2017, Burghart received grant funding to direct the project, and received help from both unpaid and paid volunteers[3]. The website charts deaths by fire, vehicle, stabbing, choking, suffocation, pepper spray and more. Fatal Encounters also uses Freedom of Information Act requests, which provide data on deaths that may never get reported on or appear in newspaper obituaries (Burghart, 2017b). This citizen data came up with numbers that were in many instances larger than those published by the US Department of Justice.

Organisationally, Fatal Encounters is a hierarchy run by Burghart, who delegates access privileges, manages the data’s backend, and designed the Google document that formats and standardises all entries. Data contribution, however, is federated: anyone who wants to contribute to the data set can do so through a Google Form vetted by Burghart[4]. The data then populate a private Google Sheet that feeds into a CSV file that streamlines the metadata and is backed up and maintained by Burghart. To collect the data, Fatal Encounters’ volunteers draw from a multitude of sources: FOIA requests, public records, police records, media reports, coroner reports, social media submissions, photographs, original reporting and crowdsourced verification (see footnote 4). Fatal Encounters’ founder double checks all the reports received against local news stories before publication. Fatal Encounters tends to track and record more data than other groups (such as the counts maintained by The Guardian and The Washington Post). Because Fatal Encounters values exhaustive and comprehensive verification, some cases may stay in the database until such time that the cause of death has been clarified, either through public records, FOIA requests or updated media reports. These data are finally made public on a Google spreadsheet that is accessible and downloadable, but not editable, online.

In the interest of time and financial resources, the group uses free Google software – Google Forms and Google Sheets – to solicit data from the public and manage the data they collect from FOIA requests, independent investigation and public reports (Burghart, 2017a). Using free software works well for this group, since it creates a very low bar for participating in terms of technological skill (see footnote 4). In cases of more politically vulnerable data, however, this practice of using free corporate software may not suffice.

Problem 2: creating new data
Kosovo is one of the EU’s most polluted countries, and, by 2015, the consequences on citizens were becoming apparent through rising rates of cancer, respiratory tract infections and cardiovascular diseases (Making Sense, n.d.; McQuillan, 2015). The government response was to remain silent amidst this health crisis, and its Environmental Protection Agency refused to release air quality data that could stir public outrage. In this context,
the country became one of the pilot sites for Making Sense, a citizen sensing project that determined to make the country’s environmental problems visible.

Making Sense is a European project involving five partners, with research for policy and action led by faculty at University of Dundee. One of the project’s critical outputs is the Making Sense Toolkit, a collection of resources for communities who want to deploy citizen-led campaigns to capture and share open data about the environment[5]. The Toolkit offers detailed case study reports, documentation of technological requirements and a sensor onboarding guide, among other documents, and it describes how citizens can come together in open, collaborative settings to set data collection strategies, learn how to use sensors and coordinate publicity campaigns around their findings.

In Kosovo, Making Sense joined forces with the Peer Educators Network and Science for Change Kosovo Movement, a grassroots collective devoted to breaking the government’s silence on pollution. As one of the organisers describes it, the 30 participants, many of them youth, built Making Sense on radical democratic participatory approaches of non-exclusion and semi-horizontal structures where decision making took place through weekly general assemblies. Participants held a three-day training workshop, and then self-selected into groups in charge of either communications or sensing and devising protocols[6]. Three campaigns followed, from April 2014 till June 2017 (Making Sense, n.d.).

In the first campaign, organisers focused on using sensors in locations scattered around the country to find areas with the highest concentration of pollution; members generated 73 sessions of data from every Kosovo region (Making Sense, n.d.). The second campaign narrowed to one of its most polluted cities, the capital Prishtina, where volunteers concentrated much of their efforts on a primary school that they monitored for two months. The third campaign looked largely at areas that had proximity to coal powered plants, which were some of the most significantly polluted sites in the country.

The first phase used analog diffusion tubes that were not connected to the internet but provided a meaningful baseline for analysis in a lab. Participants had to collect this data, which measured nitrogen oxide levels, and then share it manually (McQuillan, 2015). The sensors were calibrated with equipment provided by the US Embassy, whose instruments were considered more reliable than the Kosovo EPA[7]. After data collection, the first campaign was able to demonstrate that levels of nitrous oxide at hotspots exceeded EU limits by large margins. In the second campaign, Dylos DC 1700 Sensors measured for PM2.5 particles, micro-particles that increase a person’s chance for respiratory diseases and lung cancer. Volunteers found these dangerous micro-particles prevalent on the primary school grounds most days (PEN and Science for Change Movement, 2017).

In terms of data management for these campaigns, participants were focused on aggregating data from the sensors and then interpreting the data for immediate publicity. Participants who collected data could, via their sensors, see the peaks and troughs of their measurements, their walking route and hotspots of poor air quality that showed up in red on mobile app (see footnote 9). After completing the measurements, participants sent their geo-tagged data to a single member who processed it for aggregated longitudinal data collection; our interviewee called this person “the black box of Kosovan data collection”. From there, the participant uploaded the data to GitHub and indexed it on a free, open source platform called Smart Citizen[8].

The Smart Citizen platform, created by the Fab Lab Barcelona, provides a data management tool for citizen sensing projects; it stores sensor data and showcases it through a dashboard and a map of sensing data uploaded by all the platform’s registered users worldwide. On the map, a user can select specific sensors for more detailed analysis and to see how the sensed phenomena changes over time (Making Sense, 2016). Smart Citizen has a distributed version control system, allowing decentralised control and ownership of the data, so the Making Sense member who uploaded the data could access and add to it; the account could
either be shared with other members or members could create their own accounts and upload data. Making Sense therefore did not operate as a networking tool for the Kosovo activists; instead, it put their data in the context of the worldwide community sensing movement.

Once the data were aggregated, another Making Sense team member interpreted the findings by providing a short overview of the values, air pollution levels and possible health impact. These details formed the basis for articles sent to mainstream and social media and drove their campaigns around the issue. Participants designed a media campaign that entailed taking slogans and dummies with masks to the street to open up the conversation around results of data collected. Because of the participants’ foundation of radical democratic, participatory approaches, said our interviewee, they had the competencies to make their collective action highly effective (see footnote 7). One of the primary results was that air quality conditions became publicly visible and tied to local health problems, and this visibility pressured the KEPA to publish its environmental data for public use (Making Sense, 2016). Even more significantly, a citizen’s right to clean air was written into Kosovo’s Constitution thanks in part to the pressures of the campaign.

Problem 3: preserving data for the public domain
The Environmental Data Governance Initiative began in November 2016, soon after Donald Trump was elected to the presidency of the USA. Internationally, scholars shared concerns that Trump’s ideological position on climate change would result in the removal of already-existing public resources on this and related topics. Some of EDGI’s founding members are from Canada, where they remember former Prime Minister Stephen Harper’s administration physically destroying scientific libraries and archives and silencing government climate scientists (Glass, 2016; Kupferman, 2016). EDGI members similarly feared the Trump administration would reduce the capacity for scientists to produce knowledge and leverage science-based calls for reform and regulation (Paris et al., 2017; Rinberg et al., 2018).

EDGI is a primarily volunteer network[9] that investigates potential threats to the scientific research infrastructure necessary to create and enforce environmental and energy policy. It includes 160 active members, with a volunteer community of over 1,100 who identify broadly, from community organising to web development and academics (Knutson et al., 2018). New collaborators must be nominated and voted in by existing members; a consensus must be reached before any decision is made regarding the tasks to be executed. A steering committee governs the activities of the organisation (EDGI, n.d.a).

One essential part of EDGI’s earliest work involved the coordination of DataRescue events around the USA, along with the organisation DataRefuge. DataRescues, which typically took place at university campuses, invited members of the public to gather to flag and copy federal scientific data sets, documents and webpages into a patchwork of repositories (InternetArchive, n.d.). This process involved coordination with the Internet Archive’s (IA) end-of-term (EoT) crawler that routinely archives .gov webpages in periods of executive agency transition (DataRescue, 2017; InternetArchive, n.d.). However, in some cases, webpages, data sets or other elements within the volunteer-flagged websites could not be crawled and archived by the IA’s EoT crawler. In this case, participants built bespoke tools to scrape and archive the uncrawlable data sets (DataRescue, 2017).

To effectively manage the uncrawvable data sets, volunteers designed an open source web application called Archivers.space, a project management tool that uses archival principles to manage the dataset’s full lifecycle (EDGI, n.d.b). The tool tracks the data set from its uploading to an Amazon server through multiple stages of research and vetting by participants. The vetting entails providing checksums to confirm data integrity and creating a .zip file that includes descriptions of the data set’s chain of custody, context, and provenance. A subset of EDGI volunteers focused on archiving governed Archivers.space; other volunteers who work in Archivers.space would get permissions from event organisers to participate[10]. To take part in
the checksums and describing phases, volunteers needed a background in library science or to have participated in DataRescues and other EDGI events.

EDGI is currently part of a collaboration called Data Together (DT), which, along with hosting events and research, is prototyping a node to preserve and make EDGI’s data accessible to broader interested publics (EDGI, n.d.a; Knutson et al., 2018). The collaboration includes Protocol Labs, which is developing a distributed file system, also stylised as an Interplanetary File System, and qri.io, which allows collaborative data sharing on the distributed web. DT is hoping to address the needs of members of the scientific community and grassroots advocates and organisations who may not have the data infrastructure expertise necessary to extract meaningful information from government data portals. The DT collaboration is unique in that it seeks to conceptualise and practice distributed, community-driven data stewardship (https://datatogether.org/). Each organisation participating in the DT partnership grants institutional approval on major decisions, such as how sharing privileges will be determined, and the mode of consensus used for decision making[11]. The DT team, comprised of members from EDGI, Protocol Labs and qri.io, uses EDGI’s model described above for garnering consensus to adjudicate the further construction of the platform, including technical decisions about data infrastructure[12].

EDGI suggests the potential for the open data movement to be interrogated through activist practices, by critiquing the inequitable power relationships between citizens, government and the private sector to access information and use it to shape society. The open data movement, much like the open software and open access movements, advocates for placing research, administrative and civic data into the public domain, often with the stated goal of improving governance (Sánchez and Viejo, 2017; Kitchin, 2014; Obama, 2009). The case of EDGI shows that providing and promoting open data can also be an activist project. EDGI also addresses fundamental issues of ownership and control at the level of infrastructure, which concern any project with long-term preservation goals. EDGI’s DataRescue work not only supplements scientists’ research, but also pays close attention to the politics of technological infrastructures by designing a low-barrier, distributed, participatory platform with traditional archival protocols.

Scale, temporality, governance and values in design
In all three case studies above, data management infrastructure plays a critical role in shaping the tactics and political formations of data activists. Whether the data are being collected, shared or archived, the placement of the data into a publicly accessible repository in all three cases is a crucial part of mobilising collective action, creating accountability, building community and exposing an issue to the public. Yet when comparing these projects, they differ in their temporal dimension, geographic scale, governance structures and sociotechnical politics.

Matters of data management can be affected by a geographic scale. In the first and third cases, contributors to the project are geographically dispersed, so their data management strategies included an accessible interface to elicit and inventory contributions from far-flung volunteers. For Fatal Encounters and EDGI, the web interface both networks the participants and manages the data, with various levels of access privileges to participants depending on different phases of data management in each project. In Kosovo, on the other hand, data contribution was neither web-generated nor web-based; the group did not rely on networked platforms to carry out their work but met to make decisions and share knowledge and outcomes. Aggregating and uploading the data to the Smart Citizen platform was the work of one person; rather than organising and mobilising distributed volunteers, the online platform was put to use for media campaigning in the project’s publicity phase and to connect the project to the wider citizen sensing movement. So a geographical scale in part determines how much data management infrastructures also act as networking platforms, and therefore shape the relations among participants.
Temporality plays another factor in data management practices. Urgent issue-oriented campaigns need data as evidence to make claims to the public and authorities. In many cases, data activist projects do not require a long-term data strategy, especially when the data can be transformed into political communication and immediately put to use. Each of these three projects deploys a different temporal approach towards their data. In Kosovo, the project was more concerned with capturing an immediate snapshot of air quality in the country and its capital and putting these to use in existing environmental campaigns. Currently, the data are static, and there are no signs that the activists plan to contribute beyond the data sets collected during the original three campaigns. Fatal Encounters, on the other hand, does rely on software that can easily facilitate long-term, ongoing data capture. The project uses off-the-shelf, corporately-owned freeware to maintain the data over the long-term, as is common in many volunteer-led projects with no formal institutional or technological support; these tools get the work done of mobilising volunteers and publishing data for others, such as journalists, to access easily. EDGI, in our third example, designed archival principles into its bespoke open source data management software. Such a strategy makes sense for ensuring control over scientific data that must be highly reliable and available to establish long-term environmental trends such as climate change.

The governance structures of the three projects also played a role in data management and access. Burghart centrally controls Fatal Encounters by maintaining the data over time and vetting all contributors, who are largely anonymous to each other. For Making Sense, contributors came together to decide collectively on data collection and publicity strategies, but one person largely took control of the data aggregation and publishing steps. EDGI's processes show how all aspects of data management can be collaborative and federated – including the design of software itself – while still maintaining some access restrictions to maintain data integrity.

Yet, while Fatal Encounters has the most top-down management structure, it is also the easiest for participants to contribute to both in terms of technological know-how and access permissions. To add to Fatal Encounters database, one fills out a Google form and waits for vetting by Burghart. EDGI's Archivers.space, on the other hand, requires participants to learn the system and have some specialised knowledge to take part in certain aspects of the archival process. Making Sense, as well, required training before participants could use the sensors, and the Smart Citizen platform requires an account and understanding of how to sync data to its platform. None of the projects, therefore, were entirely horizontal but had various asymmetries in terms of governance and access depending on the stage of the data handling. Again, data management processes in this way shape, as much as are shaped by, projects' governance and access structures.

Finally, in two of the cases, the data management strategies and software used reflect the political structures and ideologies of the collective action projects themselves. The use of open source software was a deliberate choice for EDGI and Making Sense, groups devoted to openness, semi-horizontal governance and inclusivity. Archivers.space reflects a commitment to collaborative but federated and decentralised contributions that still leave room for various levels of access. To publish their data, Making Sense selected an open source platform that contextualises their political activity in relation to hundreds of other citizen sensing projects around the world. This custom-build software reflects citizens' political choice to support public domain resources and to remain autonomous from corporate data capture, a decision that can be especially important for activists collecting sensitive personal data. That said, open source software can also create greater technical barriers for participants who do not have the skills or luxury time to design or learn custom software for their needs. Fully bespoke software custom-built for a project, such as Archivers.space, can be a difficult bar for most activist projects. Instead, activists can try to seek out not-for-profit data management software alternatives to corporate platforms, such as Smart Citizens, that can be used by many activist projects at once.
“Back Up! Back Up! we want freedom! freedom!”

Data activism makes use of powerful tools for constituents to voice their perspective, whether it be through holding law enforcement accountable for poor and dangerous policing practices, or the empowerment that comes from shared scientific evidence. This paper argues for scholars to give more attention to the data management practices of activists; it provides some heuristics for analysing activists’ data management infrastructures, primarily asking about the ability of participants to take part in aspects of the data management and the politics of the technical platforms used. Through a comparative case study analysis, we show how these infrastructures can relate to a project’s temporal goals, its governance structures among participants, the project’s geographic scale and the need for activists in some cases to consider the political economy of their management tools.

While Black Lives Matter protesters in Ferguson chanted loudly, “Back Up! Back Up! We Want Freedom! Freedom!” at lines of riot police, we can see how this mantra also applies to data activists in the face of enormous power asymmetries in terms of data ownership and control. While data activism may not appear as valiant an act as a street protest, managing and maintaining grassroots data promotes immeasurable public good in the long term.

Notes

1. Data management is an interdisciplinary subject that is also widely treated in literature from data and computer sciences, which focusses mostly on technological dimensions.
2. ICPSR’s repository includes 250,000 files of research in the social and behavioural sciences and 21 specialised collections in in education, aging, criminal justice, substance abuse, terrorism and more. www.icpsr.umich.edu/icpsrweb/content/datamanagement/dmp/elements.html
6. Interview with Professor Mel Woods, conducted 15 August 2018.
7. Interview with Professor Mel Woods, conducted 15 August 2018.
8. The platform was developed in Java and HTML5, and it allows developers to build new features on top of existing applications (Diez and Posada, 2013). Certain digital sensors can send data directly to the Smart Citizen dashboard, but that was not the case here.
9. A handful of EDGI members are employed through grant funding to keep the organisation running (Knutson et al., 2018).
12. From Paris’ participation in conversation with Data Together through the Spring of 2018, including a Data Together Community meeting held 12 March 2018. Stream of the meeting accessible at: www.youtube.com/watch?v=zeY_fYknM8&t=587s&index=14&list=PLtsP3g9LafVuUgCtMYGm9sz5FUWr5bu

References


Further reading


Corresponding author
Britt S. Paris can be contacted at: britt@datasociety.net

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

What a difference do data make?
Ownership and control over publicly accessible platform data

Teresa Scassa
Faculty of Law, University of Ottawa, Ottawa, Canada

Abstract

Purpose – The purpose of this paper is to examine how claims to “ownership” are asserted over publicly accessible platform data and critically assess the nature and scope of rights to reuse these data.

Design/methodology/approach – Using Airbnb as a case study, this paper examines the data ecosystem that arises around publicly accessible platform data. It analyzes current statute and case law in order to understand the state of the law around the scraping of such data.

Findings – This paper demonstrates that there is considerable uncertainty about the practice of data scraping, and that there are risks in allowing the law to evolve in the context of battles between business competitors without a consideration of the broader public interest in data scraping. It argues for a data ecosystem approach that can keep the public dimension issues more squarely within the frame when data scraping is judicially considered.

Practical implications – The nature of some sharing economy platforms requires that a large subset of their data be publicly accessible. These data can be used to understand how platform companies operate, to assess their compliance with laws and regulations and to evaluate their social and economic impacts. They can also be used in different kinds of data analytics. Such data are therefore sought after by civil society organizations, researchers, entrepreneurs and regulators. This paper considers who has a right to control access to and use of these data, and addresses current uncertainties in how the law will apply to scraping activities, and builds an argument for a consideration of the public interest in data scraping.

Originality/value – The issue of ownership/control over publicly accessible information is of growing importance; this paper offers a framework for approaching these legal questions.

Keywords Copyright, Sharing economy, Platform economy, Data ownership, Data scraping

Paper type Research paper

Introduction

Internet platform companies host a significant amount of data on their sites. Some, although not all, of this information is personal information and often much of it is user contributed. While the data – and the ability of the public to access and view them – are an important part of the business model of these platforms, these data are often of significant interest to those beyond the immediate sphere of platform users. In a data-driven economy, publicly accessible data can be an important resource. Because of this, questions arise as to who has the right to control access to and use of such data, and in what ways and circumstances such control can be exercised. The answers to these questions will have important implications for innovators, researchers, civil society and even governments.

This paper considers questions around ownership and control of publicly accessible data, using Airbnb as a case study. Airbnb is a major, global platform that hosts a great quantity and variety of data. The nature of its business requires that these data are made publicly accessible – in order for hosts to share information about their rental units and for potential or actual guests to be able to browse this information, and add to it with comments and reviews. Airbnb is an interesting case study because its operations have had significant impacts on many cities, raising questions about, among other things, the platform’s effects on the cost and availability of long-term accommodation, its impact on incumbent short-term accommodation providers, the incidence of discrimination in Airbnb rentals and pricing and the extent to which the platform is used to support full-scale commercial ventures. The data hosted on the

The author gratefully acknowledges the support of the Social Sciences and Humanities Research Council of Canada. Thanks to Nathan Hoo and Joël Boisvert for their research assistance.
Airbnb site can be scraped and analyzed so as to provide important insights into these issues. In the absence of adequate voluntary data sharing by a company, data scraping remains a primary source of such data. Airbnb platform data are also of interest to a wide range of businesses, many of which are not in direct competition with Airbnb, but which instead offer services – including analytics – related to Airbnb’s activities.

This paper considers the complex “ecosystem” of users of Airbnb platform data in order to identify and assess the nature and extent of public and private interests in using such data. In order to understand the impacts of Airbnb – and in order to build innovative or opportunistic businesses that draw upon Airbnb’s data – it is necessary to be able to access, harvest and manipulate these data. While any company may protect its confidential commercial information from undesired access and reuse, the rights of companies to protect and limit the reuse of publicly accessible data are more tenuous. Any such rights may also be subject to countervailing users’ rights. The legal status of publicly available information is therefore important. In a rapidly evolving data economy, legal uncertainties in relation to ownership of and rights of access to data risk being resolved by litigation between business competitors, which risks overlooking and unduly limiting the strong public interest in access to and use of such data. This paper argues that a data ecosystem approach to publicly accessible platform data is necessary to prevent the normative framework for data scraping from being unduly shaped by the platforms themselves.

**Literature review**

Although a great deal has been written about the sharing economy and its impacts, relatively little scholarly attention has been paid to the massive quantities of data that are amassed by platform companies, and more specifically about issues relating to access to and reuse of these data. This has started to change somewhat, as developments in the artificial intelligence (AI) sector raise questions about access to data to train algorithms (Geiger *et al.*, 2018). The data-sharing practices of social media companies have also come under recent scrutiny with the Cambridge Analytica scandal, with preoccupations in this area relating to the automated extraction and reuse of personal information (Information Commissioner’s Office, 2018). Much less has been written about access to personal and non-personal platform data for other types of research.

Access to data about platform companies’ activities can be difficult to obtain. For example, the impacts of short-term rental platforms on the availability and affordability of long-term accommodation in cities has led to numerous studies and reports, many of which lament the lack of easily accessible data (Jamasi and Hennessy, 2016; Sawatzky, 2015; Vancouver City Council, 2016; Cutler, 2015). As documented by Scassa (2017), a number of cities have resorted to using data scraped either by civil society actors or by consultants. Scraped data have formed the basis for a number of studies and report about short-term rental platform economy impacts (Scassa, 2017; Sawatzky, 2015; Clampet, 2014).

The practice and the legality of data scraping have received relatively little academic attention, although this is beginning to change as such activities become increasingly widespread and more commercially significant (Snell and Care, 2013). Quite apart from the issue of whether scraping infringes copyright by taking a substantial part of an original selection or arrangement of data, legal scholars have considered whether data scraping is a form of trespass to chattels (Din, 2015; Warner, 2002), or whether (in the USA) it violates the *Computer Fraud and Abuse Act* (Din, 2015; Hirschey, 2014).

Legal disputes over data scraping have begun to heat up, although the bulk of this case law involves competing businesses. Some cases involve data scraping by relatively direct competitors (*Century 21 Canada Limited Partnership v. Rogers Communications Inc.*, 2011; *Trader Corporation v. CarGurus, Inc.*, 2017; *Ryanair Ltd v. PR Aviation BV*, 2015), others
involve companies in the same field but operating with a different business model. For example, the news aggregator Meltwater has generated litigation over its scraping of news headlines on both sides of the Atlantic (Newspaper Licensing Agency Ltd and Ors v. Meltwater Holding BV and Ors, 2011; Associated Press v. Meltwater U.S. Holdings, Inc., 2013). In other cases, data scrapers harvest data for new forms of analytics. In the USA, litigation between LinkedIn and a number of companies that actively scrape its data promises to produce interesting case law around the legality and the limits of such practices (Conger, 2016). A very recent US case, Sandvig v. Sessions (2018) challenges the application of the Computer Fraud and Abuse Act to data-scraping activities carried out for research purposes. However, the emerging case law will not provide clear answers to all questions regarding the legitimacy of data scraping as a means of acquiring publicly accessible data. In the first place, some of the decisions turn on the form in which data are presented. For example, if photographs are scraped (Century 21 Canada Limited Partnership v. Rogers Communications Inc., 2011; Trader Corporation v CarGurus, Inc., 2017), or newspaper headlines (Associated Press v. Meltwater U.S. Holdings, Inc., 2013; Newspaper Licensing Agency Ltd and Ors v. Meltwater Holding BV and Ors, 2011), these forms may attract a greater level of copyright protection than would be available for compiled data. Second, most, though not all, data-scraping disputes involve commercial competitors and such disputes are less likely to raise issues of users’ rights or the public interest. This means not only that these issues are rarely explored in the emerging court decisions, but that the decisions themselves may shape the law in ways that develop robust concepts of the rights of data “owners” while doing nothing to consider or articulate the nature and scope of users’ rights. There are a couple of notable exceptions in the USA (Sandvig v. Sessions, 2018; hiQ Labs, Inc. v. LinkedIn Corporation, 2017) but these cases largely address US-specific legislation that, depending on its interpretation, might criminalize data scraping in some circumstances.

The thirst for data in the AI sector has prompted considerable legal interest around the world in creating text and data-mining exceptions to copyright infringement (Geiger et al., 2018). The data-scraping discussion thus now also takes place in the shadow of broader concerns over rights to access and reuse data for AI research and processes. These discussions have also touched on other issues relevant in the data-scraping context, including the impact of terms of service (TOS) that prohibit automated extraction of data, and the use of technological protection measures (TPMs).

Methods
The analysis of data scraping was carried out using a single platform company – Airbnb – as a case study in order to provide a rich context for the assessment of data scraping. The users of Airbnb data are as diverse as the users to which the data are put, which helps ease out the complex competing interests.

The research behind this paper involved a detailed study of Airbnb’s platform, including a web-based review to identify users of Airbnb data, how data are accessed by these users and the uses to which the data are put. Studies, reports and other documents that relied upon scraped Airbnb data were analyzed, and materials regarding difficulties in accessing Airbnb data, and critiques of voluntary releases of data by Airbnb were gathered from a review of print and online sources.

Because data scraping is the primary means by which Airbnb’s platform data are harvested for reuse, the research also involved a scan of the primary (laws, case law) and secondary (scholarly articles and commentary) legal literature regarding data scraping. Legal materials from Canada, the USA and the UK were analyzed to provide the basis for a discussion of the law of data scraping. Since data scraping is also impacted by aspects of private law, the legal documents that structure Airbnb’s operations were reviewed.
These include its TOS, privacy and other policies. Legal claims in these documents, including ownership or control of data, contractual limitations such as prohibited conduct with respect to data and site usage, and privacy commitments were considered, along with their interaction with applicable laws.

Results

Airbnb impacts

According to its website, Airbnb operates in over 191 countries and over 65,000 cities worldwide (Airbnb). It also claims to have more than 3m listings, with over 150m travelers finding accommodation through its platform. Like many platform companies, Airbnb exploits the rhetoric of facilitating small-scale sharing of individuals’ surplus resources. It claims to help ordinary individuals monetize their underutilized living space, whether in the form of a spare room, or their entire unit while on vacation. However, with the rise in the popularity of the site, concerns have grown over the use of the platform by those who make entire units available year-round; as well as hosts with multiple available units. Indeed, a growing concern is that long-term accommodation is being converted by urban entrepreneurs into short-term rental accommodation via Airbnb (Office of the Attorney General of the State of New York, 2014). Such activities have raised serious concerns about the impact of the platform company, particularly in cities where there is a shortage of long-term accommodation as well as problems with affordable housing. In addition, policy makers and civil society groups have argued that Airbnb contributes to gentrification (Cox, 2017; Office of the Attorney General of the State of New York, 2014; Jamasi and Hennessy, 2016); undermines or changes the character of neighborhoods (Scassa, 2017); and creates nuisances (Scassa, 2017). Condominium associations and landlords have also raised concerns over the impact of short-term rentals on the character of their buildings, the over-exploitation of shared spaces, disregard of noise, non-smoking and other policies and security (Scassa, 2017). Incumbent short-term rental industries have also complained that Airbnb hosts are not subject to the same level of regulation and do not pay taxes, thus enabling them to unfairly compete within the market (Reyes, 2015).

Airbnb data

Not all data collected by Airbnb are exposed on its platform, much data – including personal information of its hosts and guests – is kept confidential. Airbnb generates its own confidential analytics based upon its data. Nevertheless, the company makes a range of different data publicly accessible on its platform. In this respect, Airbnb is different from other platform companies such as Uber. In order to meet its goal of connecting hosts with guests, the Airbnb platform must necessarily display information about the nature and size of available units, their price, general location and general availability. The site also contains photographs of units, verbal descriptions of units, their amenities and their location, information about hosts, reviews (which may contain information about guests and what they did during their stay, information about host and guest interactions; information about the unit, about the dates of the stay and about the area in which the unit is located). All of these data come from multiple sources, including hosts (who provide photos, verbal descriptions, availability information, etc.); guests (who provide reviews); and Airbnb (which provides templates for information as well as in some cases photographs). Although the primary purpose of these data is to provide information about specific units that are for rent, taken together and subject to analytics, they can provide rich information about the number of rental units available in particular areas, the availability of those units over time, their price (varying by time of year and over time) and much more. These data can be used in analytics to assist those seeking to enter the market to appropriately price their rental units. This information can also be used to understand
the extent to which units are really just “excess space” or are diverted from the pool of available long-term accommodation. They can provide valuable insight into a range of other issues relating to long- and short-term accommodation, tourism, tax avoidance, zoning and by-law infractions, breaches of leases and other contracts. Public facing Airbnb data have also been used to explore issues of discrimination in the provision of short-term rental accommodation (Wang et al., 2015). The uses of the data are limited only by the creativity of the users.

Airbnb data ecosystem
The “ecosystem” metaphor has become widely used in scientific and technological literature. It builds upon the concept of natural ecosystems as dynamic, evolving contexts in which there are multiple interdependencies (Harrison et al., 2012). Zuiderwijk et al. (2014, p. 20) refer to metaphorical ecosystems as reflecting “the dynamic interaction between different factors in an area.” More simply put, according to Nardi and O’Day (1999, p. 49), an ecosystem is defined as “a system of people, practices, values, and technologies in a particular local environment.” Harrison et al. (2012, p. 906) observe that: “The dynamic of ecosystems is one of flow and movement – people, ideas, activities, and tools in motion as the ecosystem evolves continuously in the form of components that ‘adjust and are adjusted in relation to each other, always attempting and never quite achieving a perfect fit.’”

The ecosystem metaphor for publicly accessible Airbnb data provides a way to understand the context that is framed in terms of interdependencies and interrelationships rather than one in which there is merely a sequence of one-on-one relationships between a company and the various legitimate and possibly illegitimate users of its data. Airbnb data are contributed and created by different actors; they are used by different actors for different purposes; and they are capable of describing or of contributing to descriptions of phenomena and experiences within real communities. This concept of Airbnb data as part of an ecosystem therefore shifts the paradigm from one of corporate ownership/control of data in the context of a company’s distinct relationships with different users to one in which there are a network of different claims to rights and or interests in the data.

A thriving data ecosystem has arisen around Airbnb’s publicly accessible data. A variety of users may access and use the data in different ways and using different means. One of these means is that for which the site was created – prospective guests may browse the site in order to find information about short-term accommodation in the cities they plan to visit. Hosts may also browse the site to compare their unit with others in the same area, and in order to gain information about how they might price their unit or better present it to the public. These uses are explicitly permitted in the TOS of the site.

Civil society organizations also make use of Airbnb data. This is often done to raise awareness of issues regarding the availability and affordability of long-term accommodation. In the case of Airbnb, there are some high-profile examples. Activist Tom Slee, for example, has scraped Airbnb data and hosts a website that makes these data as well as analysis and studies based on the data publicly available (www.tomslee.net). Slee has also, in the past, made the code he uses for scraping data publicly available. Another high-profile Airbnb activist, Murray Cox, operates the website InsideAirbnb.com. Through his site he provides commentary and analysis of scraped Airbnb data.

Journalists and researchers are also users of Airbnb platform data. Typically this is scraped data. The journalists or researchers may scrape the data themselves (e.g. Sawatzky, 2016; Wang et al., 2015) or they may use data scraped by others (such as Slee or Cox, above) (e.g. Majoribanks, 2016). Not all Airbnb data that are used in research are scraped. For example, Edelman et al. (2017) who studied discrimination over the Airbnb platform gathered their data through contact with hosts over the platform.
Similar to researchers, journalists pursuing Airbnb-related stories may scrape their own data, or they may rely upon data already scraped by others (e.g. Clampet, 2014; Said, 2015).

Airbnb's publicly accessible data ecosystem also includes a range of different opportunistic businesses. These are businesses that have sprung up around Airbnb and that depend – to greater or lesser extents – on the continued operation of Airbnb. They also depend on ongoing access to Airbnb data. An example is the company Airdna. Airdna (airdna.co) offers its clients a variety of data analytics services. These include "market reports and other data products that feature occupancy rates, seasonal demand, and revenue generated by short-term rentals" (airdna.co). According to Airdna.co, its reports and analytics “are based on Airbnb data gathered from information publicly available on the Airbnb website” (www.airdna.co/methodology). Airdna is also linked to another business, Rentingyourplace.com, which offers consulting services to prospective Airbnb hosts. Airdna is not the only analytics company to mine Airbnb data. Other companies include, but are not limited to, Beyond Pricing (beyondpricing.com), SmartHost (smarthost.co.uk), Everbooked (www.everbooked.com) and PriceLabs (www.pricelabs.co).

Not all businesses that rely on Airbnb data offer analytics for those who seek to participate in the short-term rental market. Because of the importance of Airbnb data to urban planners, researchers and governments (among others), consulting companies may scrape Airbnb data in order to provide a broader range of consulting services. For example, Host Compliance LLC (2016) produced a report based on scraped data for the City of Vancouver. Airdna, mentioned above, also provides broader consulting services based on Airbnb publicly accessible data (Stulberg, 2016).

Another category of businesses makes use of publicly available Airbnb data in order to provide a different kind of service. There are a growing number of detective agencies – either general practices or ones specifically focused on short-term rental detection – that use data on the Airbnb platform in order to determine whether units in their clients' buildings are being illegally rented through the platform. While some agencies may use manual techniques (personally searching through listings) others are using automated search tools to crawl through short-term rental listings (www.buildingsnitch.com).

As can be seen from the above, many opportunistic businesses are not competitors of Airbnb in a strict sense, although in some cases they may compete indirectly or in sub-markets for Airbnb data. In the case of Airbnb, a company might scrape Airbnb data in order to combine it with other available data to provide information to those considering offering a unit for rent on a platform such as Airbnb. This information might include recommendations as to price point, peak rental periods and so on. This does not necessarily compete with Airbnb – in fact, it might complement its business by making it easier for people to list properties on the platform. However, should Airbnb choose to provide similar analytics or to sell access to its data for these purposes, then the scraping activities arguably undermine these activities. Whether this is characterized as fair or as unfair competition may turn on whether Airbnb is seen as entitled to control its public facing data as an intellectual property asset. Competition may be difficult to define or identify in a rapidly evolving context in which new applications are constantly being discovered for data, and in which the platform company's control over its publicly accessible data would give it the ability to control the commercial exploitation of these applications. Within this data ecosystem, therefore, there is some uncertainty as to the boundaries of legitimate and illegitimate conduct. These in turn are tied to notions of what rights exist in publicly accessible platform data – including rights to control and exclude and rights to access and use.

The boundaries between legitimate and unfair competition are in part at the root of the current litigation between LinkedIn and the opportunistic companies that scrape its data; these companies have found markets for data and/or analytics based on LinkedIn data and
LinkedIn objects to their commercial exploitation of these markets (Conger, 2016). While not competing directly with LinkedIn’s primary business (hosting a business networking site), these other activities arguably exploit for profit the data LinkedIn has collected. If LinkedIn has rights to control its publicly accessible data, then this exploitation by others of the data is a breach of those rights. Yet these activities might just as easily be characterized as innovation using publicly accessible data.

Discussion
Platform companies have a number of legal tools that they can use in efforts to assert control over the publicly accessible data hosted on their sites. These tools can be divided into three categories. The first category involves legal claims based upon “ownership” rights – whether this involves ownership of intellectual or personal property. The second involves limitations on access that are ultimately supported by law. These limitations may involve contractual terms or technological barriers that limit access. The third involves privacy rights.

Ownership
Ownership claims asserted by platform companies are of two kinds: intellectual property rights and rights in chattels. Intellectual property rights associated with data involve copyright, and, in the EU, may also involve database rights. Chattel (personal property) rights are asserted in relation to the physical infrastructure that hosts the data.

Intellectual property rights. A platform company’s rights in its publicly accessible data can be complex, particularly where a significant quantity of that data is user contributed. This complexity is reflected in the Airbnb TOS. This document distinguishes between content contributed by its members (“Member Content”) and content that Airbnb itself makes available over the site (“Airbnb Content”). A third category of content – “Collective Content” – reflects the combination of both Member and Airbnb content. Airbnb asserts copyright in its own content, but does not claim copyright in Member Content, asserting only a perpetual, non-exclusive worldwide license to use and disseminate it. Nevertheless, as the host and compiler of the “Collective Content,” Airbnb may have a copyright in the overall compilation on its site, as discussed below. It is certainly possible for a party to have a copyright in a compilation even if different parts of the overall compilation are contributed by others who retain copyright in their respective contributions. Article 5.2 of the Airbnb TOS states that: “The Airbnb Platform, Airbnb Content, and Member Content may in its entirety or in part be protected by copyright, trademark, and/or other laws of the United States and other countries.” Article 5.3 prohibits certain uses of the Collective Content that are consistent with claims of copyright in such content, and Article 5.4 provides a limited license to “access and view” the Collective Content. These provisions are consistent with a claim to copyright in the compilation that is the Collective Content.

Copyright claims depend upon the existence of a “work” in which copyright subsists. Protected works must fall into one of the categories of literary, artistic, dramatic or musical works. They must also be “original.” Some web-based data are represented in forms or ways that independently constitute works. For example, a photograph is an artistic work; photographs are also a way in which data can be represented. Text is a literary work, but can also be a representation of data. In some cases, data scraping from websites has involved the scraping of photographs (Trader Corporation v. CarGurus, Inc., 2017; Century 21 Canada Limited Partnership v. Rogers Communications Inc., 2011) or text (Associated Press v. Meltwater U.S. Holdings, Inc., 2013; Century 21 Canada Limited Partnership v. Rogers Communications Inc., 2011). In such cases, it can be argued that the scrapers have violated copyright in those works by reproducing them without permission.
In other cases, however, scrapers have merely extracted data (Ryanair Ltd v. PR Aviation BV, 2015). In general terms, copyright law does not protect “facts,” which are considered to be in the public domain – free for anyone to use (Tamaroff, 2011). However, a compilation consisting of an original selection or arrangement of facts may be protected (Newell, 2011; Hugenholtz, 2017). Some authors explore what it takes to have an original selection or arrangement of facts (Newell, 2011; Leaffer, 2007), with most concluding that the threshold for protection of such a compilation is quite low. Nevertheless, while compilations of fact may be relatively easily protected as “works” the extent of protection is considered “thin,” as infringement requires a substantial taking of either the original selection or arrangement. The taking of public domain facts themselves is not, on its own, infringement. Thus, any claim to copyright infringement with respect to the data hosted on a platform site will depend upon whether the site hosts a compilation of data that are original by virtue of their selection or arrangement, and whether the scraper has extracted a substantial part of that original selection or arrangement. Arguably, a platform company, by deciding what information users must provide and by creating the formats by which it is arranged online, has produced an original selection and arrangement of data. However, to the extent that all short-term rental platforms require the same categories of information about rental units and their availability, a court might consider that the selection of data is merely routine and not original. And, while the arrangement of these data may vary from platform to platform, providing a sufficient degree of originality, a data scraper who extracts the data from this context and stores it according to his or her own protocols may not be taking a substantial part of the platform’s original arrangement. Thus, copyright arguments against data scraping (as opposed to the scraping of text or of photographs) are complex and contingent.

Copyright protection for compilations of facts is roughly equivalent in the EU. However, in 1996 the EU also passed a Database Directive which established a sui generis regime for the protection of databases. This directive creates a right in the “maker” of a database who has made a substantial investment in the creation of the database (Tamaroff, 2011). The database right makes it an infringement to extract or reuse some or all of the contents of the database. While this seems to provide more extensive protection than copyright, recent court cases in Europe have considerably restricted the application of the Directive, and some now question its usefulness in protecting many compilations of data (Hugenholtz, 2017; Newell, 2011). The significance of the database right in protecting against data scraping is therefore in doubt. This may explain why debate began to stir within the EU over whether a new “data ownership” right should be created (Hugenholtz, 2017). Other data ownership/access issues that are emerging in the Big Data context include whether text and data-mining activities infringe copyright in the works that are used (which can include compilations of data) or whether and in what circumstances these activities might constitute fair dealing/fair use (Geiger et al., 2018; Sobel, 2017). These disputes highlight the significance of public interest exceptions to copyright principles and the challenges of delineating the boundaries of ownership rights.

Rights to use/access. Just as there are some legal arguments that can be asserted by platform companies to protect their publicly accessible data from data scraping, legal arguments are also available to those who seek to scrape and reuse such data.

Copyright law creates a balance between the rights of owners of copyright and those of users; this balance serves the greater public interest in the broad dissemination of works and in the free and open dissemination of ideas. If it can be successfully argued that there is copyright in the composition of data hosted on a platform website, a scraper might be able to argue that their actions in taking a substantial part of the selection or arrangement of the data constitute fair use (in the USA) or fair dealing. Fair use/fair dealing rights particularly
(though not exclusively) favor non-commercial uses and ones that support activities protected by freedom of expression values such as research, criticism or comment. In the USA, the creation of new or “transformative” works can also be fair use.

The strength and scope of such a defense may vary from one jurisdiction to another. Fair use in the USA, for example, is a more expansive defense than fair dealing under Canadian law. The purpose for which the data are scraped may have some bearing on the success of such a defense – scraping for research purposes may be more likely to be considered fair than scraping to establish a business – particularly one that is in full or partial competition with the target of the scraping. Similarly, non-commercial uses may be considered fairer than commercial ones – although not all commercial uses will be unfair.

The debates over whether text and data-mining activities infringe copyright law provide an interesting comparison with the issues raised by data scraping. The thirst for data to feed data analytics and to develop machine learning has led to a need in some sectors to absorb data from copyright-protected sources. To do so, entire texts must be scanned or entire compilations of data absorbed. This wholesale copying would infringe the owners’ copyrights unless it falls within an exception to infringement. In the USA, the flexible fair use exception is considered by some to justify text and data mining (e.g. Cox, 2015). In the EU, by contrast, a specific exception is thought necessary, and the scope and wording of such an exception is currently a matter of debate (Geiger et al., 2018). The challenge is to properly assess the different interests at play – including the public interest – and to strike the appropriate balance. This is so whether a solution is achieved by interpreting existing laws or making new ones. Similar challenges exist with the scraping of publicly accessible data, although these are made more complex by the contingent and uncertain nature of any copyright in a compilation of data from the outset.

Several factors may influence fair dealing analyses when it comes to data-scraping activities. For example, if a website’s terms of use prohibit data scraping, the fact that a user must breach contractual obligations in order to harvest the data might mitigate against a finding that this is fair use or fair dealing. Some scholars have argued that rights holders should not be allowed to alter fair dealing/fair use exceptions through contracts of adhesion (Elmahjub and Suzor, 2017; DiValentino, 2014; Elkin-Koren, 1997) but this is an area where the case law is still unsettled. The presence of robots.txt protocols to signal that scraping is not permitted might also be considered relevant in a fair use/fair dealing analysis. The automated, repeated and large-scale nature of some scraping practices might also be considered presumptively unfair.

In its litigation with LinkedIn, data scraper hiQ asserted freedom of speech rights under California law in support of an argument that it was entitled to collect and use publicly available information. The court was not persuaded by this argument (hiQ Labs, Inc. v. LinkedIn Corporation, 2017). Furthermore, in most instances, freedom of speech rights are constitutional guarantees and relate to obligations owed by the government; they are not applicable between private parties. Nevertheless, the argument touches on the tension between ownership rights and the freedom of ideas, knowledge and information. Where data are publicly accessible, what should be the boundaries of private rights to control and limit the reuse of that information, and what role should the law play in reinforcing those boundaries?

Airbnb appears to have been relatively restrained when it comes to addressing the scraping of its platform data. There are currently no records of lawsuits initiated against Airbnb data scrapers. In cases where Airbnb data have been scraped in order to produce reports or studies on the impact of the platform in cities, the company has asserted that scraped data are unreliable and unfit for purpose (Hiltzik, 2015; Sawatzky, 2015).

Although the scope and subsistence of copyright in any compilation of data is uncertain and contingent, the availability of fair dealing/fair use defenses is also uncertain. Legal uncertainty
of this kind may be enough on its own to deter those with limited resources from engaging in contested actions. Researchers, civil society organizations – others without deep pockets – are generally not able to contest cease-and-desist letters. This may explain why the data-scraping cases that have reached the courts have almost exclusively involved corporations. A rare exception, *Sandvig v. Sessions* (2018), involved claims by researchers; this litigation was supported by the American Civil Liberties Union.

**Chattel rights.** In some data-scraping cases in the USA, plaintiffs have argued that the data scraper is engaging in a trespass to chattels. Trespass to chattels is a tort action that is available when personal property is interfered with, either by intentionally dispossessing another of a chattel or by using or interfering with a chattel that is in someone else’s possession (Warner, 2002). The “chattels” in a data-scraping case are the servers on which the data are stored; the interference is remote and electronic. Essentially, the argument is that the data scraper, by using “crawlers” and “robots” to scrape data from the server, has substantially interfered with the chattel, and is therefore liable. These arguments have had mixed success, and are more likely to prevail where the scraping activities are so frequent or so extensive that they overburden and impede a server’s ability to function properly. Thus, where data-scraping activities cause a server to crash or even to respond more slowly to legitimate requests for data, it is more likely that the plaintiff will succeed with a tort claim in trespass to chattels. Nevertheless, even scraping activities that have little or no discernable impact on the host server may be actionable as trespass to chattels (Din, 2015).

**Contractual or technological restrictions**

Platform companies regularly use TOS to set the rules of conduct for their sites. These are a form of contract that bind the user of the site either through their express consent (clicking an icon that indicates that they accept the terms of use) or through their conduct (continuing to browse past the home page of the website) (Scassa and Deturbide, 2012). TOS frequently address rules regarding the use of content on the site. For example, Airbnb’s TOS provide users with only a limited right to access and view the site’s content for personal and non-commercial purposes (TOS, Art. 4). Also prohibited is the circumvention of any TPMs (TOS, Art. 14.1). Copying or adapting content is not permitted (TOS, Art. 5.3). Data scraping or any other form of automated data extraction is also specifically prohibited (TOS, Art. 14.1).

Because TOS are contracts, they have an important limitation. Generally, contracts only bind the parties to the agreement. Thus, the fact that data have been scraped in breach of the contract between the platform and the data scraper does not affect a third party who uses the scraped data. However, where there are also copyright claims in the scraped content, a third party may be restricted in their use of the content by these property-based claims. And, as was discussed above in the section on rights to use, the existence of a contractual obligation to not scrape data might be a factor in assessing whether data scraping that breaches intellectual property rights is fair use/fair dealing. The Court of Justice of the European Union has recently held that contractual TOS that prohibit scraping may provide a basis for finding liability for breach of contract (*Ryanair Ltd v. PR Aviation BV*, 2015), and a similar result was reached in a Canadian case (*Century 21 Canada Limited Partnership v. Rogers Communications Inc.*, 2011).

Where technological barriers are in place, the circumvention of these barriers may lead to different legal consequences. Anti-circumvention provisions, now found in most copyright statutes, provide additional recourse to a plaintiff where a defendant circumvents TPMs to gain access to copyright-protected content (Craig, 2010). A TPM may be as simple as a username and password for a site (Puerta, 2016). In the case of most publicly accessible data, such technological restrictions will not exist. There has been some discussion regarding
whether ignoring a robots.txt protocol – designed to communicate to web crawlers and robots that they are not permitted on the site – constitutes circumvention (Lundblad, 2007), although this would seem to be a relatively weak argument (Jasiewicz, 2012).

In the USA, the Computer Fraud and Abuse Act has been invoked in a number of data-scraping cases. This statute makes it a criminal offense to make unauthorized use of computers. While the statute was originally intended to provide recourse against hackers, it has been invoked in cases involving data scrapers. There has been some debate as to whether data scraping is actually captured by this statute, which seems more tailored to address breaches of security measures in order to obtain confidential data rather than to scraping publicly accessible data from websites (Din, 2015; Hirschey, 2014). Some data-scraping prosecutions under the CFAA have succeeded, while others have failed, creating considerable uncertainty (Din, 2015). Din (2015) argues that the CFAA should be confined to those data-scraping cases which involve the circumvention of some kind of technological barrier such as password protection or encryption, but should not apply to the scraping of publicly accessible information. This view seems to be reflected in the recent decision of the US District Court for the District of Columbia in Sandvig v. Sessions (2018). The Court found that the plaintiffs had standing to sue and to argue that the application of the CFAA to data scraping for research purposes would violate the Free Speech and the Free Press clauses of the US Constitution.

It is interesting to note that in the case of publicly accessible information, many of the platform companies’ recourses, described above, have weaknesses, and these are often significant. Copyright claims in compilations of data may be of questionable scope or strength, and trespass to chattels claims will be weak where there is no particular impact on the server. Anti-circumvention claims will depend upon the existence of effective TPMs as well as copyright-protected content. The CFAA, applicable only in the USA in any event, is also controversial in its application in these contexts. Nevertheless, the fact that such recourses exist can be a strong deterrent, particularly where there is disparity in economic power between the host platform and the data scraper. In such contexts, the recipient of a cease-and-desist letter may have little option but to cease-and-desist since any attempt to resist the asserted claims will require considerable financial resources.

As a result, the legal uncertainty as to the status of publicly accessible data and the scope of users’ rights could significantly inhibit the actions of many users in the face of even the slightest pushback by the platform company. And, as noted earlier, if under-resourced users are unable to litigate in support of these interests, any case law in this area will continue to evolve between commercial actors without adequate attention to users’ rights.

Privacy

Much publicly accessible platform data are also personal information. On a platform such as Airbnb, some user-contributed data may be personal information. Certainly some personal information about hosts is visible on the site, and guests may share personal information in the form of reviews of places where they have stayed. Although not all such information is accompanied by the full name of an individual, all that is required for data protection laws to apply is that individuals be identifiable. The scraping of such data raises important and challenging privacy issues. In some cases, publicly accessible platform data might be scraped specifically for commercial purposes relating to profiling and targeting of individuals (Canales, 2018). Thus, to the extent that publicly accessible platform data include personal information, data protection laws may impose additional restrictions on the collection, use and disclosure of these data.

Different jurisdictions take different approaches to personal information that is made publicly available on websites. In the USA, such data are generally considered fair game, since they have been made public by the data subject and therefore do not attract a
reasonable expectation of privacy, although some have challenged this view (Scott, 2017). The Airbnb Privacy Policy makes it clear that content users contribute to public portions of the site is “visible to the general public” (Art. 3.3). Nevertheless, although the information may be visible to the general public, Airbnb’s TOS prohibit the downloading, scraping or other extraction of data from its site. In theory, therefore, although users agree to share data publicly for the purposes of facilitating the rental of accommodations, they do not consent to this information being downloaded or scraped and used for other purposes. One question is therefore whether a platform could assert the privacy rights of its users as a basis for legal action against data scrapers. This argument was raised in the litigation between hiQ and LinkedIn. LinkedIn – a site that also makes a great deal of user personal information available for public viewing – asserted its privacy commitments to its users as a basis for attacking hiQ’s scraping of its website contents. In deciding a preliminary proceeding brought by hiQ, a California court expressed doubt about the extent of LinkedIn users’ expectation of privacy in the publicly accessible content, and also noted that the platform’s own actions with respect to its users’ privacy did not appear to have been particularly “zealous” (hiQ Labs, Inc. v. LinkedIn Corporation, 2017). Although it is not clear that the same approach would be taken in jurisdictions with different data protection laws, the court’s approach highlights the difficulties with raising privacy issues with respect to personal information available over a publicly accessible platform.

In Canada, private sector data protection laws would apply to the collection of personal information by a company for commercial purposes, even if that information were publicly available platform data. However, with an eye to impending reforms of the federal statute, there has been some discussion of whether such data should be excluded from consent requirements (see, e.g. Canada, Standing Committee on Access to Information, Privacy and Ethics, 2018). In the EU, publicly accessible platform data would be subject to the General Data Protection Regulation, although the public nature of user-contributed personal information might have an impact on the degree of protection available.

Conclusion
As the Airbnb example demonstrates, a diverse range of users (including researchers, journalists, competing and non-competing businesses) make use of publicly accessible platform data for multiple purposes, many of which serve a broader public interest. These uses are subject to challenge by the platform companies that asserting legal rights of ownership and control. The existing statute and case law that buttress claims of ownership/control may also provide a framework of sorts for user rights, yet this framework is not well adapted to our evolving data society generally or to platform data ecosystems in particular. The economic and power imbalances that always impact the litigation process can be exacerbated where existing laws are interpreted and applied to rapidly evolving contexts. There is a considerable risk that such power imbalances can mean that user perspectives and the public interest will not be well represented in the evolving litigation, if they are represented at all. Thus, the broader concern is how to ensure meaningful access to online data in the public interest when it is in private sector hands.

Attempts to control publicly accessible platform data must be seen in the context of the complex ecosystems that can arise around them, as illustrated by the diverse user-base for Airbnb data. An ecosystem approach is particularly useful to address the reality that, for the time being, important issues around the legitimacy of data-scraping activities are likely to be decided by litigation between commercial competitors. The high cost of litigation means that non-commercial users such as researchers and non-profit organizations, as well as small start-up companies, are unlikely to pursue issues in court. An ecosystem approach keeps the diversity of users and uses of publicly accessible
data at the forefront and can help shape more nuanced approaches to the issues. This is particularly important in a novel and rapidly evolving data context.

Different legislative solutions are available. One might be to provide clarification of the scope of protection available to compilations of data, including publicly accessible platform data. Data scraping could be addressed in a new copyright exception similar to what is being considered in the EU for text and data-mining activities. However, there are risks in taking such an approach since new exceptions have the potential of limiting reuse in the public interest simply by casting their scope too narrowly. In a country such as the USA, where fair use is a broad and flexible exception, a new exception might be less desirable than in a country such as Canada, where fair dealing is limited to specific contexts and where the public interest has often fared poorly in the hands of lower courts. Regardless, any new legislative measures must take into account the complex ecosystems that emerge around publicly accessible data, including the broad range of potential users and uses of the data. Legislative amendments to prevent bulk contracting out of fair use/fair dealing rights could also be important in this context, particularly since scraping may be prohibited outright by TOS, as is the case with Airbnb. Furthermore, TPMs in copyright law should not be interpreted so broadly as to encompass tools such as the robots.txt protocol where data are otherwise publicly available. Laws such as the CFAA in the USA should be interpreted narrowly so as to not capture scraping of publicly accessible data.

It is worth noting that the combination of barriers erected to data scrapers and the laws that reinforce them can raise ethical issues. The issue of the ethics of data scraping has already arisen in some contexts such as journalism (Shiab, 2015). It has also arisen in relation to research ethics (Fiesler, 2017; Bruckman, 2016), although some research ethics concerns have focused on the privacy implications of the use of such data (Zimmer, 2010), and not on the ethical implications of researchers breaching contractual terms of use in order to access data, or even engaging in activities that might be categorized as tortious (trespass to chattels). The evolution of the law in this area could have a significant impact on how ethical issues are addressed, and this, in turn, could lead to further restrictions on the ability of institutional researchers to make use of publicly accessible data. Even the legal uncertainties on their own can be stifling, particularly as threats of legal action combined with disparity in economic power can suppress uses/activity unless there are clear rights to access or use.

There is no doubt that these legal uncertainties will need to be resolved. This can be done through clear public policy direction from governments. The discussions in the EU over the creation of a new text and data-mining exception show that concrete action is possible to address the impact of new technologies on the copyright balance. However, such action tends to be driven by commercial interests. User interests rarely prompt swift legislative responses. Failing concrete action, the law will evolve on an incremental basis, driven by the litigation strategies of major corporate players. Within this context, an ecosystem approach to publicly accessible data becomes essential to set the context in which competing claims should be assessed. The ecosystem approach has the advantage of broadening the analysis beyond the specific claims of parties to litigation and considering instead at the diverse ways in which publicly accessible data are used and the broader public interests that may be served by such uses.

References


Further reading


About the author
Dr Teresa Scassa is Canada Research Chair in Information Law and Policy at the University of Ottawa. She is a member of the GEOTHINK research partnership, and has written widely in the areas of intellectual property law, law and technology and privacy. Dr Teresa Scassa is also Senior Fellow with CIGI’s International Law Research Program. She is a founding member of the University of Ottawa’s Centre for Law, Technology and Society, is cross-appointed to the School of Information Studies at the University of Ottawa and is a member of the Geomatics and Cartographic Research Centre at Carleton University. Dr Teresa Scassa can be contacted at: tscassa@uottawa.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@emeraldsight.com
Open government for all?
Co-creating digital public services
for older adults through data walks

Juliane Jarke
Centre for Media, Communication and Information Research (ZeMKI),
Institute for Information Management Bremen (ifib),
University of Bremen, Bremen, Germany

Abstract

Purpose – The purpose of this paper is to review interventions/methods for engaging older adults in meaningful digital public service design by enabling them to engage critically and productively with open data and civic tech.

Design/methodology/approach – The paper evaluates data walks as a method for engaging non-tech-savvy citizens in co-design work. These were evaluated along a framework considering how such interventions allow for sharing control (e.g. over design decisions), sharing expertise and enabling change.

Findings – Within a co-creation project, different types of data walks may be conducted, including ideation walks, data co-creation walks or user test walks. These complement each other with respect to how they facilitate the sharing of control and expertise, and enable change for a variety of older citizens.

Practical implications – Data walks are a method with a low-threshold, potentially enabling a variety of citizens to engage in co-design activities relating to open government and civic tech.

Social implications – Such methods address the digital divide and further social participation of non-tech-savvy citizens. They value the resources and expertise of older adults as co-designers and partners, and counter stereotypical ideas about age and ageing.

Originality/value – This pilot study demonstrates how data walks can be incorporated into larger co-creation projects.

Keywords Co-production, Co-creation, Co-design, Open data, Open government, Data walks

Paper type Research paper

1. Introduction

Open government promotes the idea of citizen collaboration and participation in the planning, design and delivery of public services. The approach has been accelerated through the Open Government Partnership, an association of more than 90 national and regional governments that have committed themselves to become more open and to develop a biannual National Action Plans in cooperation with civil society organisations. The idea of using Open Government data for new public services is simple: governments provide their data for free, online and under open licences; and civil society actors or private companies may re-use the data and develop services according to their needs or expected demand. In some cases, these co-created services are then integrated into e-government service portals. Thus, the vision is that governments can offer user-centred services without additional costs; citizens receive better services via successful and beneficial public engagement and participation (Janssen et al., 2012, p. 261).

With signing the Open Government Partnership, governments commit themselves to cooperate with Civil Society. The civil society constituency working with Open Government data mainly includes civic tech activists (also called civic hackers), who are “deploying information technology tools to enrich civic life, or to solve particular problems of a civic nature”, as Hogge (2010, p. 10) noted in a study commissioned by the Open Society Foundation. So far, the field of civic open data use (civic technology) is dominated by younger and tech-savvy “civic hackers” that develop services for their communities and cities (Gooch et al., 2018; Lee et al., 2015).

Older citizens – if at all – are often only marginally involved in such kinds of civic technology engagement. They very rarely constitute the focal user group of civic apps.
Considering the ageing population and the specific needs of older adults for usable and accessible public services, there is an articulated need to bring together city administrations as data owners, technology developers and older citizens as knowledgeable individuals and prospective users in order to co-create relevant and meaningful public services based on open data. However, most research and innovation in this area so far focusses on the use and re-use of existing open data sets, assuming that the data are easily available. Our research shows that the pledge to citizen-centricity requires additional engagement in acquiring and/or producing data, which are considered relevant by citizens. This requires new ways of engaging citizens, in particular those not familiar with technology design and use.

This paper is based on our own action research in co-creating digital public services with older adults. We report on a pilot study conducted between April and December 2017 in Bremen, Germany as part of a larger, EU-funded research and innovation project. This paper reviews interventions for engaging older adults in meaningful open service design by enabling them to engage critically and productively with open data. We argue that in order to enable older adults to become co-creators, we need to reconfigure and develop new and creative ways for engagement. Taking a situated, practice-based approach as a starting point for technology design, these methods need to relate to the everyday of participants and establish them as experts. We present and discuss the idea of walking workshops as a way to co-create digital public services, which are relevant and meaningful in the everyday life of older adults (for other methods see e.g. Jarke and Gerhard, 2018). However, such methods come with their own challenges, e.g. concerning the sustainability and maintenance of these data.

In the following sections, we will first outline why it is important to consider new ways of engaging citizens when pursuing open government. We present co-creation as a way to engage different groups of citizens and discuss different roles that citizens may assume in such participatory approaches, before introducing walking workshops as an experimental method from the field of critical data studies, which allows for creative ways of engaging with data. We analyse our approach to using walking workshops as a method of co-design with respect to its inclusiveness and the extent to which it allowed us to consider the needs and interests of participants. We conclude by arguing that walking workshops are a promising method for engaging older adults in co-design activities.

2. Related work: co-creating digital public services
Co-creating digital public services for and with older adults
Interactions between public authorities and citizens are increasingly mediated by digital technologies as more and more public services are provided via digital channels. However, in many cases, these services are not used widely and, in particular, older citizens are excluded above average, as digital services do not meet their needs and expectations. Over the last decade, the idea of open government (European Commission, 2014; House – Oversight and Government Reform, 2007; Office of the President, 2009; Presidential Directives EO 13392, 2005) has attracted attention, encouraging participation and collaboration between governments and citizens to plan, design and provide (digital) public services. One way to perform this collaboration is through the civic use of Open Government data. Sieber and Johnson (2015) identified four different approaches in which governments and citizens can interact. These approaches span from the mere provision of data by government and data use through citizens to the active co-creation of data and services through both sides:

1. Data publishing: governments provide data as open data via local or national portals. According to the requirements of the Open Knowledge Foundation, open data should be freely available to everyone to use, re-usable and re-publishable as users wish, and absent mechanisms of control such as restrictive licences.
(2) Code exchange: government explicitly encourages the development of saleable or internally useful products based on its provision of open data as mentioned in the introduction. The provision of data is accompanied by promotional or other forms of supportive activity and is often framed in the context of an “app contest”, i.e. apps developed by a developer community, including private business and civil society. It is a kind of outsourcing app development by government.

(3) Civic issue tracker: in this model, the direction of interaction is reversed. Government invites citizens to report problems like potholes or noise complaints or to give feedback on published data and documents. This model may be applied independently from the two previous models, but can also be combined, when citizens are invited to act as “sensors of their environments” and report data on phenomena they are physically close to in a crowdsourcing approach.

(4) Participatory open data: here open data are reciprocal. Data provision from authoritative sources may be followed by a request for additional data and be amended by citizen-generated data that can support service delivery and open a new channel for discussions about policy. This can take place in a co-management framework and includes the ongoing co-creation of raw data between both governments and governed and the co-production of services (Sieber and Johnson, 2015).

Sieber and Johnson see governments “at a crossroad” taking a choice between these models, as they are driven by different motivations: The first two models are motivated by the call for transparency based on freedom of information requirements and/or providing resources for economic development. The third model is motivated by a concern for more responsive relation of government to its citizens, while the fourth model demonstrates a fundamental change of the roles of government and calls for a degree of flexibility, which is hardly found. However, the authors promote the “Participatory Open Data Model” because the first two models pose the risk that governments “outsource themselves”. If, for example, Google collects all public transport data and offers transport information, people may start asking why they pay taxes if others provide public services for free. In the authors’ view, the forth model is a necessary reaction to ongoing changes in the digital world and in line with the principles of the Open Government Partnership.

The idea that people outside an organisation are involved in the development of information services, is prominent in the context of civic tech, where so-called civic hackers use Open Government data to design civic apps which offer and, at times, substitute for public services (Schrock, 2016). In principal, civic tech may involve anybody “who is willing to collaborate with others to create, build, and invent open source solutions using publicly released data, code and technology to solve challenges” relevant to their neighbourhoods, cities or states. Hence, it aims to engage citizens (including those with non-technical backgrounds) in practices relating to different types of open data use such as the requesting, digesting, contributing, modelling and contesting of open data (Schrock, 2016). However, civic tech apps are mainly developed in app competitions and hackathons (often run by public administrations) or through continuous civic tech work such as CodeForAmerica. Software development in such settings is rarely participatory and the resulting apps do not necessarily relate to the needs of other citizens (Lee et al., 2015).

Often civic tech developers anticipate the needs and wants of citizens based on their own experiences with lack or insufficient knowledge about other prospective user groups. However, in order to create value that benefits administrations as well as citizens, it is crucial to engage citizens who are often forgotten when it comes to technological innovations. This implies a citizen-driven rather than a data-driven approach that takes citizens’ everyday practices as the starting point instead of embarking from the data sets available.
When considering the co-creation of digital services specifically, there is a long tradition of user involvement in information system development. Ever since the users of information systems (IS) became a different group of professionals from those that design and implement such systems, there was a gap between the expertise of professional software systems developers and prospective users. By involving users in the software design, their specific expertise about the use context and how they may be supported can be fed into the requirements specification. Although user involvement usually involves higher costs, there is agreement that the outcome of such involvement leads to higher user satisfaction and take-up (e.g. Vines et al., 2013; Bratteteig and Wagner, 2016; Ehn, 2008).

The success of participatory service design projects depends on the involvement of appropriate and representative users (Gidlund, 2012). The roles of citizens differ across the spectrum of these approaches. While participation in some co-creation initiatives is limited to the co-design of an interface of an application, others also involve citizens in generating topics and contents. Hence, participants can take different roles. In general, the roles citizens may assume have been either:

1. defined along the service design and provision process – plan, build, run (e.g. Voorberg et al., 2015):
   - citizens as initiator;
   - citizens as co-designers; and
   - citizens as implementers.

2. or, with respect to specific tasks – exploring, forming ideas, designing, diffusing (e.g. Nambisan and Nambisan, 2013):
   - explorer: identify problems to be solved;
   - idea former: generate solutions to well-defined problems;
   - designer: design and/or develop implementable solutions; and
   - diffuser: facilitate the adoption and diffusion of the developed solution.

When it comes to software design for older adults, most software development projects are based on the designers’ assumptions regarding older people’s needs. However, critical scholars in STS-inspired social gerontology but also human-computer interaction demand a more critical engagement with technology design for older adults (e.g. Neven, 2011; Peine et al., 2015; Wanka and Gallistl, 2018). In particular, they question the representations of “age” that are often scripted into technologies and call attention to the potential consequences of their use. Engaging older adults prior to the design process embraces alternative measures and attributes of “success” in later life (Vines et al., 2015, p. 20). Amongst others, these changes and extensions to the meanings of becoming old reveal the diversity and heterogeneity amongst the group of older people (Höppner and Urban, 2018). However, so far, there are few studies when it comes to digital services co-design with older adults. What is hence required are the development and evaluation of interventions and methods for engaging older adults in meaningful ways. In the following, we present a method that has been applied and adapted in critical interventions to smart cities: walking workshops or data walks. Data walks are particularly interesting with respect to co-design projects with older adults as they directly relate to everyday practices and experiences while, at the same time, allow for a critical engagement with data.

**Experimental ways of citizen engagement with data: data walkshops**

Walking is a human activity, engrained in urban and rural culture. It is also becoming a prominent method in projects related to critical data studies (Wieringa and van Es, 2018)
as well as participatory design (Kanstrup et al., 2014). What makes such walks an interesting and important tool for engaging (critically) with data is their embeddedness in everyday urban life. Data walks have been proposed and conducted in a number of projects aiming to engage with data and putting an “emphasis on the everyday experience of data” (Wieringa and van Es, 2018) as well as the relationality of design (Kanstrup et al., 2014).

Wieringa and van Es (2018) mapped a number of different formats each comprising of different set-ups and goals. For example, Greenfield and Kim (2011) set out to raise awareness/literacy on “networked urbanism” among citizens. Van Zoonen et al. (2017) and took city employees on walks through their own smart city. While Greenfield and Kim only delimited an area on a map, Van Zoonen et al. defined the routes beforehand. The focus of their walks was “identifying big data in the city and connecting it to political and ethical issues” (Wieringa and van Es, 2018). In so doing, Van Zoonen et al. not only raised awareness on data issues amongst civil servants, they also learned about the knowledge and beliefs of their participants with respect to the datafication of their city. Building on Greenfield and Kim, Powell (2018) experimented with different forms of data walks: initially to teach students about big data related to urban issues, later to create “bottom-up knowledge”. In her walks, participants assumed different roles from note-taker to photographers. Yet another format of data walks was conducted by Hunter (2018), who did not only want to raise awareness amongst participants but also collected environmental data on specific areas and built multi-layered “dataspaces”. Table I provides an overview on these different types of walks.

Walking and mobility within the immediate environment are particularly relevant when engaging older adults. In the context of co-creation with older adults, it relates to the importance of ageing in place and neighbourhood (Wiles et al., 2012; Manchester and Facer, 2016). A study conducted by Wiles et al. (2012) characterises “ageing in place” by the positive perceptions of older adults as a sense of attachment and social connection, a sense of security and familiarity and a sense of identity, linked to independence and autonomy. To assist older adults to remain in their communities and neighbourhoods with some level of independence, rather than in residential care homes, requires to consider not only their immediate housing options but also “transportation, recreational opportunities, and amenities that facilitate physical activity, social interaction, cultural engagement, and ongoing education” (Wiles et al., 2012). Appropriate information about the available resources in a neighbourhood can have a positive effect on social participation, if it relates to the (mediated) information practices, the abilities and limitations of older adults (see e.g. Beneito-Montagut et al., 2018).

One question that participatory design approaches allow to ask is what kind of (digital) information is relevant and useful to (a variety of) older adults, and what kind of data, data visualisations and data processing (e.g. filtering, searching) are required in order to provide this information. In the following, we present three dimensions along which we will evaluate the format of walking workshops for engaging older adults in the co-creation of digital public services. These dimensions are based on the objectives of participatory design projects and hence also hold up to methods aiming to engage future users in participatory open data projects.

3. Evaluation framework

Sharing control: openness and diversity of process

Rooted in the political agenda of Scandinavian participatory design, one of the main aims of participatory approaches is the destabilisation of power structures by sharing control over the design process and outcome (Vines et al., 2013). This is grounded in a moral proposition: participatory design is commendable because “the people whose activity and experiences will ultimately be affected most directly by a design outcome ought to have a substantive
Humans ought to be regarded as ”actors”, not “factors” (Bødker, 2006). Hence, when a co-creation process shall lead to a relevant and user-centred service for a certain target audience, the process has to be open for members of this target audience. If there is a heterogeneous target audience, one of the criteria for an effective engagement process is to make it equally accessible to different subgroups. Walking workshops hence need to be evaluated as interventions that ensure openness and diversity.

**Sharing expertise: older adults as experts in co-creation processes**

To include future users’ input in the design process increases the chances of a successful design outcome by taking into account their “expert perspectives and preferences regarding the activity that the design will support, and most likely transform” (Carroll and Rosson, 2007, p. 243). Pragmatically, hence, it is argued that “having the users participate makes it easier to implement the design result” (Bratteteig and Wagner, 2016, p. 426). One of the most common ways of eliciting users’ expertise are workshops in which teams of researchers, designers, system developers, future users and other stakeholders come together to identify
challenges and develop new ideas. In these workshops, “boundary objects” (Star and Griesemer, 1989) are co-developed that act as “shared articulations of knowledge of those participating in the design process” (Vines et al., 2013, p. 430). Depending on the design context and the quality of user participation, the interpretative weight of the design team differs.

Walking workshops are one format in which encounters between future users, designers and other stakeholders may happen. When considering the suitability of this format, it is important to evaluate to what extent it enables participating older adults to assume the role of experts and facilitates their role-shift from passive design subjects to active participants (Sanders and Stappers, 2008; Jarke and Gerhard, 2018).

Enabling change: relevance of process and value of outcome
Another important criterion to evaluate is the quality of interventions in a co-creation process with respect to their relevance for participants. In order to assess how relevant interventions were to the participants and to what extent their needs and interests were considered, the following questions need to be asked:

- What were the needs and interests that motivated participants to join?
- To which extent and how did the interventions address these needs, interests and motivations?
- How relevant, interesting and useful were the interventions?
- Did the process have any relevance beyond the participants?

Participatory design approaches aim to enable some kind of change. In order to do so, interventions need to allow designers to understand people’s current practices, experiences and how future design products may become appropriated (Vines et al., 2013). As such, the output of a co-creation process (e.g. digital public service) refers to a social innovation in the form of software and data that is embedded into a larger public online portal and provided to the general public. The value of such a digital public service for older adults needs to meet the central value proposition of open government and provide a more relevant service of higher quality and better accessibility than existing services.

4. Case study: data walkshops in Bremen

Background
In this paper, we are reporting on our experience of data walks as a method for co-creation with older residents. The co-creation project was conducted in a district in one of the project’s field sites: Bremen Hemelingen between April and December 2017. It resulted in a digital neighbourhood guide, which is now provided via the city information portal.

District 1 is split into various neighbourhoods that are both physically and socially segregated from one another. In close coordination with local intermediaries and social care providers that were already engaged in the wider research project, we developed the idea of co-designing a digital walking guide that would provide relevant and appealing information on walks in the district, and support the social aspect of walking by providing some kind of organisation and/or communication tool. Throughout the process, the value proposition of the service came to be formulated as follows: provide relevant and appealing information to older adults which activates and motivates group walks in the district and supports service providers in organising and announcing these kinds of walks by exploiting the full potential of multi-media technologies.

The research in this project was conducted by following an action research approach (Hayes, 2011). We carefully planned each of our interventions, observed and documented
them and adjusted further interventions accordingly. We used a reflective learning journal for documenting our interventions. This learning journal documented for each intervention the date, its length, the number of participants as well as the objectives of the intervention, a description of methods and activities, the results and a reflection on, e.g., the appropriateness of methods or surprising outcomes.

In total, 46 older adults from the district were engaged throughout the process. A core group of six people participated in almost all walks and continued to engage in subsequent design and prototyping activities as well. In addition, ten intermediaries and service providers were engaged throughout the process. A project board that consulted us on an ongoing and regular basis consisted of seven service providers and intermediaries. We conducted eight focus groups with older adults throughout the process. In addition, we conducted four interviews with members of the project board during the process and four interviews with social care service providers and local government after the process. Those interviews were recorded and transcribed, and analysed using thematic analysis (Guest et al., 2012).

Recruitment of participants
The target audience of the app was broadly defined as so-called third agers – older adults still relatively mobile and independent[1]. The recruitment was open to a broad range of older adults, and participants of the co-creation process were, to some extent, self-selecting. Furthermore, the participants themselves defined what characteristics made a difference with respect to experiencing ageing in their neighbourhood. The target audience of the co-creation process hence became refined throughout the process and continuous engagement with participating older adults and intermediaries. The refinement of the target audience helped narrowing down the “problem focus” and defining a service.

Recruiting participants for a co-creation process whose outcome is somewhat undefined by nature and with tasks unfamiliar to most older adults was a great challenge. Our recruitment strategy for older adults considered the different requirements and emphasised that digital skills were welcome, but that other competencies such as good local knowledge was equally important. We set up a project board in order to engage local stakeholders and to facilitate the recruitment of older citizens. The local service providers and intermediaries that were engaged in the project board supported the recruitment through individual address, via leaflets and through newspaper articles. Engaged participants also often invited acquaintances.

Phase 1: detailing the service idea for digital walks
In order to detail the concept for a digital service and define the data (categories), the first walking workshop was conducted in June 2017 together with a social activity manager of a senior citizen centre. The participants were recruited through the staff of the senior citizen centre but also via newspaper announcements. Most participants could walk without support, and few had walking aides. The intended goal was to identify relevant attributes for walking routes (what information older adults need or are interested in on walking routes). In addition, the aim was to raise interest in the project so that participants would become engaged throughout the process.

The route had been defined in a preceding meeting with the project board. The announcements in the newspapers foregrounded the joint walk through the neighbourhood rather than the technology focus of the project itself, in order to keep the barriers for participation low. It was planned to walk together along the route and fill out a questionnaire on what attributes may be considered relevant. The questionnaire had been developed based on literature on accessible and age-friendly neighbourhoods and cities by the team facilitating the project. It asked the participants “to mark what you think is
important for the description of walks and paths and make notes if you have discovered something accordingly on the way” and offer response items in the following areas:

- points of interest (architecture/buildings, historical, green areas, art, other);
- helpful things (benches, restrooms, railing/handrails, street greening (shade), illumination, other);
- useful things (shops, services, sport, playgrounds, other);
- rest points/provision of food and drinks (cafés, restaurants, kiosk, bars, other);
- sidewalks (inclination/longitudinal and/or transverse inclinations, narrow places, separation of footpaths and cycle paths, obstacles, breadth, height of the curb, cleanness, surface condition, other);
- road crossing/unavoidable road use (traffic light available, traffic island available, lowered curb, surface of the road to be crossed);
- size (lanes/tracks) of the road, traffic intensity, pace, other;
- annoying things (dog excrement, dirt/waste, noise, smell, cyclists on footpaths, other); and
- public transport stops (shelter, other).

Nine older residents from the district participated in this first walk. Most of them had lived there for a long time and were very knowledgeable about it. They had a lot to tell about the historical developments in the district, which turned out to be a main point of interest for walks. The analysis of the questionnaire confirmed the impression that the participants were more interested in historical and recreational attributes than in information on accessibility. Five participants were interested in architecture and buildings; four were interested in historical information. Six were interested in recreational spaces. While seven stated to appreciate information on benches and toilets, only three were interested in information about traffic lights and almost none listed any of the attributes concerning the pavement and the road crossing. In a subsequent focus group, which was meant as a debrief of the results, it became apparent that, in addition to the accessibility of walks, a thematic focus of the digital walking guide on historical and recreational walks was commended.

The results of this first walk confronted us with the recognition that the data required to realise this co-created service concept were not available. We had expected that the target group would be particularly interested in the accessibility of routes and buildings, public transport, benches, toilets, restaurants and other practical aspects, on which open data sets are (easily) available. However, we quickly realised that the required information on the history of and stories about the district as well as tips about recreational places (e.g. for walking) was not available: all of the participants had their personal stories to tell which revealed surprising and interesting facts about the historical development of the neighbourhood. Some of them knew places unknown to the others they wanted to share. In order to collect this local knowledge and make it available via a digital service to a broad range of older adults in the district, we started conducting data co-creation walks.

**Phase 2: conducting data co-creation walks**

The walks were collaboratively defined with different stakeholders. They differed in their scope and framing:

- walks in parks and recreational areas (walks 1–4): three of the walks were conducted in collaboration with the senior citizen meeting place in one of the neighbourhoods; and
- guided historical walks (walks 5–6): we conducted two walks that were each conducted by an older resident that talked about the neighbourhoods’ history.
Each walk was announced via the local newspapers, the district’s website as well as the network of service providers. They were between 2 and 3 km and lasted between 1.5 and 2 h. This time was proposed by the network of service providers (project board) as most suitable (also for people with mobility issues) and contained time for breaks. The starting points were well-known places in the district and reachable by public transport. Each of the walks included at least one stop for either lunch, or cake and coffee. The descriptions of the walks featured places with lunch offers for older adults or coffee and cake as well as public toilets and benches. Figure 1 presents an overview of the different stakeholders participating in the walks.

The older participants and service providers assumed different roles in the walks:

- **Organiser**: one of the local social care service provider acted as organiser of the walks. They published the announcement in their networks and newspapers and also organised with other service providers for visits during lunch time or for coffee and cake.

- **Guide**: the tours were either guided by knowledgeable residents on historical points of interest or planned as walks through parks and recreational areas.

- **Data collector**: most participants on the walks used a clipboard to note down points of interest, issues with the infrastructure (e.g. missing benches) and other noteworthy things.

- **Data validator**: one of our participants checked the location of benches on the walks as provided by OpenStreetMap. If benches were missing on OSM, he added them; if benches were listed on OSM but not existent, they were deleted.

- **Photographer**: overall, three older adults supported our data collection by taking pictures. Not all pictures could be taken during one of the walks, so all of them volunteered to visit points of interest again.

During the walks, a central topic that the participants discussed was the age-friendliness of the urban infrastructure. Since the discussion on the walks was recorded, valuable data on problems about and with the physical infrastructure were collected. Subsequently, the data were presented during one of the district council meetings in order to suggest improvements (e.g. installing new benches) meetings. The data collected on the walks were then used to co-create a walking guide that visualises the routes and provides the relevant information as well as appealing multi-media content that is meant to motivate older adults to explore their district jointly. In order to do so, a number of design workshops were conducted in which participant produced multi-media content.
**Phase 3: user testing**
In order to review the functionality of the app, which was developed in subsequent workshops and the quality of the data, a last walk was conducted where participants tested the digital public service by using the application on tablets. They were asked to review and discuss the functionalities, the relevance of the content and the quality of the data. This led to a number of usability and functional issues that had to be resolved.

**Summary: phases 1–3**
Overall, the walkshops conducted helped us define and refine a service concept, co-create data and test the digital service developed. Table II provides a summary of the three different formats of walks. Participants in those walking workshops assumed a number of different roles, from explorer (what kind of walks are of interest to other older adults), to idea former (what kind of information may be of interest to others), to data creators and validators, users and testers of digital apps.

In the following, we evaluate how these walking workshops performed against our participation framework and allowed for the sharing of control by enabling an open and diverse co-creation process; the sharing of expertise by establishing participating older adults as experts; and the enabling of change by addressing the needs and interests of participants and creating value for (other) older adults.

## 5. Evaluation

**Sharing control: openness and diversity of data walkshops**
The district walks addressed all older people who were interested in exploring the district or the different neighbourhoods jointly. We made sure that the length and quality of the routes allowed a broad range of older adults to participate. This included also people with walking aides. In so doing, we wanted to include people for whom the technological aspect of the project might have been deterrent. Thus, we emphasised the value of local knowledge. The walks were well attended, but only a few participants engaged in other, more technology-related tasks of the process. The neighbourhood manager suggested that this was due to people’s prime interest in neighbourhood walks, or more specifically only walks in particular neighbourhoods. She argued that this may have been due to people being interested in meeting acquaintances and being able to socialise during the walks rather than

<table>
<thead>
<tr>
<th>Type of walkshop</th>
<th>Ideation walk</th>
<th>Data co-creation walk</th>
<th>User test walk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Occurrence during project</td>
<td>1</td>
<td>6</td>
<td>2</td>
</tr>
<tr>
<td>Goals</td>
<td>Defining relevant categories/ information needs</td>
<td>Collect data on pre-defined categories</td>
<td>User testing of the new app</td>
</tr>
<tr>
<td>Number of participants</td>
<td>5</td>
<td>Between 5 and 20 (usually with 5 active members)</td>
<td>Older adults</td>
</tr>
<tr>
<td>Type of participants</td>
<td>Older adults and service provider</td>
<td>Older adults and service provider</td>
<td>Older adults</td>
</tr>
<tr>
<td>Roles of participants</td>
<td>Explorer</td>
<td>Navigator</td>
<td>User</td>
</tr>
<tr>
<td></td>
<td>Idea former</td>
<td>Photographer</td>
<td>Tester</td>
</tr>
<tr>
<td>Duration</td>
<td>60 min</td>
<td>60–90 min</td>
<td>60 min</td>
</tr>
<tr>
<td>Duration of event</td>
<td>~ 2 h</td>
<td>~ 2 h</td>
<td>~ 2 h</td>
</tr>
<tr>
<td>Event makeup</td>
<td>Walk-discussion</td>
<td>Walk-break (coffee/lunch)-walk</td>
<td>Walk – debriefing</td>
</tr>
<tr>
<td>Outcome</td>
<td>Initial list of information needs</td>
<td>Written responses on walks</td>
<td>List of technical issues</td>
</tr>
</tbody>
</table>

Table II. Comparing different types of walking workshops
wanting to develop a digital district guide. She further suggested that participants were interested in the history of the district and wanted to learn about it. Judging from the number of participants per walk, we could clearly see that the two historical walks had the highest number of participants.

Two participants from the later formed design group confirmed that they experienced the recruitment strategy as open and accessible. One stated that she particularly liked the opportunity to “have no barrier, just being able to see how it goes”. Another one stated that she liked the fact that people got “lured out of their house”. A potential weakness identified by participants related to the socio-economic diversity of participants. The neighbourhood manager suggested that we mainly engaged senior citizens from the “middle class”. This was confirmed by a participant from the core group who can be considered part of this “middle class”. According to their view, the challenge was to get those people involved with low socio-economic status (“Getting them, that’s the art”). Another participant, herself at this “lower end of the income scale” by contrast, observed that residents from the better-off neighbourhoods were missing, as they did not have as much of an incentive to leave their gardens for a walk as residents without private outdoor space.

As we organised the walks in collaboration with social care service providers, we mainly addressed those older adults who were already participating in their activities. In addition, others joint through newspaper announcements. Engagement may hence effectively secured through local service providers as they are already involving a broad range of older adults from their district. The drawback may be that some people might not feel addressed by certain places/organisers (e.g. the church, a certain neighbourhood). What is hence important is to consider organising activities with different hosts and places in order to give a variety of people a chance to participate and engage in the process.

Sharing expertise: older adults as experts in co-creation processes

The walks were important for establishing the participants as experts. While walking along routes and places that the participants knew well, they were given the opportunity to contribute their local and/or historical knowledge. Several participants described themselves as “contemporary witnesses”. In particular, after conducting the data co-creation walks, the participants felt encouraged to share their historical and local knowledge. This experience remained an important point of reference also in subsequent, more technical workshops and meetings. For example, one of the female participants said that even though the men were more knowledgeable with technology, she could contribute with her knowledge about the district’s history.

Overall, participants confirmed that they felt a sense of ownership over the resulting app. This was for example expressed through active involvement and shaping of the data co-creation:

- participants suggested and planned routes/walks;
- participants volunteered to guide a historical walk or facilitated contact with a local historian; and
- a few participants from the core group regularly looked at the prototype and pointed out errors and missing data.

Not all participants were fully aware of the overall goals of the project. This was partly due to the different ways in which they had been invited. Some people only participated in one or two walks. In conversations along the way, they stated that they did not have the time to commit to a longer project (e.g. because they were caring for a relative and simply took the opportunity to go on a walk because it fitted with their schedule this particular week) or they were not interested in further engaging with technology. The walks hence allowed a variety of people to contribute to the overall project, even if they did not engage in the prototyping part as such.
Enabling change: creating value for older adults

Finally, we were interested in learning to what extent the process addressed the needs and interests of participants and thereby enabled change. There was not one particular need to be satisfied with the co-creation process, but rather five overlapping interests:

1. doing something for the home district or getting to know the district better;
2. engaging with new technology;
3. learning new things;
4. doing something to improve the image of the neighbourhood/district; and
5. socialising with others.

Most of the participants mentioned an interest in the district or a specific neighbourhood as motivation to join the process. For others, doing something for the home district was a strong motivation. One participant emphasised her sense of self-efficacy to be politically engaged and not to leave things to the politicians. Her participation in the process was part of her local political engagement and her interest in local history.

In particular, participants stated that they wanted to improve the image of the neighbourhood/district. This related strongly to the issue of segregation that was emphasised by the participating older adults as well as other stakeholders. For those who wanted to learn something about the district, the walks were relevant as well as for those who could share their knowledge. In addition, participants expressed an interest and the feeling to need to engage with new technology. This interest was based on their feeling of being socially excluded through non-use but also in a genuine interest in how software development “works”.

All stakeholders we interviewed stated that the final digital service was relevant to older users. A social activities manager said that “going for a walk is much more part of the reality of older adults than of younger generations”. In addition to the overall relevance of walks for older adults the service providers, intermediaries and participants defined the value of the service for particular groups of older adults: Most emphasised the value for older people who do not know the district very well or have limited financial resources. The information provided also allowed for better planning of walks and hence increased people’s confidence in being able to “master” a walk in an unknown neighbourhood.

Hence, similar to accounts from other data walks, the participants were able to engage with their neighbourhoods in different ways. Drawing on an everyday activity such as walking and turning this experience into a digital public service created value for different groups of older adults.

6. Discussion and conclusion

The re-use of Open Government data is part of the core objectives for civic co-creation projects (Sieber and Johnson, 2015), yet it is also one of the most demanding ones with respect to engaging (older) citizens. The co-creation of citizen-driven – rather than data-driven – digital services entails a number of challenging activities:

1. As part of the service co-creation, categories and objects of interest to citizens need to be defined.
2. A survey about existing data concerning these objects needs to be conducted and their completeness needs to be assessed. This may lead to the collection and validation of data that have been identified as relevant but are not yet open or need to be collected across various data owners.
3. Subsequently, attributes for the objects need to be defined and data for these attributes collected.
Missing data need to be collected and/or co-created with citizens. The service and collected data need to be presented in a meaningful way to users. Editorial work (such as descriptions about data objects) is necessary, as well as the long-term maintenance of the data and the service.

Online information service designers adopting co-creation approaches therefore need to take into account that information identified as relevant by citizens may not be available as open data and plan ahead to collaborate with various data owners (e.g., service providers). They need to allow sufficient time for data creation and curation during co-creation processes. In addition, suitable methods for collecting and creating data as well as user-friendly interfaces to digitising these data are required.

Above we presented data walkshops as a co-creation method to engaging older adults in the design of a digital neighbourhood guide and co-creation of open data. The three types of walks that we conducted were complementary with respect to how they facilitated the sharing of control and expertise, and enabled change for different groups of older citizens. Table III summarises how the different walking formats contributed to each of the co-creation principles and specifies the roles that citizens assumed.

Overall, our findings suggest that for older adults' data walking workshops proved to be an effective and satisfactory form of engagement. This age group has a sustained interest and knowledge about their neighbourhoods and what it means to grow older in a particular place. Walks combine a social aspect with physical activity — both are viewed as having a positive effect on health and well-being. Furthermore, giving older adults the opportunity to

<table>
<thead>
<tr>
<th>Co-creation principles</th>
<th>Guiding questions</th>
<th>Ideation walk</th>
<th>Data co-creation walk</th>
<th>User test walk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sharing control</td>
<td>How open and diverse is the method? Was a variety of citizens included? Who was excluded?</td>
<td>Allowed to define relevant categories and articulate information needs Role: explorer</td>
<td>Included planning of walks (which route) Allowed for a variety of citizens to participate (low threshold, related to everyday activities) Role: navigator</td>
<td>Participants evaluated the digital app and suggested further improvements Role: tester</td>
</tr>
<tr>
<td>Sharing expertise</td>
<td>(How) were participants established as experts? What kind of expertise did they contribute?</td>
<td>Participants defined relevant categories and information needs based on their own experience Role: idea former</td>
<td>Participants collected and validated data on pre-defined categories Roles: photographer; note-taker</td>
<td>Participants contributed with feedback as life-world expert Role: user</td>
</tr>
<tr>
<td>Enabling change</td>
<td>What were the needs and interests that motivated participants to join? To which extent and how did the interventions address these needs, interests and motivations? How relevant, interesting and useful were the interventions? Did the process have any relevance beyond the participants?</td>
<td>Data walkshops catered for participants' interest for their/in neighbourhoods (and their improvements)</td>
<td>Data walkshops allowed participants to discover their neighbourhood ( anew), including those with mobility issues, other commitments (e.g. caring for a relative) or financial constraints Role: user</td>
<td></td>
</tr>
</tbody>
</table>

Table III. How data walks meet co-creation principles
share their experiences and knowledge was appreciated by the participants. Collecting this information and making it available in a digital service further values the participants and, at the same time, is beneficial to a broader target audience.

Hence, using this experimental form of engagement allows not only for critically engaging with data (Van Zoonen et al., 2017; Wieringa and van Es, 2018; Hunter, 2018; Powell, 2018), but also to engage a variety of citizens in civic tech activities to co-design, implement and evaluate digital public services that benefit their communities. Data walks are a promising method to facilitate “participatory open data projects” (Sieber and Johnson, 2015) by engaging citizens that are often excluded as partners in digital innovation. They are a method to enrich the current civic tech formats and allow a variety of citizens to engage with data about their neighbourhoods, districts and cities in a meaningful way. Such walkshops may attract participants beyond the “usual suspects”, but they are also in themselves a meaningful activity to contribute to social participation. Hence, even if not all participants of walkshops continue their engagement in the digital service development, they still benefit from participating in and contributing to the process and its outcome. What needs to be admitted is that not everybody is willing or able to participate in a longer-term process. Nevertheless, such walks provide an opportunity for any community member to become involved selectively.

The data walkshops as described here were part of a larger co-creation project to design and implement a digital neighbourhood guide. There are a number of pre-conditions that framed the ways in which the co-creation project, in general, and the walks, in particular, were framed. These relate to the existing collaborations of local stakeholders and the existing services they provide to residents. Conducting effective co-creation activities means to get such local stakeholders on board and include them in the recruitment of participants. If a digital service is to be developed that is sustainable and maintained after a project ends, the service needs to contribute to their service portfolio. Existing open data are important to consider, and some will already be used for the delivery of existing services. However, data maintenance is a key challenge of participatory open data projects and it is important to consider how newly created data will be maintained after a project terminates.

In conclusion, there is a clear tension between data-driven app development and citizen-driven service co-creation as much of the information identified as relevant in co-creation processes is not necessarily available as open data. We argue that effective and relevant services for older adults should not be driven by what data are available, but rather have to be based on the needs and requirements of the target audience. Through the pilot work presented above, we identify that data walkshops provide a way of engaging older adults in the co-creation of data and digital public services. Through such interventions, older adults cease to be subjects of digital innovation and become co-designers. Age and ageing are not merely understood as a problem that needs a technological fix, but rather older adults’ expertise and lived experience become resources for the co-creation of value, knowledge and technology.

Acknowledgement
MobileAge has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 693319. This co-creation project would not have been possible without the support of the many older residents and local social care service providers in Bremen Hemelingen. In particular, the author would like to thank the participating older adults, the district councils and the Netzwerk Alte Vielfalt. In addition, the author would like to thank her colleagues Herbert Kubicek and Ulrike Gerhard for being such a fantastic team; Frank Reins and Frank Berker from the MobileAge project for joining her on the walks and this co-creation journey; and Jo Bates for the valuable and constructive feedback on an earlier version of this manuscript.
Note

1. Laslett’s (1991) distinction of the third and fourth age is helpful in defining the target audience of a service, since the specific needs of older adults differ not so much with regard to their biological age but to their life circumstances, capabilities and needs.

References


**Corresponding author**

Juliane Jarke can be contacted at: jjarke@ifib.de

---

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 Tower of Babel problem: making data make sense with Basic Formal Ontology

Andrew Iliadis

Department of Media Studies and Production,
Temple University, Philadelphia, Pennsylvania, USA

Abstract

Purpose – Applied computational ontologies (ACOs) are increasingly used in data science domains to produce semantic enhancement and interoperability among divergent data. The purpose of this paper is to propose and implement a methodology for researching the sociotechnical dimensions of data-driven ontology work, and to show how applied ontologies are communicatively constituted with ethical implications.

Design/methodology/approach – The underlying idea is to use a data assemblage approach for studying ACOs and the methods they use to add semantic complexity to digital data. The author uses a mixed methods approach, providing an analysis of the widely used Basic Formal Ontology (BFO) through digital methods and visualizations, and presents historical research alongside unstructured interview data with leading experts in BFO development.

Findings – The author found that ACOs are products of communal deliberation and decision making across institutions. While ACOs are beneficial for facilitating semantic data interoperability, ACOs may produce unintended effects when semantically enhancing data about social entities and relations. ACOs can have potentially negative consequences for data subjects. Further critical work is needed for understanding how ACOs are applied in contexts like the semantic web, digital platforms, and topic domains. ACOs do not merely reflect social reality through data but are active actors in the social shaping of data.

Originality/value – The paper presents a new approach for studying ACOs, the social impact of ACO work, and describes methods that may be used to produce further applied ontology studies.

Keywords Data ethics, Applied computational ontology, Semantic technology, Social ontology, Tower of Babel problem

Paper type Research paper

Introduction

Applied computational ontologies (ACOs) are standardized metadata vocabularies that provide rules to structure data through organizing and labeling, in a manner that can be understood by specialists and users working in different disciplines. ACOs can be found in products as diverse as virtual assistants like Siri, Cortana, Alexa and Bixby, in semantic web metadata on websites, apps and platforms, and in scientific research software and databases. In these areas, data exist in formats that are often incompatible and formalized locally. Data-labeling standards, for example, are made using general terms, are based on natural language or are adopted using formalized but limited classification systems. Such a lack of quality vocabularies for accessing and reasoning with heterogeneous data in uniform ways makes it hard to achieve the semantic interoperability of data across systems. Developed by researchers over the past three decades, one solution has been to provide logical (computable) definitions using controlled metadata vocabularies of preferred labels for describing data combined with tags – a practice known as applied ontology making.

Ontology engineering projects, in their quest to create semantically interoperable data entities, may be prone to several communication problems stemming from assumptions and biases in data reasoning. For example, ontology builders may disagree on shared terms or propose contradictory logics in the construction phase, or ontology users may mistakenly apply ontological principles. Since this is both a computational and a social process, analyzing such contextual ontology-making scenarios and communities requires the tools of
qualitative inquiry and historical analysis along with digital methods. This paper is a first attempt at analyzing data-driven ontology practices through the framework of data assemblage theory (Kitchin, 2014; Kitchin and Lauriault, 2018) and proposes a multifaceted approach to studying applied ontology work. Building on qualitative work in knowledge representation and information infrastructure studies (Edwards et al., 2009, 2013; Plantin et al., 2018; Ribes and Bowker, 2009; Ribes and Finholt, 2009; Bowker et al., 2010) and research into data ethnography (Knox and Nafus, 2018), I present several years’ worth of research on an emerging, data-intensive form of scientific media that I refer to as ACO and offer several lenses through which to study the work of ACOs and their practitioners.

The paper’s last section contributes to knowledge through a discussion of the ethical implications of ACOs. As others have shown, ACOs have ethical consequences (Vang, 2013; Pulsifer and Brauen, 2017; Iliadis, 2018). Is there evidence that ACOs typify semantic logics or biases? What types of data do ontologies organize? How are ontologies practically applied in social contexts? To answer these questions, this paper looks to a powerful and widely used upper-level ACO called Basic Formal Ontology (BFO) and draws on research from unstructured interviews conducted with leading BFO ontologists at the National Center for Ontological Research (NCOR) from 2015–2016, as well as examples of BFO’s internal logics, including ontology visualizations, a partial analysis of BFO’s syntax, and NCOR member discussion data scraped from BFO public message boards. This paper also examines how BFO has been applied to data about social entities and their relations – products of collective intentionality and constitutive rules – and ends by suggesting that, because ontologies make claims while normalizing social roles in data organization, ACOs should undergo ethics reviews before they are rolled out into social data domains.

**Methods**

BFO proposes a new way to organize and communicate data between domains through metadata interoperability and is used by hundreds of ontology-driven endeavors throughout the world. To better understand this community and their practices, I conducted interviews with experts in the domain. For example, I was involved in ongoing interviews and conversations with ontologists involved in ACO engineering at NCOR, who were interviewed over an internet-connected telephone over a two-year period. The interviews were unstructured, conducted over Skype, and recorded using CallGraph for Windows. The content was anonymized and transcribed using CastingWords. Interviewees were asked whether they viewed ACOs as solutions to data communication problems and all replied that this was the case. Representative questions asked during these interviews included: how is applied ontology practiced? How does logic contribute to building applied ontology frameworks? Why are some computational ontologies preferred over others? Each interview was conducted with the aim of understanding more about how ACO communities, infrastructures and theories assist with semantic data interoperability. The interviews also provided a firsthand account of the practices of ontology engineering, including the people, places, and technologies that have contributed to the field. I used Protegé software, freely available from Stanford, to visualize BFO and lower domain ontologies, and scraped relevant websites and message boards with HTTrack, a website copier. As such, this paper follows a mixed methods approach (Creswell, 2013), utilizing a mixture of digital ethnography (Pink et al., 2016) and digital methods (Rogers, 2013). I conducted a digital ethnography of BFO as a relational and ecological infrastructure (Star, 1999) via thick description (Geertz, 1973) and long-form interviews (Weiss, 1995) with scientists and philosophers involved in the applied ontology-building process, and utilized archival research (Ramsey et al., 2009; Carmichael, 2012) for probing the large online repository of resources made available by the BFO project team. Ethical clearance was received to conduct this research.
Data assemblages
In recent years, science and technology studies (STS) has engaged applied ontology as an empirical object of inquiry (Woolgar and Lezaun, 2013). A special issue of Social Studies of Science published in 2013 under the title “A Turn to Ontology in Science and Technology Studies?” describes the “ontological turn” in STS as consisting of “multiple discussions deploying the language of ontology” (Heur et al., 2012, p. 341). Included among these discussions is the wider philosophical debate between constructivism and realism, empirical discussions of ontology’s instruments and classification, and methodology in the social sciences and the humanities in general. The approach to ACOs taken in this paper falls in the second category, focusing specifically on an ACO’s instruments and classification system and the communication technologies of its builders. Building on this recent turn to ontology in STS, I follow the framework of data assemblage theory (Kitchin, 2014; Kitchin and Lauriault, 2018) by focusing specifically on the communicative tools and practices that are involved in making up ACO-generated data. The data assemblage framework presented here should be understood as a theoretical construct for situating research around material data structures that emerge, through a variety of social processes existing at multiple scales. A data assemblage points to a complex of entities that form the underlying production of data at multiple levels and in a plurality of domains – an example of what Kennedy and Bates (2017) have referred to as data power in material contexts.

As Kitchin (2014) notes, data assemblages “frame how data are produced and to what ends they are employed” (p. xvi). Data can be conceived as “the central concern of a complex sociotechnical assemblage” that is “composed of many apparatuses and elements that are thoroughly entwined, and develop and mutate over time and space [...] they interact with and shape each other through a contingent and complex web of multifaceted relations” (Kitchin, 2014, p. 24). Computational ontologies, as a specific type of digital materiality and infrastructure involved in shaping semantic data practices, may be critically examined to see how semantically enhanced data are generated by persons but also institutions, financing, and forms of knowledge that are never neutral but networked in ways that serve specific ends. Semantic data integration, as the aim of computational ontology, should be considered along with the apparatuses and infrastructures that make it possible. Computational ontologies are suitable objects of inquiry for such a data assemblage approach, since they are comprised of multiple histories, groups, institutions, standards, and methods.

By foregrounding the infrastructures of ACOs, I highlight the hidden work that goes into building semantics into data products. Products like virtual assistants, semantic web platforms, and data repositories all depend on ACOs to produce semantic interoperability. A critical approach to studying ACOs would be “a struggle against the tendency of infrastructure to disappear” (Bowker and Star, 2000, p. 34), specifically in the context of the semantic enhancement of data. Bowker and Star (2000) write that “infrastructure inversion means recognizing the depths of interdependence of technical networks and standards, on the one hand, and the real work of politics and knowledge production on the other” (p. 34). Data run through hands-on and political infrastructures in applied ontology work – this paper foregrounds these infrastructural data journeys (Leonelli, 2016; Bates et al., 2016) by calling attention to the cultural work of applied ontology practitioners and the data frictions (Edwards et al., 2011; Bates, 2018) that occur in the ACO data lifecycle.

Applied computational ontology
“Ontology” was used intermittently in early conversations about AI, information theory, and computer science ( McCarthy, 1980) but it was in the early 1990s with the publication of a series of papers by Gruber (1991, 1993a,b, 1995) that ontology spread as a popular term for achieving semantic interoperability among heterogeneous data. In his entry for
“Ontology” in the *Encyclopedia of Database Systems*, Gruber (2009) elaborates, writing that “in practice, the languages of ontologies are closer in expressive power to first-order logic than languages used to model databases” (p. 1963). A philosophical concern for centuries, ontology is now a practical concern for researchers and practitioners who must grapple with data-driven labeling practices. In computer and information science, a metadata infrastructure of entities and descriptions of their attendant meanings, definitions, and relations is an example of a computational ontology, defined by Guarino et al. (2009) (Guarino is another early practitioner of applied ontology work and a pioneer in the field) as a “means to formally model the structure of a system, i.e., the relevant entities and relations that emerge from its observation, and which are useful” (p. 2).

As standardized metadata vocabularies for annotating and structuring data, ACOs are a complex and pervasive form of emerging scientific media (Smith, 2016) that stand to revolutionize industries and domains of social life (Staab and Studer, 2009). Computational ontologies assist with data integration and interoperability at the intersection of a variety of disciplines, from bioinformatics (Bodenreider and Stevens, 2006) to management (Allen and March, 2012), military intelligence (Dragos, 2013) to farming (Sivamani et al., 2013). Largely invisible to individuals who use digital technologies in everyday life, ACOs operate in the background. They assist with processing divergent data that are about entities, attributes, and relations (of portions of reality) in various social, governmental, economic, and scientific data contexts by describing data in a “hands-off” way. One senior ontologist at NCOR described combing data structures using ACOs in the following way (telephone interview, 2015):

I would say that the idea of making data structures cohere can be understood in two ways. One way is that you rebuild the data structures so that they cohere. The problem with that approach is that it’s expensive and it creates new errors. Every change can lead to a problem, because somebody makes a mistake, or some machine isn’t programmed properly. The other way of making data structures cohere is to describe them in a hands-off way, using a common vocabulary.

Ontology building involves multiple partnerships and is a largely interdisciplinary endeavor (Okada and Smith, 2008). Work in applied ontology building can involve philosophers who are able to logically define categories and their relationships (Smith, 2003), as well as computer and information scientists who construct technical software, like Protégé (available for free through Stanford) for classification systems. Ontologies can be “domain specific” (meaning they can be about a topic or field, containing specific terms related to that field) or they can be “upper level” to provide logical rules for combining multiple domain-specific ontologies (BFO is an example of an upper-level ontology). Figure 1 is an example of a domain-specific ACO – the elementary Beer Ontology, displayed in the

![Image](https://www.cs.umd.edu/projects/plus/SHOE/onts/beer1.0.html)
ontology-editing Protégé software. In bioinformatics, ontologies such as the Gene Ontology are more complex and used to organize data from divergent experiments to compare multiple items such as diseases and species (Mayor and Robinson, 2014). In business, ontologies can be used to make data available across multiple departments (Michel, 2016).

Ontologies include definitions and relationships that are logically formalized to produce greater data intelligibility (Heiler, 1995). Outside of specific domains, ontologies can enable understanding among various research fields by allowing better data communication (Kallinikos et al., 2013). Ontology construction is practiced in many emerging research areas, including bioinformatics (Stevens, 2013), geospatial analysis (Kitchin, 2014), management systems (Orozco, 2012), chemical engineering (Marquardt et al., 2010), commerce (Fensel, 1998), judicial knowledge (Casellas, 2011), computer and information science (Polí et al., 2010) and food (Boulos et al., 2015). Such ontologies are more than taxonomical hierarchies in that they provide context and explanatory power for how data entities are related.

There are several differences between taxonomies and ontologies. The goal of both in the field of computer and information science is to produce semantic structures that can be used to order information in a way that is legible to different groups of users. For example, a library or a database may have a taxonomy in the form of a schema that lists the contents of the search field – most books have indexes at the back, libraries have catalogs, and databases have relational models. The semantic strength represented in these examples is relatively weak considering they mainly deal with hierarchies of concepts (subclass and superclass). The relationship between entities in a taxonomy is structurally like that of parent and child – taxonomies are basic organizations of classes without qualifications about the properties of the entities. Ontologies sit at the other end of the spectrum and provide strong semantics, depending on their degree of expressivity. For example, ontological metadata may be used to qualify the physical nature of a piece of information in the form of mereological (part_of, has_part, overlaps), topological (boundary_of, connected_to, adjacent_to) or dependence (inheres_in, bearer_of) relationships. Such qualifications provide a higher level of expressivity and context for data entities using the rules of first-order logic.

Applied ontologies can reduce bureaucratic bloat (Riaño, 2009) and generally assist in knowledge discovery and innovation using big data (Wagner-Pacifici et al., 2015; Kitchin and McArdle, 2016) while enabling better human-computer understanding across complex sociotechnical domains (Geels, 2010). They allow for data integration and harmonization so data from divergent domains can be synthesized to produce new forms of knowledge (Bodenreider, 2008). In this, applied ontologies sit at the intersection of science and technology – neither scientific theories nor technological determinism satisfactorily account for the relational work of applied ontologies. When harnessing pre-existing scientific data with complex logics and computational sorting tools, applied ontologies may produce new knowledge that contributes to scientific progress in ways that did not exist previously (Brodaric and Gahegan, 2010). Ontologies fill in the gap that exists between science and technology by using technology to expand pre-existing scientific data to produce new scientific discoveries (Bundy, 2008). To use a rather clunky metaphor, ontologies are like a good translator that not only translates languages instantly but also can discover new compound words, neologisms that are more accurate constructs of words that previously existed in the original language (e.g. connecting “after” and “noon” to create “afternoon”). Applied ontologies use logical rules and axioms to provide comprehensive and accurate representations of data that are used in scientific research, online digital platforms, and semantic web tools (Munn and Smith, 2008).

The Tower of Babel problem
Like many growing disciplines, problematic issues in ontology engineering are the result of a perennial problem – typically, this is referred to as “the Tower of Babel problem”
The Tower of Babel problem (ToB) states that each time a new database or ontology is constructed new terms are developed that represent an ever-changing language, thus complicating applied ontology building, the goal of which is to produce semantically strong ontologies that can last over time. Sometimes a group of databases can be paired in such a way that they share the same language. Yet, in many cases, databases that exist in similar domains remain blocked from each other due to labeling differences – their definitions and relations do not cohere. The ToB problem is what prevents ontologists from realizing the full potential of ontologies. Each new category and relation from a different domain threatens to undermine an ontology by the heterogeneity of the labels and data structure. As a leading scientist involved in applied ontology building with NCOR explained (telephone interview, 2015):

I quite often make the claim that, if we want to advance science, we should stop talking. I honestly believe that natural language did not evolve in a way that allows us to speak about reality in the way that we should speak, because of all the discoveries that have been made. And that is not just a matter of adding new terms to the vocabulary. It has mainly to do with the way, when we hear sentences and how they are phrased grammatically, that gives us already a bias toward interpretations, things that have clearly been demonstrated in the work by George Lakoff. Sometimes we fall also in that trap; sometimes I read my own work from five years ago and I must say that I am not sure anymore that I meant what I said.

If the goal of ontology building is to eventually construct a language hierarchy of entities, attributes, and relations through which human users can process and search large quantities of disparate data, how does the malleability of language and the transient nature of word adoption enable or impede the development of applied ontology? There has been a widely recognized need for “practical methodologies and technologies, which can assist a variety of user types with ontology development” (Suárez-Figueroa et al., 2012, p. 1). Multiple international organizations, projects and centers have been created to assist with ontology engineering and solving the ToB problem, the development of methods for semantically processing disparate data domains, and create successful metadata vocabularies. These include the Institute for Formal Ontology and Medical Information Science (IFOMIS) at the Philosophy Institute of Saarland University, the Laboratory for Applied Ontology in Italy, NCOR, the National Center for Biomedical Ontology (NCBO) in the USA, the Schema.org partnership between Google, Microsoft, Yahoo, and Yandex, and the World Wide Web Consortium, among others. There are journals, societies, and conferences dedicated to ontology, including Applied Ontology: An Interdisciplinary Journal of Ontological Analysis, the International Association for Ontology and its Applications, and the International Conference on Formal Ontology in Information Systems, among others.

Ontology communities
That communication remains at the center of ontological enterprise means that ontology communities are an important part of the ontology-building process. Currently, there is a lack of the literature addressing the social and critical dimensions of ACOs and the interdisciplinary communities of practice (Brown and Duguid, 1991) that produce them – although Yim (2015) and Hui (2016) are two exceptions.

Early contributors to AI research, ACOs provide shared vocabularies that support data integration (Jakus et al., 2013) – but as semantically constructed knowledge representations (Davis et al., 1993), ACOs provide a medium for the human-centered communication of data. Building on research in sociotechnical information infrastructures (Karasti et al., 2016; Millerand and Bowker, 2009; Ribes and Bowker, 2009; Ribes and Polk, 2015), I argue that ACOs should be critically studied as products of human-centered communication – that is, not only as machine readable infrastructures for AI and machine learning but also as
products of human-centered data communication – that enable one specialized knowledge group to interact with another. Human communication is central to ontological enterprise in a way that reaches beyond technical specifications and abstract logics. Users must be able to understand the meanings produced by other humans in ontology building and in this ACOs are deeply engaged in the practice of communication.

As communicatively constituted (McPhee and Zaug, 2000; Putnam et al., 2009; Putnam and Nicotera, 2009, 2010) forms of data organization, ACOs are the product of communal deliberation, reasoning, and decision making. Ontologies are co-constituted and co-constructed and must be communicatively maintained as their upkeep depends on groups of different editors and users. Bowker et al. (2010) highlight the role of such editors and users alongside technological and philosophical specifications since “who’s in charge of crafting the ontology remains at stake” (p. 102). The notion of community is central to understanding ontologies as constituted artifacts; ontology work involves “taking knowledge out of a closed community of practice and allowing for its reuse and reshaping by others in different fields” (p. 109). Ontology engineering is “always coupled with the background work of identifying and informing a broader community of future ontology users” (p. 110). On this point, there have been calls for greater collaboration between philosophical ontologists and computer and information scientists (Smith and Welty, 2001).

As a quintessential team science (Bozeman and Boardman, 2014), communication research in ontology construction depends on talking to researchers who are actively involved in building applied ontologies. The life of ontology building involves ontologists engaged in daily decision making and reasoning practices. To sufficiently understand ontologies as a form of communication and as the product of communal deliberation entails looking at and beyond their technological specifications to the teams of researchers involved in their construction and maintenance. Following early work in STS on science teams and ontology (Latour and Woolgar, 1979; Mol, 2003) and current research in critical data studies (boyd and Crawford, 2012; Crawford et al., 2014; Dalton and Thatcher, 2014; Dalton et al., 2016; Iliadis and Russo, 2016; Neff et al., 2017), applied ontology researchers should pay attention to the interactions among data scientists, ontologists, and their communications. Ontology development is predominantly manual and laborious – though recent research in ontology expansion has attempted to automate this task (Pesquita and Couto, 2012). Full ontology automation will likely never be possible (computers would have to achieve perfect semantic interoperability) and ontologists will continue to debate even minor rules and regulations in their ontologies, thus placing communication as central to the ontology-building process.

**Ontology institutions**

Institutions play a large role in applied ontology work, a costly and time-consuming process that requires significant resources and infrastructure. Today, applied ontology building is practiced within a variety of institutions in the Northeastern USA, with many located in Buffalo. As one researcher there put it to me, Buffalo is quickly becoming “the Silicon Valley of ontology research” (telephone interview, 2015) with much of the ontology work attached in some way to the University at Buffalo. “I think now most people would say it is Buffalo which is the most important player,” they told me – “Buffalo is probably the largest single community of people who are building, or maintaining, or using ontologies.” Buffalo has been or is currently home to many ontology research groups and centers, including the Ontology Research Group, NCOR, CUBRC’s ontology team which develops the Common Core Ontologies, used in many projects, including, for example, space research, the Center for Multisource Information Fusion, the Biomedical Data Science Shared Resource, the Institute for Healthcare Informatics, and the Division of Biomedical Ontology in the Department of Biomedical Informatics, which is the first university teaching unit devoted to ontology.
NCOR was created in 2005 with the aim of conducting ontological research by building tools and measures for ontology evaluation and quality assurance. The National Institutes of Health thought that it was important to support the Gene Ontology (a domain ontology) and similar efforts because of the importance of the Human Genome Project for medical research. The principal investigator of NCOR was Mark Musen (Musen is the creator of Protégé and currently at Stanford) and Barry Smith served as co-principal investigator. The pair thought that it would be important to have something similar for non-biomedical ontology and so they created NCOR for areas which were at that stage restricted to a small amount of military work and a larger amount of theoretical work in domain and discipline-neutral ontology work. Within a short time, NCOR moved to be fully located in Buffalo and Smith became the director. Currently, NCOR conducts work for military projects and has practiced most of its work within the military ontology research area, though it is not restricted to military projects and is still active in areas such as financial services, economics, and legal ontology. According to their website, ontologists working at the University at Buffalo participate in the center and its activities and collaborate with scientific, private, and public institutions in the USA and around the world by organizing ontology-themed research activities, conferences, publications, and funding opportunities. NCOR operates as an infrastructural hub that enables the coordination and review of organizations that use ontologies in different fields, including national defense and intelligence, management and healthcare. The center provides resources for those engaged in applied ontology by helping them find funding and establish interdisciplinary teams. It also provides consultants for ontology-related projects, particularly in security and healthcare. They engage in training and outreach that are designed to spread ontology research around the world and to include more institutions and individuals in the applied ontology-building process.

Much of the work at NCOR grew out of Europe’s IFOMIS at the Philosophy Institute of Saarland University. IFOMIS was founded in 2002 after Smith won the 2001 Wolfgang Paul Award from the Alexander von Humboldt Foundation (with additional funding supplied by the Volkswagen Foundation’s Forms of Life project and the European Commission). The Wolfgang Paul Award was granted then for the first time to 14 promising researchers. The award was worth 4.5m German marks (the equivalent of just over £2m) and was one of the most valuable research awards for a scholar at that time. It provided winners with the freedom to pursue their research projects away from administrative constraints at a German academic research institution and to create their own interdisciplinary working groups of researchers. The Federal Ministry of Education and Research financed the awards, which were made available from a federal government program that existed at the time named the Future Investment Program. In total, 14 scholars received the award (a total reaching almost £26m), and Smith was one of only two recipients from the humanities, having been trained as a philosopher. The other recipient from the humanities was a linguistics professor. Most of the awards went to individuals in the fields of physics, mathematics, engineering, and geoscience.

In the beginning, IFOMIS was established at the Faculty of Medicine in the University of Leipzig but it eventually relocated in 2004 to Saarland University in Saarbrücken to capitalize on interdisciplinary collaboration at the frontier of computer and information science research. IFOMIS set the task for itself of advancing research in ontology in the field of bioinformatics and to prove how the knowledge of analytic metaphysics and logic can be greatly beneficial for such fields. Doctoral researchers in various fields including philosophy but also medicine, linguistics, and computer science have interacted with IFOMIS and its training and research modules. IFOMIS is largely responsible for bringing about a worldwide transformation in the logical development of ontology research and have developed highly refined techniques for evidence-based applied ontology development which have spread in popularity and are now used worldwide by various well-known and
highly regarded ontology groups. The methods developed at IFOMIS led to the creation of BFO, a top-level ontology that organizes multiple domain ontologies, which is now serving as an integrating framework for a large variety of ontology projects. In 2005, Smith joined the Gene Ontology Consortium to establish the Open Biomedical Ontologies library, which later in that same year become institutionalized as the OBO Foundry, a collection of coordinated medical ontologies like the NCBO’s Biportal. Smith is still heavily involved in OBO Foundry activities and in the development of BFO principles (Smith et al., 2007; Ceusters and Smith, 2015; Spear et al., 2016). BFO is also currently undergoing a certification process with the International Organization for Standardization (ISO) as a top-level ontology for information technology.

Basic Formal Ontology

In the preface to *Building Ontologies with Basic Formal Ontology* (2015) – the official instruction manual for conducting applied ontology research with BFO – Arp, Smith and Spear write that even though they were professionally trained as philosophers, “What follows is not, however, intended as a contribution to philosophy. It is intended, rather, to form part of what we conceive as the rich, new technical discipline of ontology” (p. x). The trio describe ontology as a part of this new applied field. BFO is a small, upper-level ontology that is used for organizing domain ontologies and provides the abstract rules and grammar that organize the particulars that populate specific domain ontologies. It is one of the most widely used upper-level ontologies in existence today and is used (for example) to coordinate the OBO Foundry (Smith et al., 2007). As such, BFO does not contain any specific references to entities that would belong in domain ontology – there are no references to genes, particles, files or chemicals, but rather only abstract descriptions, qualities, and relationships. BFO is a truly formal ontology that contains only those logical descriptions that are abstract enough to satisfy the organization of domain entities and their relations. It emerged from a philosophical project which is focused on the task of providing a genuine upper ontology for domain ontologies that are used in scientific research (such as those found in the OBO Foundry).

The theoretical work which led to the construction of BFO was started by Smith in 2002 and then developed by Smith and Grenon in a series of papers (Grenon, 2003; Smith and Grenon, 2004; Grenon and Smith, 2004; Grenon et al., 2004; Neuhaus et al., 2004). Since that time, various individuals have contributed to the BFO project, many of whom are listed on the BFO project website (Figure 2), including over 100 other individuals involved in the BFO Discussion Group. Much of this work has been conducted in Buffalo, though BFO is used by over 250 ontology-driven projects throughout the world. Some of these include the

![BFO Basic Formal Ontology](https://example.com/bfo.png)

*Figure 2.* The Basic Formal Ontology (BFO) website and BFO in the ontology-editing Protégé software

Source: Screengrab by Iliadis (2018) and http://basic-formal-ontology.org
Alzheimer Disease Ontology, Adverse Event Ontology, Actionable Intelligence Retrieval System, Bacterial Clinical Infectious Diseases Ontology, Bank Ontology, Beta Cell Genomics Application Ontology, BioAssay Ontology and the Bioinformatics Web Service Ontology, among many others. A complete list is available on the BFO project website.

BFO is “lightweight” compared to other upper-level ontologies, meaning that it is purposefully abstract and minimal enough in its definitions of physical entities and relations to enable widely successful domain ontology integration. BFO’s top-level category entity is divided into two main categories called continuant and occurrent which are intended to stand for entities that continue to exist through time (continuants) or entities that unfold themselves in time (occurrants). Continuant is subsequently divided into three categories called generically dependent continuant (things like qualities and functions), independent continuant (things like you and me) and specifically dependent continuant (things like the geospatial regions that things occupy). Occurrants have four subtypes that include process (something that unfolds), process boundary (the thresholds at the beginning or end of processes), temporal region (the time in which processes occur) and spatiotemporal region (the space where processes occur). These are then further broken down into subtypes of boundaries, regions, and objects (see Figure 2). More information about these categories, including their definitions and rules for application, can be found in the BFO manual (Arp et al., 2015).

As mentioned previously, BFO’s method serves as the top-level instructional basis for organizing a series of domain-specific subontologies. The idea is that if a group of data sets describe their data in a hands-off way by constructing an ontology that uses BFO then those data sets can be combined or grouped together in an interoperable and semantically enhanced way, leading to knowledge synthesis and, ideally, scientific progress. The main outcome of this approach – organizing multiple subontologies using the BFO method – is that portions of reality can be partitioned and aligned according to various levels of informational granularity and abstraction. Entities at one level or domain may be aggregates at a different level or domain, each part (or set) a piece of one large ontological puzzle. BFO individuates entities using a so-called “realism-based” approach as far as the entities to which BFO refers are assumed to exist (according to empirical science). In this, BFO runs counter to the historically accepted definition of applied ontology as “an explicit specification of a conceptualization” (Gruber, 1993b, p. 908). The term “conceptualization” is avoided by BFO developers, who generally argue in favor of a “realist orientation” over a “concept orientation” (Arp et al., 2015, p 7), following the recent paradigm shift in health informatics (Schulz et al., 2013). Their reasoning for this is that BFO should be useful for organizing data in domains of empirical science (that refer to entities that exist) to increase the semantic intelligibility of data (when they become interoperable with other data). Yet, BFO ontologists do not deny the existence of abstract entities. In lieu of the language of “concepts,” authors and practitioners of BFO (at NCOR) have developed an adjacent, BFO-supported domain ontology called the Information Artifact Ontology (IAO). The IAO is a similar, realism-based approach (Ceusters, 2012) to domain ontology for accurately representing information entities “like protocols, databases, experimental logs, published literature, and so forth” (Arp et al., 2015). I spoke to one ontologist about IAO who said they created it once they “started to think very seriously about what data and information actually is and how it relates to reality. We needed to give a good ontological description of what elements contribute to data and information and so on. That’s the part of the information artifact ontology” (telephone interview, 2015).

Information content entities in IAO are a subtype of BFO’s generically dependent continuant and are an attempt at solving the problem of how to best describe the ontological status and organization of informational objects and abstract artifacts. Hui (2016) provides a comprehensive account of this problem while outlining the philosophical distinctions
between formal (upper) and domain ontology, focusing specifically on “objects that take shape on a screen or hide in the back end of a computer program, composed of data and metadata regulated by structures or schemas” (p. 1). As one ontologist described it, a domain ontology about abstract (mostly digital) information entities like the IAO is an attempt to address information artifacts like databases, publications, footnotes, protocols and so forth, that exist in “biomedical investigations, physics experiments or reports about human intelligence observation of people moving around in the backstreets of Baghdad” (telephone interview, 2015). BFO ontologists decided to create IAO with the idea that people were seeing information as a “kind of jelly” – they wanted to focus on the information artifacts which were always created by human beings without getting bogged down by philosophical issues such as “Is the genome an information object?” They wanted to think about boring things like publications, databases, receipts, bills, orders, licenses – items that are used in the process of carrying out an experiment. NCOR were thus “forced to add a new branch to BFO in order to deal with information artifacts,” and so they created BFO 1.1 (telephone interview, 2015). BFO’s current version is 2.0 – so far, there have been three versions. BF0 2.0 is a tidied-up version of BFO 1.1. The ambitious goals that NCOR had for BFO 2.0 have now been postponed for BFO 2.1.

Apart from the kinds of informational artifacts represented in IAO, representing socially constructed entities has also proven to be a complex part of the ontology-building process. How exactly are social entities (things like names and roles) defined in an ontology and what is their status? What are the specific methods and conceptual frameworks used to identify them? BFO identifies such topics as fiat entities, which Smith (2001) describes as boundary objects owing to acts of human decision. In the same way that there are “real” entities that exist (so-called bona fide entities), fiat entities exist equally according to logically veridical measures. On BFO’s theory:

Each true empirical judgment can be seen as effecting a division of reality in fiat fashion in such a way as to mark out a certain truthmaking region consisting of those entities that are relevant to the truth of the judgment in question. Truth itself can then be defined as the relation of correspondence between a judgment and its corresponding truthmaking region, in such a way that a true judgment would be something like a map of the corresponding portion of reality. (Smith, 2001, p. 140)

For example, one may think of a chart displaying cuts of meat or a map of the USA. Both representations refer to specific entities that are partitioned by fiat, and such fiats are tied to empirically true observations of the reality of those entities. Statements about “chuck” as fiat object corresponds to an empirical boundary in the cow, in the same way that “Indiana” as fiat object is tied to an empirical boundary in the USA. According to Quine, all that is necessary (for fiats) is that a theory “is committed to those and only those entities to which the bound variables of the theory must be capable of referring in order that the affirmations made in the theory be true” (1948, p. 33). BFO ontologists reference and view Quine as responsible for providing an ontologically rigorous account of these sorts of fiat objects. Statements about the fiat objects chuck and Indiana, as they exist in an applied ontological framework, need only refer to the relation of correspondence that is established in the empirical observation of their portions of reality. BFO’s brand of computational ontology is responsible for partitioning reality into such fiat levels of granularity and abstraction. In this way, reality is presented as structured, and data can be parsed using the methods of applied ontology. In BFO, social ontological categories might be identified by fiat object (something like a state), fiat spatial boundaries (something like the equator), fiat processes (something like a century) and fiat temporal boundaries (something like a season). Fiats, for example, would include domain data about things like roles and money. Figure 3 shows information about the role fiat in BFO’s syntax, expressed in the Web Ontology Language (OWL).

The application of social ontological fiats to data entities might be deserving of questioning in the context of ACOs. Such entities, such as roles, can change regularly, and
who collectively is responsible for designating roles remains at stake. In response, BFO embraces what has been referred to as the “ontological traffic law principle.” Ontological standards “are indispensable to every successful large-scale ontology development initiative, and this is so even if they are selected arbitrarily provided they enjoy widespread assent among those working in the relevant research community” (Smith and Ceusters, 2010, p. 182). Emphasis is placed on the widespread adoption of fiat terms, leaving less room for consideration about how fiats may be arbitrarily, mistakenly, or mischievously applied. There are other benign and arbitrary rules reflected in BFO such as the “law according to which all terms within an ontology should be nouns and noun-phrases that are singular in number” (Smith and Ceusters, 2010, p. 182). Smith defends the existence of common fiat entities in that “there are still too many clear examples of fiat and bona fide objects at given levels of granularity that the dichotomy itself to be dismissed as spurious. Mesoscopic physical objects (people, walls, items of furniture) do not merge continuously into each other. Political and administrative units do not in any sense exist as a part of the physical substrate of reality, but rather only as a product of our fiats” (2001, p. 146). Yet, there are those in the ACO community who debate the ontological status of fiats and ontological realism in general. Many scientists and engineers still take sides in the realism vs conceptualism debate, and there are a variety of blogs that discuss this issue. The blog OntoGeek (https://ontogeek.wordpress.com/) contains a series of posts on applied ontological realism with titles such as “Realism, Really?” and “Yes, really” (OntoGeek doubled down on realism). Other blogs contain views against realism, such as those expressed in An Exercise in Irrelevance’s (www.russet.org.uk/blog/) post “Why Realism is Wrong.”

**Debating ontologies**

Getting ontologies to succeed is a difficult problem that requires many users. One ontologist explained to me that they think of the term “success” in ontology work in the following way. Suppose that you are building a telephone network for a country and you have fantastic hardware and a fantastic way of keeping track of telephone numbers – but there are not more than three subscribers. This would not be a successful telephone network. Success for ontology is, to a large degree, a function of the number of users. BFO has been used by over 250 different ontology groups. 100 or so are biomedical and there are some groups in different areas who are applying BFO to topics such as financial services, developmental
nanotechnology, or military projects. In that respect, BFO is by far the most successful ontology in that it has the greatest number of users.

Individuals involved in massive group operations in ontology building, like those at NCOR, must communicate with each other while sometimes being in different geographic locations. A close look at such groups and their communities of practice illuminates the methods through which decisions are made and discussions are conducted. In the case of BFO, the public material that has been generated by the community that has formed around applied ontology shows that there is a degree to which rhetorical appeals play a productive role in the communication, formation, and maintenance of BFO methods (Gooch, 1975; Depew and Lyne, 2013). The BFO community uses a variety of tools and techniques to maintain contact, including technologies such as Google Groups and other forms of online social networking. The BFO Discussion Group is one such community (Figure 4) where members involved in the day-to-day activities of BFO participate and discusses issues concerning methods, implementation, editing, and infrastructure. There are currently 624 topics in the BFO Discussion Group which effectively act as problem-solving message threads that contain individual messages. The group started in 2006 to provide a space to enable groups of researchers interested in ACO a home to work through some of BFO’s theoretical and methodological problems. The group has been the main method of contact for individuals involved in construction and use of BFO.

Within such groups, members discuss the terminologies that must be adopted by BFO, including borderline cases in the natural sciences, but also how various types of documents are to be represented in BFO (Smith, 2014; Almeida et al., 2012). For example, users discuss things like how a digital document like a prescription should be referenced in BFO. The BFO Discussion Group allows for debates to be aired openly and in public so that input can be received from any individual. For example, on top of debating the ontological status of scientific entities in fields such as biomedicine, members of the group have debated document types (virtual digital artifacts and virtual transactions) and how such artifacts should be represented in BFO, including forms, templates, memos, but also things such as entire archives, protocols, amendments, dates, maps, photographs, and diagrams. They also discuss what can be done to documents, including things such as stamping, approving, canceling, and filing. BFO Discussion Group members debate how to include things such as funding data and legal actions in the ontology, and things like errors, forgeries, and invalidity. Institutional systems and entities such as government agencies and nongovernmental organizations must also be capable of being represented by the ontology.

In the example given in Figure 4, a user asks “Do OBI: physical_entity and material_entity belong under snap:object and immaterial_entity under snapsite?” The question concerns how BFO functions once it is populated by the content of another ontology, which in this case is the Ontology for Biomedical Investigations (OBI). Complications can arise in the translation of terms from OBI to BFO. A user asks whether

Source: Screengrab by Iliadis (2018) and https://groups.google.com/d/forum/bfo-discuss
“obi: population is_a bfo: object_aggregate” to see if the translation from OBI to BFO principles is correct. Such a translation of an existing data ontology into more abstract terms of categorization may potentially undermine the existing data structure, especially if the individuals who originally defined the data are not present to interact and discuss translation rules before integration. Similarly, in a threaded discussion that runs from February 4, 2013 to April 25, 2013, members of the BFO Discussion Group argue over the definitions of processes and entities. Combing through the vast archive of publicly available material on the list, I saw numerous examples where members of the group engaged in heated dialog with one another on some of the basic principles of ontological realism. For example, in a post from February 24, 2007, senior ontologists intervene in a debate that was happening in the discussion board to clarify mistakes concerning philosophical principles in boundary logic.

Members of the BFO Discussion Group participate and attempt to answer questions about ontological realism as they come up from a variety of users around the world. Such a group represents a subset of the ontology research community, one that has formed around a specific subject (BFO) using a specific technology (Google Groups) to facilitate community action. As an example of scientific culture forming online, tools like the BFO Discussion Group facilitate what Latour and Woolgar (1979) have referred to as the “arguments and beliefs to which there is a constant appeal in daily life” of scientists (p. 55). The BFO Discussion Group acts as a venue to extend dialog around issues, providing space for arguments to be made and belief systems to be expressed, that can potentially affect how BFO works or how it is perceived. BFO, and ontologies in general, are open to revision. For example, in another message, an ontologist attempts to reason with the group to explain why boundaries should be considered independent continuants and how they should be included in BFO. A user asks “How can a boundary of an object be an independent continuant? Surely it intimately depends upon the thing it is the boundary of?” Another user answers that “The boundary can exist even if the thing it is a boundary of doesn’t. For instance, think of a ball. We can define a sphere which is its boundary. But even without the ball we can think of the same sphere.” Another user chimes in: “The boundary is at any given time coincident with a certain sphere. But it is not identical with the sphere, any more than you are identical with the [...] shaped region of space you happen to occupy at any given time.” Such exchanges show that BFO is subject to debates and questioning that can potentially affect its methodology or how users apply the BFO method, and this suggests that there is at least some degree of rhetorical force involved in the construction and communication of BFO itself in terms of its scientific principles (Gooch, 1975).

There is also evidence of some tension between different ontology groups and users regarding the languages that are used to express BFO principles, such as OWL. As one scientist related the following to me (telephone interview, 2015):

I refuse to collaborate in any way on attempts to express ontologies by means of OWL. I won’t do it and I don’t take any responsibility for what is there. An example is, for instance, the Ontology for General Medical Science (OGMS). I am one of the coauthors of the paper where the definitions, the descriptions, and the axioms were given for what became the OGMS. But I disagree with how OGMS is represented in OWL, simply because OWL is not expressive enough to really be able to express everything that is important if you want to have a good description of first order reality.

OWL is used rather extensively in the construction of ACOs, yet the ontologist related that OWL is built on the assumption, adopted by many computer scientists, of “bullshit in, bullshit out.” I assume that what the ontologist meant by this was that many technicians involved in ontology work do not see the ToB problem as being their niche problem, and that they would rather produce ontologies that work, and that can “consistently reason with bullshit” – as the ontologist added. Such individuals call themselves ontologists, according to my ontologist, but do not pay attention to semantics. According to my ontologist, the
logic goes something like: “Yeah, well, but there is nothing better for the time being, and at least you can say some things in OWL, so then it is better to be able to say something than nothing at all.” My ontologist says they are more principled in the sense that they refuse to work on a solution which cannot be perfect.

I then asked what areas they thought needed the most attention in ontology work. What areas need more development and research? The first thing, they said, is that there are different levels – the basic principle of referent tracking is that anything you want to say something about should be uniquely identified, but this principle is not widely adopted. It is adopted for a few things like patients who get unique identifiers, doctors organizations, and x-ray machines, but not much else. The ontologist’s claim is that everything that you want to say something about should first be given a unique identifier, but not before checking to see if someone else has already created one. If you are sure that nothing has been said about what you want to describe then you assign a new unique identifier, a principle that needs to be there. Second, the ontologist thinks that all ontologies should take consideration of the dimension of time more seriously (telephone interview, 2015):

It is nonsense to come up with statements like “all humans have a heart”, because that’s not true during heart replacement surgery. Or that all humans have two legs. Look at the street. So those things should just not be said like that. You should at least specify a certain type. You should say that whenever there is a human leg, it has been part of some human being at some time, but it might have been cut off. So those kind of statements, I think that’s important. Assertions, which, both in ontologies as in individual statements, take the time elements seriously.

Other ontologists are slightly less critical of OWL. One explained to me that first-order logic is not, from a computational point of view, ideal. If you have an ontology which is using first-order logic, it will often not execute queries – the computer will not be able to result queries in a reliable way. The computer will not be able to reliably execute queries, not because the computer will create false results, but because the computer will never end its process of trying to work out what the results might be – it will take an infinite time. In consequence to this, the military and other agencies have been working on trying to find fragments of first-order logic which will execute reliably. The current preferred fragment of first-order logic is OWL, one of whose founders is Tim Berners-Lee. Berners-Lee founded OWL as a part of the Semantic Web to create a version of the web which would enable kinds of search, combination, comparison, and reasoning through metadata. OWL is today the default language of choice for ontology work. OWL’s expressivity is weak, but its computable properties are good. One ontologist told me that there are features of BFO which they would like to be able to express using OWL, which they cannot. There are some things that can be expressed easily using first-order logic which cannot be expressed easily using OWL. The tradeoff is that researchers involved in BFO do not want to create a BFO which no one will use because it is too complex, and so they are trying to find a way of resolving this issue. Keeping BFO simple, keeping its capacity to deal with time, which is where the problems primarily arise, but without sacrificing the computational qualities that OWL provides.

BFO ontologists at NCOR are now attempting to make people take the view that BFO exists in different forms. There is an OWL version, there is a first-order logic version, and there is also an English language version. All these versions have their good qualities and their bad qualities, and all of them should be kept alive, and will be kept alive, one ontologist said. They should be kept alive in such a way that the three versions are compatible as far as they can be. But because OWL has weak expressivity, there will be parts of BFO that cannot be expressed in OWL. OWL is like the alphabet (A, B, C, D...), while BFO is like, and, or not, thing, process, adjective. BFO is the next level of structure after the alphabet. There is some structure in OWL, but it is not a competitor to BFO. “Some people think that if you have an artifact which has been built using OWL then you have an ontology,”
one ontologist said. “I think that in order to have an ontology which is useful for anything, you need a lot more than just a piece of correct OWL code.”

The BFO Discussion Group is not “official” but is rather an informal ad hoc community formed around a recognized need to provide support to the ontological realist project. Like the many other historical ontology discussion groups noted by Yim (2015), the BFO Discussion Group is the latest iteration in a line of communities that has formed around the practice of applied ontological engineering on the internet. Such virtual communities (Rheingold, 1993) contribute to transparency and add to the overall value of the realist ontological project by enabling individuals direct access to knowledge bases and specialists whom they might not have access to otherwise. Historically, such groups are familiar in the early development of emerging technologies – the internet and e-mail being just two examples. Similarly, as Yim (2015) has shown, ontology work since the 1990s has embraced a somewhat inclusive and community-oriented nature owing to the large amounts of interdisciplinary resources that are required of applied ontology work. There is a certain sense in which applied ontology work does not fall under any specific domain and that it is the result of numerous forces of activity and specialized knowledge that form in ad hoc communities.

The openness and community-centered work of BFO ensures access and increased accountability in the ecology of information and the sharing of ontology resources, commentary, and critique (Christen, 2009). The BFO Discussion Group represents the type of shared community actions that coalesce around problems in the application of ontology. What is interesting to note is the sheer number of individuals who are involved in the discussions and decision-making process. BFO’s original creators are engaged in discussion regularly, as are numbers of regular engineers, computer scientists, even other philosophers. The discussions are often illuminating and provide a snapshot of the rhetoric that ontologists engage in when arguing about ontological realism and its principles, suggesting that there is a degree to which scientific rhetoric (Depew and Lyne, 2013) plays a role.

Social ontology
I want to end by addressing the status of social entities in BFO and what some of the consequences of this might be for future data subjects. A type of fiat object, BFO treats social artifacts, represented as nouns, as universals – things like dollar, meter, traffic law, organization, mortgage contract, etc. It also includes roles as externally grounded realizable entities. A role may be something like a student or a subject of a clinical trial. An entity may have a role in BFO because of something that happens or obtains externally – for example, a student is enrolled in a school. As BFO designers put it, a role “is a realizable entity that is possessed by its bearer because of some external circumstances (e.g. the bearer has been assigned the role by some other persons, who have roles of their own which grant them a certain authority). A role is thus always optional; the bearer does not have to be in the given external circumstances” (Arp et al., 2015, p. 99). More recently, entities like quality, role, disposition, and function have been described by BFO experts; following “the ontological realist view, instances of universals in each of these categories exist in reality and are studied by science” (Spear et al., 2016, p. 105). Yet, importantly, “roles are always optional” (p. 112). It is my position that such social ontological categories as roles lead to potential ethical issues that may appear in the application process when they are applied to human beings. For example, what kinds of social data will be integrated using the role fiat, and did the data subjects anticipate or consent to such semantic enhancement and the future integration of their data with other data sets? Would harm come to data subjects due to such unanticipated data harmonization?

Thinking of social ontology, I raised the issue of ethics in applied ontology with one ontologist and he concluded that ethics in applied ontology work can be approached at two levels. At the technical level, if one were to look at an ontology as being the
representation of the shared understanding of the meaning of a thing, among members of a given community, in a way that can be processed by both humans and machines, then ontologies can be viewed as ethically neutral. The question is analogous to asking: “Are there ethical problems in applying logic?” or even “Are there ethical problems in applying statistics?” Yet, on another level, like all applications of technology made by humans, these are almost bound to be ethical issues – the more powerful the technology, the more issues will likely exist and need to be addressed. This will be analogous to asking: “Are there ethical problems in applying laser technology?” or “Are there ethical problems in applying bio-technology?” or even “Are there ethical problems in developing artificial intelligence?” The key word is “applying.” What is the application? Who is applying? How is it applied?

What, then, are some of the potential ethical issues associated with ACOs in terms of social ontology? BFO has been applied in areas outside of the natural sciences, in fields such as military intelligence, social planning, and economics, where arguments appealing to the universality of ontological realism might create problems when users misapply (or mischievously apply) BFO methods to social data. I argue that ACOs should be subjected to ethics reviews when they are used to integrate heterogenous data sets that concern such social data. More specifically, below, I outline five “ontology troubles,” adapted from Pulsifer and Brauen (2017):

1. Ontologies process social data: ACOs make claims about the social world and have real consequences for people. We need to understand how these claims are made and what they mean. What new forms of power and power asymmetries are created in the construction and maintenance of ACOs?

2. Data subjects are unaware of ontologies: we do not know when our data are being harmonized and made interoperable with other data sets. ACOs are largely hidden and operate in the background of data interoperability projects and technologies. There is a need to spread education and literacy of ontologies.

3. Lack of consent in applied ontology: there are few mechanisms in place to provide opt-in or opt-out options for data subjects whose data may one day be amalgamated with other heterogenous data sets. How can we reconceptualize the autonomy of data subjects considering applied ontological practice?

4. Ontologists do not conduct ethics reviews: ontologists argue about logic but seldom about ethics. This needs to change. In their application, ACOs enable data integration through labeling. Labels need to be accurate and, more importantly, they need to avoid misidentifying social entities and causing harms. Thus, ethics reviews would be helpful in the design and application stages of ACO work.

5. Harm in normative social categories: social context is unsatisfactorily accounted for in applied ontology research. We need to have conversations about ontology in context, particularly around what a push for normative (or universal) social categories might mean for data subjects who do not identify in a single way.

Paying attention to such ontology troubles might be useful in considering computational ontology work since ontologies are applied in a wide variety of contexts, including social, governmental, commercial, and political contexts. Further, there are many circumstances where multiple contexts can exist at once while overlapping. For example, in a military context, there may be social entities related to government, commerce, and science. Emphasis should be placed on the idea that each context can be present at once – ontologies as technologies of individuation span contexts. Rather than focusing on one domain, computational ontologies must be scrutinized in the many domains of application in which they are found.
BFO principles are being used to create globally unified ontology standards in intelligence for entities such as the USA Military, the Central Intelligence Agency, and other intelligence agencies (Figure 5). I spoke to one ontologist about their work with the military—“The area where I’m probably being most influential now is military intelligence.” The ontologist worked on projects for the Intelligence and Information Warfare Directorate which consisted of an attempt to address the following problem. There is a large amount of data, for instance data pertaining to terrorists or something similar. These data come from many kinds of sources. Some are human intelligence data, some of are signals intelligence data and so on. The intelligence analysts must use these data to answer questions and there are various rules they use to get answers to questions. Typically, each intelligence analyst will understand the structures of the databases that he or she must work with only superficially, except for a small number of databases, where they are experts. Intelligence analysts thus have good access only to a small fraction of the entire data available and do not have a quick way of gaining access to all the rest. This is a simple kind of problem and the reason for it was because the data in all those databases were described in different ways. The introduction of BFO to create the military ontology was a solution.

Several ontologies, like the military ontology, that use BFO contain entities that express what has been referred to by Searle (2006) as social ontology. Social ontology seeks to

**Figure 5.** The Military ontology website

*Note:* Top: early version of the BFO-powered military ontology; bottom: the military ontology as it exists today

provide the invisible structure of social reality – things like institutional facts, social phenomena, and social facts. Searle (2006) writes that social ontology “is both created by human actions and attitudes but at the same time has an epistemically objective existence and is a part of the natural world” (p. 12). Some of the fundamental concepts needed to explain the existence of social ontology include: the notions of collective intentionality, the assignment of function, and constitutive rules. Perhaps the most important notion is that of status functions in institutional ontology, which Searle (2006) describes as “the glue that holds society together because they create deontic powers, powers that work by creating desire-independent reasons for action. Thus, social ontology locks into human rationality” (p. 12). If the ontological realism endorsed by BFO is dependent on the universal laws and structures of science, social ontology is dependent on the invisible rules and laws that society follows – the former individuates scientific entities (natural kinds) while the latter individuates social entities (social kinds).

BFO follows social ontology and has continued the practice by describing institutional systems to which documents belong, positional roles within such systems, and the production of documents. The entities represented by social ontology are certainly real in the sense that they carry purpose in the world and exist as actual entities (there are things like presidents, mothers, deeds, decrees, documents, and so forth). Yet, social kinds are said to be different from the natural kinds produced by science in that they are subjective and depend on mental attitudes (Searle, 1995) – social kinds are interactive and malleable. It is here where social ontology gets tricky, particularly in applied forms such as the BFO-powered Military Ontology, which depends on the ontological realism presented in BFO while identifying entities that belong in the realm of social kinds. What I argue is that the BFO methodology (and others like it) need to be ethically analyzed when applied to the types of data that belong to the realm of social kinds.

The Military Ontology was built in response to a Chairman of the Joint Chiefs of Staff Instruction (CJCSI) referring to “horizontal integration of warfighter intelligence” (Smith et al., 2012). The CJCSI’s mandate to integrate intelligence databases resulted in the application of BFO to social and governmental data, yet there has been no review of the BFO methodology when applied in social ontology contexts. The social ontology practiced in the Military Ontology depends on the scientific methodological realism of BFO, yet such methods call for additional ethical analysis when applied to the types of data that belong to the realm of social kinds. For example, “Femur is_a Bone” is a typically uncontroversial standard definition in scientific ontologies using BFO. An example such as Mohamed is_a Key Leader is a definition that carries additional political and social weight as the product of collective intentionality and fiat. Such social ontological commitments should be subject to ethical review when expressed in ACOs like BFO. That “Femur is_a Bone” should be uncontroversial in an ontology using BFO in that this is a universally true statement and not contested. But “X is_a Key Leader” in wartime is obviously not the same type of statement, in that it is not universally true and is the product of collective intentionality and fiat. Such social ontological commitments should be subject to ethical review when expressed in computational ontologies that then integrate social fiats with vast troves of additional data for knowledge extraction and intelligence.

Conclusion
This paper has served as a springboard into the qualitative and critical study of ACOs. It has discussed the infrastructure and communities that inform BFO to both provide an example of how to study ACO’s and to show how BFO contributes to science. A final task was to show how BFO is used in projects that practice social ontology – like the Military Ontology. This is only one example of an ACO being used in domains that deal with social data. And BFO is only one upper-level ontology; there are others.
In domains, ACO’s should be studied by qualitative and critical researchers and their potential ethical impact must be evaluated.

In concluding, I should say that there seems to be a direct connection between philosophical ontology and computational ontology. BFO’s ontological realism works, as proven by its widespread use – communities of practice are important to shaping BFO. BFO is also applied in social, governmental, and other contexts. This is significant because ontology has influenced scientific knowledge production and changed scientific practice and communication. Ontologies are a new way to communicate data. Researchers should plan to refine the theory and developing case studies to discuss the ethical impact of ACO’s that operate in various contexts. Communities that form around ACO’s like BFO observe what Slayton (2013) describes as disciplinary repertoires, “the quantitative rules, codified knowledge, and habits of problem solving that enable experts to structure, estimate, and quantify uncertain technological futures. Disciplinary repertoires allow experts to rhetorically distinguish subjective, politically controversial aspects of a problem from putatively objective, technical realities” (p. 2). Such disciplinary repertoires are clearly visible in ACO’s like BFO when they are used in scientifically individuating social reality and the individuals who make it up. The move of labeling realism-based ontology as a purely scientific problem can potentially ignore the ways in which technologies of individuation stand to impact everyday social life.

References


Hui, Y. (2016), On the Existence of Digital Objects, University of Minnesota Press, Minneapolis, MN.


Kitchin, R. (2014), The Data Revolution Big Data, Open Data, Data Infrastructures and their Consequences, Sage, Los Angeles, CA.


**Corresponding author**

Andrew Iliadis can be contacted at: andrew.iliadis@temple.edu
Abstract

Purpose – Traditional public health methods for tracking contagious diseases are increasingly complemented with digital tools, which use data mining, analytics and crowdsourcing to predict disease outbreaks. In recent years, alongside these public health tools, commercial mobile apps such as Sickweather have also been released. Sickweather collects information from across the web, as well as self-reports from users, so that people can see who is sick in their neighborhood. The purpose of this paper is to examine the privacy and surveillance implications of digital disease tracking tools.

Design/methodology/approach – The author performed a content and platform analysis of two apps, Sickweather and HealthMap, by using them for three months, taking regular screenshots and keeping a detailed user journal. This analysis was guided by the walkthrough method and a cultural-historical activity theory framework, taking note of imagery and other content, but also the app functionalities, including characteristics of membership, “rules” and parameters of community mobilization and engagement, monetization and moderation. This allowed me to study HealthMap and Sickweather as modes of governance that allow for (and depend upon) certain actions and particular activity systems.

Findings – Draw on concepts of network power, the surveillance assemblage, and Deleuze’s control societies, as well as the data gathered from the content and platform analysis, the author argues that disease tracking apps construct disease threat as omnipresent and urgent, compelling users to submit personal information – including sensitive health data – with little oversight or regulation.

Originality/value – Disease tracking mobile apps are growing in popularity yet have received little attention, particularly regarding privacy concerns or the construction of disease risk.

Keywords Surveillance, Privacy, Mobile apps, Data, Disease tracking, Surveillance medicine

Paper type Research paper

Introduction

Imagine waking up in the morning and, along with the day’s weather and breaking news, you get an update about your risk of contracting a contagious disease. It warns you about which illnesses are prevalent in your neighborhood, just as a weather forecast might tell you it is warm and sunny with a chance of afternoon showers. A live map warns when you enter a “zone of contagion,” or when a sick person draws near; a numerical score corresponds to your calculated risk of becoming diseased. This is not a vision of the future: it is today’s technology.

The app and website Sickweather – a so-called “Facebook for hypochondriacs” – collects information from social media and across the web, as well as self-reports from its users, so that people can see who is sick in their neighborhood. In 2011, the site reportedly detected an outbreak of whooping cough two weeks before public health officials (Miller, 2014).

As the Sickweather website proclaims, “Just as Doppler radar scans the skies for indicators of bad weather, Sickweather scans social networks for indicators of illness.” The app identifies “sick zones” and helps “keep you and your family safe” with its SickScore, an estimation of your current risk of contracting disease[1]. A future version of the app will allow users to see which of their friends are talking about being sick on Facebook or Twitter (Kotenko, 2013). Surprisingly, few concerns have been raised about potential privacy infringements, or the capacity for Sickweather to panic a public already primed by the media to overreact to news of contagious diseases (Greenberg, 2014;
SteelFisher et al., 2015). Caduff (2014) describes how tools such as Sickweather contribute to a “networked communication environment of contemporary ‘epidemic intelligence’” and questions whether this results in an “inevitable condition of incomplete information” that “creates a chronic desire for more information” (pp. 39-40).

This paper explores digital disease tracking tools, focusing on platforms that depend on contributions from networks of users, or “crowdsourcing.” For health- and fitness-related apps and websites, there are concerns around privacy and surveillance, with little oversight or regulation surrounding the collection, storage, transmission and ownership of personal information (Helm and Georgatos, 2014; Huckvale et al., 2015). Google’s company DeepMind, which specializes in developing artificial intelligence, recently announced that it was working with the National Health Service (NHS) in England to build an app called Streams that will be able to help medical professionals monitor kidney patients. DeepMind’s foray into medical databases has raised much concern. Rather than focusing on a few thousand patients with kidney injuries, which many had assumed would be the case, the company is accessing the NHS records of 1.6m patients who use three hospitals run by the Royal Free NHS trust. The records include information from the patients’ medical history such as HIV status, drug overdoses and abortions, alongside logs of day-to-day hospital activity including records of the location and status of patients, who visits them, and real-time data and historical records from critical care and emergency departments. DeepMind claims that it needs access to the entire patient database to produce accurate medical alerts and potentially diagnose diseases sooner. Yet many are concerned that DeepMind’s database could allow for much more than the original stated purpose. Further, with these data being controlled by one of the largest companies in the world, there are fears that Google could quickly establish a monopoly over health analytics (Shead, 2016; Kopstein, 2016).

Overview of disease tracking apps: past to present
Sickweather is far from the first digital disease surveillance tool: perhaps the most well-known is the now-defunct Google Flu Trends, which tracked users’ search terms and other online activity to “nowcast” the flu – essentially, forecasting the flu the same way the weather is monitored – based solely on people’s searches. When people are sick, many of them search for flu-related information, which can supposedly be used as a proxy for overall flu prevalence or spread. When combined with information from the Centers for Disease Control and Prevention (CDC), accurate estimates could be provided up to two weeks earlier than using CDC data alone (Lazer and Kennedy, 2015). Yet by 2013, Google Flu Trends, as many media outlets reported, had “failed spectacularly,” over-predicting the prevalence of the flu by more than 50 percent. The so-called poster child of big data approaches to disease tracking had come up short. Google’s algorithm did not properly account for certain seasonal trends in search query volume, and it did not account for changes in search behavior over time. This was foreshadowed in October 2011, when Flu Trends data were notably skewed due to pop singer Rihanna tweeting about having the flu, leading to a spike in search queries from fans who were curious about the celebrity’s health (Lazer and Kennedy, 2015).

Since the rise and fall of Flu Trends, other disease tracking apps and services have been introduced, in many cases supplementing their algorithms with “small data” approaches (more traditional epidemiological methods, surveys, health reporting and so on) to avoid the failures of Google’s early attempt at disease tracking (Lazer et al., 2014). An example of a “big data success story” is HealthMap – an online system created by researchers at Boston’s Children’s Hospital – which collects and analyzes information from a variety of platforms, including social media, online news and travel sites, to provide early detection and surveillance of disease outbreaks. The creators say that the primary goal is to provide
real-time data on emerging infectious diseases to agencies and international travelers, noting that although such data are already abundant, it is typically “unstructured, unorganized, and untapped,” and thus infections from a new disease outbreak might be initially overlooked as separate, unrelated incidents (Nelson, 2008, p. 596). They hope that by combining data from a broad range of sources, such outbreaks can be detected more quickly and reliably. HealthMap made headlines in 2014 for detecting references to Ebola infections from local newspapers in Guinea, more than a week before government authorities in the country informed the World Health Organization about the outbreak (Gilpin, 2014).

Even earlier, the Global Public Health Intelligence Network provided alerts about the Severe Acute Respiratory Syndrome outbreak in 2003 (Mykhalovskiy and Weir, 2006). Yet in contrast to these previous tools, which involved collaboration with public health organizations such as the CDC and the WHO, Sickweather was not designed as a public health tool but is instead geared toward individual use; it commodifies disease tracking, packaging it into a commercial app on the iTunes and Google Play Store. It skips the “middle man” of institutionalized health authorities and speaks directly to the consumer/patient. Unlike HealthMap, the Sickweather app and website displays maps that mark off the location of users who have self-reported symptoms, allowing people to move down to street level to see who is sick in their neighborhood. Further, users can opt to connect the Sickweather app to their Facebook and Twitter profiles, to find out which of their friends are sick based on their social media posts (Kotenko, 2013). In other words, it is not possible to opt out of the network: if one of your Facebook friends or Twitter followers uses Sickweather and you post a status update about being sick, you have automatically participated in this disease tracking assemblage.

Crowdsourcing and peer production
Crowdsourcing projects can be viewed as examples of how communication networks have the capacity to empower people, fostering self-governance and democratic, community-based peer production (Benkler, 2006; Castells, 2007; Jenkins, 2006). As a business practice, crowdsourcing has been positively framed as a method for capturing user-driven innovation, allowing for a more fluid and responsive relationship between a business and the users of its product that also substantially lowers labor costs, by offloading at least some of the costs of problem solving and production onto the consumers of the product (Busarovs, 2011). Many government agencies and organizations are attempting to draw on crowdsourcing “to enhance democratic engagement, improve service delivery, collaborate across organizations, and communicate with stakeholders and the public,” and in these contexts, crowdsourcing tools may help improve access to information and facilitate public debate and engagement (McNutt, 2014). Yet others have argued that notions of “presumption” or “consumption labor” are attempts to mask the exploitation of labor and acceleration of capital accumulation through rhetoric that merely sounds democratic and collaborative (Fuchs, 2013; Kleemann et al., 2008).

Selection of apps for study and research question
HealthMap and Sickweather were selected for study, as the former is a prominent example of a public health tool that uses big data to track contagious diseases, while the latter is a commercial product that uses crowdsourcing (among other methods) to identify disease threat.

This paper examines both Sickweather and HealthMap, guided by the following research question:

**RQ1.** What are the privacy and surveillance implications of using these (increasingly prevalent) digital disease tracking tools?
Methodology
The walkthrough method (Duguay et al., 2017; Light et al., 2016) provides a structure for analyzing the features and embedded meanings of apps, engaging with the interface as well as relevant external information (such as promotional materials or app store descriptions) through step-by-step observation. This involves downloading and registering with the app and attempting to recreate everyday use while taking note of technical and symbolic elements. The analysis first focuses on the environment of expected use, which includes the app’s vision, operating model and governance. Next, the technical walkthrough documents everyday usage.

An app’s vision refers to its intended purpose and target demographics, which may be communicated through the app store page, marketing, associated blogs or websites. The operating model considers expected sources of revenue and business model, such as an upfront cost or in-app purchases that may grant additional features or functionalities, and the app’s governance encompasses “how the app provider seeks to manage and regulate user activity to sustain their operating model and fulfill their vision,” produced through the rules, parameters, community standards and terms of service that control user conduct, or policies surrounding the ownership and handling of data (Light et al., 2016). The technical walkthrough is the “central data-gathering procedure” that involves “engaging with the app interface, working through screens, tapping buttons and exploring menus […] while applying an analytical eye to the process of acquiring the app, registering, accessing features and functionalities and discontinuing use” (Light et al., 2016). Field notes and screenshots are generated through an “STS approach of systematically tracing key actors” as the researcher documents the stages of everyday usage (Light et al., 2016).

As Light et al. (2016) describe, Actor-Network Theory is the foundation of the walkthrough method, as sociocultural and technical features are considered mutually constitutive arrangements and “user interfaces and functions are therefore understood as non-human actors that can be mediators” (Light et al., 2016).

Some work has been done in the past examining big data or crowdsourcing projects and tools through cultural-historical activity theory (CHAT),” which draws attention to the instruments, sign systems and joint practices that culturally mediate activity (Asmolov, 2015). Examined through this lens, crowdsourcing platforms can be conceptualized as mediating artifacts of activity systems that suggest a particular framework of potential actions and behaviors. In other words, crowdsourcing platforms can be approached as a mode of governance. Relying on CHAT, we can deconstruct crowdsourcing platforms as platforms that suggest a particular range of actions and define a particular type of activity system, analyzing the internal contradictions and conflicts within an activity system. These tensions can be considered as a process of constant mediation and renegotiation of the boundaries of activity systems. “Tensions,” here, refers to who is dominating in a particular activity system, whether it is the structures of the system or individual agency of the users. This can be uncovered by examining the boundaries of an activity system and their purpose, the degree of flexibility within the system, the structure of community and division of labor, and most importantly, who exactly is defining and mediating the boundaries of the activity system.

Guided by the walkthrough method, and grounded in the principles of CHAT, I performed a content and platform analysis of Sickweather and HealthMap by downloading them and using them over the course of three months, from May 18, 2017 to August 18, 2017, taking regular screenshots on my phone and keeping a detailed user journal. This involved taking note of the imagery and other content, but also the functionalities of both apps, such as the characteristics of membership, “rules” and parameters of community mobilization and engagement, monetization, moderation by designers or owners. These kinds of questions concerning power and control over the particular platform or system highlight the differences between HealthMap and Sickweather. This allowed me to study
HealthMap and Sickweather as modes of governance that allow for (and depend upon) certain actions and particular activity systems. As part of this process, news media coverage, official company statements, press releases, blog entries and marketing materials were also analyzed. The app was only opened when there was a new push notification or alert, which happened between one and three times each day during the data collection period.

Although screenshots were collected and used to guide the analysis as outlined above, due to the terms of service of the apps, textual descriptions have taken the place of these screenshots within the article.

Next, I conducted a policy review of relevant data protections to provide regulatory background, and examined how the app companies treat user data in their terms of service and user agreements, looking at what types of information is collected, how long this user data is kept, where information is stored, and under what conditions it is disclosed. Although this is approached from a Canadian context, as this is where the apps were downloaded and predominately used over the course of data gathering, this is contrasted with laws and policies from other regions.

Environment of expected use
Sickweather’s Google Play store description tells users that they can “See what’s going around with Sickweather,” asserting that the app is the world’s first “real-time map of sickness” and “the largest illness crowdsourcing community of its kind.” The functions of the app are listed: it “provides real-time alerts whenever you enter a Sick Zone,” and the “SickScore widget” shows users the “threat level of contagious illness” in their immediate area. Sickweather is sold as a way for users to keep themselves informed of disease risk, so that they can take steps – including avoiding certain locations – to decrease their chances of falling ill. The app attempts to engage users by presenting disease risk as constant and ubiquitous, noting in the Play and App stores that “Some viruses can survive on surfaces for up to 48 hours and can have a viral life cycle of 2 weeks[2],[3].” These descriptions, and the imagery on the Play and App stores aim to instill a sense of urgency about disease risk, positioning Sickweather as a tool that allows users to stay vigilant – and thus avoid disease.

Sickweather also encourages users to invite friends and family to create accounts and “track each other’s symptoms and other health events,” and allows for specific locations to be monitored, such as “schools, workplaces, restaurants, hospitals and more!” A testimonial on the Play and App store proclaims that “It’s really great if you’re a parent!” and one of the highlighted screenshots of the app shows how a user could view disease risk information about a specific school (see footnotes 2 and 3). A news article shared on the Sickweather Facebook page in March 2018 describes how an eight-year-old child in North Carolina almost died from septic shock, caused by “A potentially deadly combination of influenza, pneumonia and a bacterial superinfection[4].”

Concern for the wellbeing of loved ones – and particularly, a parent’s concern for their child’s safety – is leveraged to portray the app as a means to stay informed about an always-shifting, ever-present risk. It is suggested that the effectiveness of the app can be increased by recruiting friends and family to create accounts and share more information with the network.

In press releases, app store descriptions, social media posts, and on its website, Sickweather frequently describes itself as “the largest illness crowdsourcing community[5].” This could be viewed as an attempt by Sickweather to portray the app through a positive, communitarian lens, wrapping itself up in the vernacular of collaboration and peer production that is typically used to describe projects such as Wikipedia or open source software (Benkler, 2006; Benkler, 2011). Yet to put it in Castells’ (2011) terms, Sickweather is a private company that controls the structure and profits of
the network, leaving little space for the exercise of counterpower by other social actors (users) within the network.

Sickweather is a commercial app that uses advertising (as well as a paid “pro” version, discussed more below) to generate revenue, targeting individual consumers and, as described on its website, clients that include “some of the biggest names in pharmaceuticals, insurance, retail, household hygiene and OTC[6].” It is notable that in its marketing (on the website and on the download pages in app stores), Sickweather does make some attempts to position itself as a public health tool, evidenced by language, such as “We put the public back in public health,” and describing goals, such as “reducing health care costs, preventing hospital re-admissions, and decelerating the spread of illness” [see footnote 6]. Yet its position as a tool for commodifying disease is undeniable. Last year, Sickweather introduced “Sickweather Pro,” paid licenses to the software that are available for $799 per month for non-commercial use and $1,250 per month for commercial use; purchasing the Pro version gives read/write access “to millions of geotagged illness reports, top trending illnesses, and our famous SickScore […] And much more!” Corporations and advertisers are encouraged to use “Publishing Tools” to reach the Sickweather community, adding locations and sponsored messages (see footnote 6).

However, for a typical user, Sickweather is free of charge – there are no additional features or functionalities within the app that can be purchased. Since the company does not collect subscription fees or other direct costs from its users – other than the Pro licenses being sold for research or commercial purposes – its business model presumably depends on advertising and the collection of user data. The Sickweather privacy policy is available on the app’s website and can be navigated to within the app by bringing up the side menu, selecting “About Us,” and then tapping on the words, “Privacy Policy,” small, hyperlinked text at the bottom of the screen. The privacy policy notes that users are offered the possibility of connecting their social media accounts, such as Facebook and Twitter, and that doing so means consenting to the app accessing personal information from those accounts, including the third party that provides the social media accounts accessing and publishing information about users or their friends from Sickweather[7].

In addition to logging users’ IP address, geographic and device information, Sickweather maintains the right to store and transmit this information, including to third parties, such as partners involved in operating and delivering the app’s services. Advertising partners may also deliver ads to users’ web browsers when visiting other sites or applications, based on cookies set up by the third party advertising network partners. This involves collecting data that is not only submitted to the app voluntarily, but using information collected about users from elsewhere on the web, such as which web pages users have viewed. This allows third-party vendors to tailor and provide ads based on demographic information, device properties, browsing behavior, and more (see footnote 7).

The privacy statement describes how users’ information may be shared with members, affiliates and agents for advertising purposes, and that Sickweather also reserves the right to use the data for other purposes they may deem desirable, subject to requirements under law to seek users consent. Despite assuring users throughout the privacy statement that personal information is anonymized, or simply analyzed as aggregate data, it also states that users acknowledge and agree that their name or other identifying characteristics may be revealed to advertisers or third parties, and in a section that has since been removed, stated that the developers disclaim any liability for any breach of their systems or interception of data transmission (see footnote 7).

In contrast to Sickweather, HealthMap is not positioned as a commercial product, but a public health tool, designed to deliver information to “libraries, local health departments, governments,” and individual users[8]. On the Google Play Store, the description of HealthMap simply states that the app “brings you the latest disease outbreak information,”
providing users with “real-time” data[9]. There are no statements about “keeping friends and family safe,” or imagery of schools or children.

As described in the Terms of Use, the app does not build advertising profiles or sell data to third parties, but does require users to sign up with an e-mail in order to submit disease reports, for “research purposes, quality assurance and correspondence.” It is explicitly stated that this contact information will not be shared, sold, or otherwise revealed to any third party “except as required by law, or to address issues of noncompliance[10].” As a public health tool designed by researchers from Boston Children’s Hospital, Healthmap does not have a “business model” or any kind of revenue stream. This also allows the app and website to exist as an open and transparent platform, as it does not depend on a proprietary algorithm to compete in the app marketplace. On its website, Healthmap lists the freely available information sources that its content is aggregated from, from mailing lists and news sources about emerging infectious diseases, to World Health Organization data and news feeds from the Wildlife Data Integration Network, as well as the open software and apps that it relies on, such as GoogleMapAPI for PHP and xajax PHP AJAX library (see footnote 8).

Technical walkthrough

Disease tracking in Sickweather is given an urgent quality, designed to update users in a way that mimics social media feeds: updates, notifications, and “forecasts” are displayed within the app and users are prompted to receive alerts outside of the app. A typical alert, by default settings, appears on users’ phones similar to text or e-mail notifications, marked by the appearance of a window on the lock and home screens that displays text such as, “Attention! You’re near a fever, sore throat and flu report.” If users tap on the notification, it brings them into the app and displays a live-updated map that marks off the locations of reported illnesses, denoted by small bubbles with the word “sick.” Tapping on the “sick” bubbles provides additional information about the illness report, specifying the type of illness (such as flu, cold, pneumonia) and the date and time that it was reported. The SickScore widget – which is always visible on the home screen of users’ devices – presents a constantly updating numerical representation of the user’s current chance of contracting a disease, classified as either a low, medium, or high risk, alongside a list of “top contributing illnesses.”

With this constantly present calculation of “disease risk,” live-updating maps, and disease alert notifications, Sickweather works to discursively construct disease threat as an omnipresent, inescapable reality, placing contagion fear in users’ pocket or the palm of their hand; alerted by a sound from their phone, at any moment their supposed disease risk can change and instantly make itself known. Point here is not to focus on risk perceptions of disease, but to connect these design features to the idea that the app is trying to compel users to check the app and continue to submit personal information.

Within the Sickweather app, users are encouraged to “Share Sickweather,” promoting the app through Facebook or other means, to “Help keep your friends and family safe.” Information about users is collected, logged and used for advertising and other purposes, and users are encouraged to provide their gender, birthday, location, race and more demographic data. Users are also able to post messages and updates that are tied to specific locations, such as schools or restaurants, that are visible to other users.

Compared to Sickweather, the imagery and tone of HealthMap is more subdued and clinical. User submissions are described as “reports” rather than the social media-themed “status updates” of Sickweather, and users are informed that moderators may edit and delete these contributions as they see fit to maintain the integrity of the platform. Whereas many of the features of Sickweather are seemingly designed to encourage users to submit as much personal information about themselves and others as possible – such as the location-specific messaging features, and the fact that the app requests users to reveal their
age, birthday, gender and race – most of the menus and navigational screens within HealthMap provide additional information about current public health issues, identify the data sources for outbreak reports, or visualize information about outbreaks through supplementary graphs and charts. For example, users may view a chart that summarizes recent cases or outbreaks of diseases; by clicking on a specific case, a new window opens shows the source of the information – possibly a newspaper article or a tweet – as well as a summary of the source, and the option to rate and comment on the accuracy of the alert.

Users may view graphs displaying the prevalence of different diseases over a period of time in different geographic areas; other charts summarize global outbreak data and categorize the information into vectorborne alerts, respiratory alerts and so on.

**Policy, regulations and privacy agreements**

In Canada, there are a number of laws and regulations in place that are relevant to the information gathering and handling practices of mobile apps, such as the Canadian Medical Devices Regulation (“Food and Drugs Act,” 1985). The Office of the Privacy Commissioner of Canada has outlined best privacy practices for developing mobile apps, and outlines the privacy rights of app users and how developers are responsible for the information they collect, use and disclose (OPCC, 2012). Federally, the Personal Information Protection and Electronic Documents Act (PIPEDA) dictates how information about individuals may be collected, used, or disclosed by organizations undertaking commercial activities. For example, users have a right to see the information collected about them, and to ask for corrections. Personal information may include anything from IP addresses to contact lists and location information (OIPC, 2008, 2013; OPCC, 2010, 2012). In addition to these more general privacy laws, most provinces in Canada have dedicated health care privacy legislation, such as Ontario’s Personal Health Information Act (PHIPA) and Alberta’s Health Information Act (HIA), and organizations such as the Canadian Nurses Protective Society and the Canadian Medical Association have issued recommendations and guiding principles for using mobile health applications (Cavoukian, 2004; CMA, 2015; CNPS, 2013; Health Information Act, 2011). These principles include, for example, trying to raise patients’ awareness of the potential risks to privacy associated with sharing and storing health information through apps (CMA, 2015). In Ontario, health information custodians (HICs) are required to notify users if personal health information has been disclosed, including accidental exposure through a data breach, and the custodian must also notify the Privacy Commissioner (IPC, 2017).

Despite the existence of these laws and regulations designed to protect personal information, in practice, there are many barriers to effectively protecting users’ data. For health care specific provisions, there are issues around what does or does not qualify as a “medical device”; there are difficulties concerning the regulation of apps and services that originate from different countries; many of the laws and regulations are broadly defined; finally, the mobile health app marketplace – and apps in general – is growing and evolving at a pace that makes it difficult for lawmakers to keep up.

More than 100,000 new mobile health apps were released in 2016, bringing the total number to 259,000; as of last year, these apps have been downloaded 3.2bn times (Research 2 Guidance, 2016). The nonprofit group Privacy Rights Clearinghouse examined 43 popular health and fitness mobile apps, and found that 72 percent posed a “medium to high risk regarding personal privacy” due to intrusive analytics that track users’ behavior in unexpected ways, insecure data storage, or connecting to third-party sites and sending data unencrypted without user knowledge (Ackerman, 2013, p. 21). The report also found that less than half of the reviewed free apps provided a link to a privacy policy; of the ones that did post a privacy policy, about half were “accurate in describing the app’s technical processes” (Ackerman, 2013).
Despite the fact that mobile health (mHealth) apps “are increasingly handling sensitive data for both professionals and patients,” these apps, from step counters and calorie trackers to disease surveillance apps and websites, fall outside of regulatory protections and frameworks such as the Health Insurance Portability and Accountability Act (HIPAA) in the USA, which provides national standards for electronic health care transactions (He et al., 2014, p. 645). This means the apps “are free to handle data using lower assurances than those typically applied to HIPAA entities,” despite the fact that the data being handled is often just as sensitive (He et al., 2014, p. 645). This is particularly concerning due to the broad nature of the data being collected, as these apps often not only record symptoms and other health information, but combine it with location tracking, social interactions, and more; further, this information – once collected and stored – is often accessible to third parties, hackers or other groups that the user may not be aware of, due to the information being sold or breached (Filkins et al., 2016; He et al., 2014). Perhaps in response to these growing concerns, in 2016 the Federal Trade Commission (FTC) released new guidance for developers of mobile health apps, including a web-based tool for developers that is aimed at helping them understand (and comply with) laws that might apply to their products and service (FTC, 2016).

On May 25, 2018, enforcement came into effect for Europe’s General Data Protection Regulation (GDPR), a set of laws and regulations concerning data gathering practices. Passed by the European Union in 2016, the news rules technically only apply to the data of EU citizens, and build on prior measures such as the Privacy Shield and Data Protection Directive. However, the provisions of the GDPR go further, requiring companies to receive explicit informed consent from anybody in the EU who they collect personal data from, and must also provide users a way to withdraw that consent and request to see all their personal data that the company has stored. Further, there are new requirements for companies that acquire data second hand, which will affect the ways that companies and app developers approach analytics and advertising (Hull, 2015; Koops, 2014; Voss, 2016).

Although only applicable to EU citizens’ data, the measures extend to companies based outside the EU, and maximum fines per violation are set at 4 percent of annual global turnover, or $20m – whichever amount is larger (Tankard, 2016). Questions remain about how much control publishers and companies, like Facebook, for example, will maintain over audience data, as well as some of the details concerning ad networks and the storage and use of data. It also remains to be seen how consistently and aggressively the rules will be enforced, whether the rules will more seriously affect smaller companies and, thus, push the balance of power further toward larger entities such as Google and Facebook, and if companies will aim for a single set of privacy rules across regions, or split off EU data. Koops (2014) argues that these rules depend too much on consent, which means users will be denied access to services if they do not agree to terms and conditions, and that there is no way to ensure individuals have any meaningful awareness of data practices. Indeed, Gorman (2012) notes that users in this situation are presented with a difficult binary: they either have to accept all the provisions in the terms of service, or avoid using a company’s services altogether. Further, as mentioned above, there are difficulties concerning the regulation of apps and services that originate from different countries, which means that “even if the GDPR is applicable to certain conduct of US companies under international law, penalties for violating the law may not actually be enforceable” (Wimmer, 2017, p. 18). Time will tell whether this potential gap between applicability and enforcement impacts the effectiveness and reach of the GDPR.

In Canada, health information privacy laws govern how health care providers and organizations collect data, requiring personal health information to be protected, giving users the right to access the information and see when it has been changed or accessed by others (OPCC, 2015). Yet these laws and regulations are in place for the
handling of patient information by health care professionals, and have not kept up with commercial apps.

In 2014, the Officer of the Information and Privacy Commissioner of Alberta evaluated around 1,200 apps and contended that almost one-third required access to personal information that was beyond the scope of their purpose, or engage in data handling practices that reduce autonomy and control over personal information, such as terms and conditions of use that commonly require users of the apps to grant a license to the developer to the user's content. More than a quarter of the apps evaluated were found to offer no privacy policy at all, or one that raised “serious concerns regarding how their information would be collected, used and disclosed.” Many apps (three quarters) requested permissions, such as device location and ID or access to the camera and contacts. The privacy documentation of the apps often did not explain why the app needed access to certain information (OPCC, 2014).

Ontario’s PHIPA outlines how HICs are required to take “reasonable steps” to protect users’ information from threats, such as unauthorized use, copying, modification or disposal. The wording is general and does not specify physical or electronic safeguards that must be put into place, such as workstation security, access control and authentication, security measures for data transmission and so forth (Cavoukian, 2004). Further, US laws are often not easily aligned with Canadian federal or provincial standards. PHIPA states that users must be notified of data breaches or unauthorized access, and provided a description of the safeguards in place (Cavoukian, 2004). Many apps (including Sickweather) are designed outside of Canada, or at least use cloud-based storage outside of the country, and US-based apps and services are unlikely to comply with multiple sets of laws beyond national borders. As Parker et al. (2017) contend, the collection or sharing of sensitive mental health information for purposes unrelated to the main utility of an app, for example, is not allowed under Australian legislation, yet due to the “complexity of the so-called ‘mobile ecosystem,’ ” in which a complex network of developers, advertisers and other third parties may collect and store data, oftentimes app developers – let alone users – do not know which data are being shared with whom or under what circumstances (3).

Finally, disease tracking apps, such as Sickweather, are unlikely to be classified and regulated the same way as mHealth apps that doctors and patients use to monitor chronic conditions – despite the fact that Sickweather collects, stores and transmits health information, and has begun integrating data from FDA approved medical devices such as the Swaive Smart Ear Thermometer.

Network power, surveillance medicine and “diseaseable subjects”
Disease tracking apps, such as Sickweather and Healthmap, may be located in ideas of network power and control societies, which together can help describe the system of relations that has come about from the rise of globalization and emergence of information technology (Levina, 2015; also see Castells, 2011; Deleuze, 1992; Grewal, 2008). This assemblage of actions from large numbers of people is not an act of collective decision making; rather, sites such as Sickweather and HealthMap demand a global connectivity and place an individual’s subjectivity in relation to others in the network (Levina, 2015).

As previously mentioned, simply abstaining from downloading and using these disease tracking apps is not enough to opt out of the network. Sickweather, for example, not only collects information voluntarily submitted by its users, but also social media posts that are captured by the app’s web crawling algorithms. As Castells (2011) articulates, “power is exercised not by exclusion from the networks but by the imposition of the rules of inclusion” while “the value of being in the network increases exponentially with the size of the network” (pp. 773-774). A value is placed on our identity as “diseaseable subjects” (Gerlach and Hamilton, 2014), as illness status is valuable information that improves the effectiveness and worth of the network.
As Solove (2012) argues, the current paradigm for protecting privacy online is “privacy self-management,” in which people are expected to independently determine the costs and gains from the collection of their personal information, with this supposedly informed consent then legitimizing powerful organizations and agencies to collect and use personal data. Yet there are “structural problems” to this approach, which highlight the inherent power imbalance in the network: there are so many nodes of control and information collection that it is unrealistic for people to manage their privacy in an informed manner, especially with often hidden “potential downstream uses” of their personal data. This regulatory approach, which places the onus on the individual to understand and negotiate a “series of isolated transactions,” is flawed because privacy costs and benefits “are more appropriately assessed cumulatively and holistically” (1880). Further, simply opting out of the network may incur social and professional costs. In popular media, many articles and editorials advise people to simply “quit social media” in order to protect their privacy and personal information (see e.g. Adams, 2013; Manjoo, 2009). Yet this overly simplistic prescription to “just quit” overlooks the costs of leaving social media, which may not only include access to an increasingly entrenched platform for social organization, learning and self-expression, but even professional opportunities (Hartzog and Selinger, 2013). Indeed, this demonstrates how the articulation of network power “can lead to the progressive elimination of the alternatives over which otherwise free choice can be collectively exercised” (Grewal, 2008, pp. 774-775).

Much of the surveillance studies literature frames the issue of privacy in the digital world as one of social control, pointing to the fact that data are collected from anyone who participates “in almost any form of citizenship or consumption” (Best, 2010). The concept of the “control society” is often extended to describe how digital and networked surveillance operates in an increasingly dispersed manner, moving away from central control by institutional authorities, and toward the lateral, self-surveillance and self-discipline of the people living under this control society (see Hardt and Negri, 2000; Palmás, 2011). The purpose of control, here, is to gather and manage information, and in the context of disease tracking apps and services such as Sickweather and Healthmap, this operates as a form of surveillance medicine (Levina, 2015; also see Armstrong, 1995), gathering and using data about the positions and states (healthy/sick) of bodies. The fact that digital disease monitoring tools draw on a range of social media platforms, collecting our Tweets and location, seems to connect to the “convergence of what were once discrete surveillance systems to the point that we can now speak of an emerging ‘surveillant assemblage’ ” (Haggerty and Ericson, 2000, p. 605).

I contend that disease tracking apps represent a fusion between surveillant assemblage and “diseaseability” (Gerlach and Hamilton, 2014). As Levina (2015) explores, digital disease tracking tools are often framed in the discourse of citizenship; with Sickweather, users are encouraged to be “good citizens” by providing information, and people may be compelled by a looming specter of risk (represented by ever-present notifications and alerts in Sickweather) into providing information and increasing the power and worth of the network (Levina, 2015). Yet as we see with Sickweather, this information is arguably gathered not primarily for public health purposes, but to make the network more valuable for the owners, for advertising and other revenue streams that rely on the aggregation of fragmented data streams. Indeed, disease tracking apps use lateral (or participatory) surveillance as a method of gathering and disseminating information. In line with the body of surveillance studies literature cited above (also see Elmer, 2003; Ericson and Haggerty, 2006; Lyon, 2003; Lyon, 2006), Levina (2015) suggests that the structure of these disease surveillance networks facilitates control and the exertion of power – by those who control the network over those who do not; this is merely one example of the ever-increasing use of networked technologies in our lives.
allows for the pervasive surveillance of mobile populations, aggregating increasingly fragmented data (Andrejevic, 2005; Haggerty and Ericson, 2000).

The particular dynamic embodied by disease tracking apps illustrates some of the fundamental weaknesses of rules and regulations that aim to protect user data, including the GDPR. Consent-oriented models not only depend on users’ awareness of the increasingly complex network of actors that store, use and transmit their data, but hinges on their capacity to decline terms of service (Koops, 2014). Saying “no” means being shut out from a part of the mobile ecosystem, and by design, disease tracking tools compel users to volunteer personal data (on themselves and others) in exchange for feeling safe, in the form of information about omnipresent, always-shifting disease threat (Caduff, 2014). Rules such as the GDPR are predicated on users acting as rational decision makers in a free marketplace that offers meaningful alternatives, giving people the awareness, power and choice to decline a service and control their personal data. Time will tell what kind of impact the GDPR has on the mobile app marketplace. If most services (especially productivity apps and social networks from large companies such as Facebook and Google, which now occupy a central role in many people’s professional and personal lives) do not change their actual data collection, use and management practices, then increasing users’ awareness of these practices will be a somewhat hollow exercise. Further, through the construction of disease threat and risk, disease tracking tools arguably reduce a user’s capacity to rationally weigh the costs of potential privacy infringements against the supposed benefits, supporting the need for data protection reform that more meaningfully regulates data collection and handling (Koops, 2014).

Conclusion
Mosco (2014) contends that so-called “big data” and “surveillance” constitute a broad range of ideas, practices and techniques, occurring in a variety of contexts; certain kinds of ends and possibilities may be evident in one context but not another. Marketing, health care, anti-terrorism and policing – all popular application sites of big data – are not of course the same practices, and the possible benefits and harms vary. Indeed, Healthmap and Sickweather – despite carrying out similar functions, as “disease alert apps” – occupy very different positions in terms of their aims, business models, construction of disease risk and privacy implications. The former, a public health tool that uses open data sources and freely available software, was designed by researchers to improve the detection of disease outbreaks. It does not collect personal information of users (even submitting an e-mail is optional, and only required to submit disease reports) to sell to third parties or build advertising profiles. Further, disease information is provided to users in a contextualized manner, clearly displaying the source of disease alerts as well as data about disease rates over time and space. In contrast, Sickweather is a commercial app that collects and sells user information to third parties and advertisers. Disease risk is arguably constructed to appear omnipresent and inescapable – unless users stay vigilant and take steps to protect themselves, which means subscribing to disease alerts from the app, following location-specific messages from other users, and encouraging family and friends to create accounts.

Turning back to Google’s foray into public health, archival data from the Google Flu Trends website is available online. Yet Google’s various platforms and services, including DeepMind, lack transparency and openness. This is understandable, from the perspective of a large corporation trying to protect its products. Yet when it comes to rhetoric concerning crowdsourcing and the empowerment of users, there is only truly “collaboration” insofar as people who use internet services and mobile apps sign agreements that allow for the collection and use of their private data; the exact algorithms and inner-workings are closed off from the public eye. This means that cultural work, such as defining and negotiating concepts like health and disease, has been entrusted to digital technologies such as databases and algorithms, giving rise to what Galloway terms “algorithmic culture,” leading
to a societal “black box” in which largely unseen algorithms determine patterns of inclusion and exclusion, invisibly defining and controlling interactions (Galloway, 2006; Pasquale, 2015; Striphas, 2015; Gillespie, 2014).

The point here is not to vilify disease tracking apps or corporations such as Google. Rather, the point here is to examine how big data and crowdsourcing approaches to tracking disease are a particular kind of activity system that might be embedded with certain power relations, boundaries and divisions of labor. Connecting this to concepts like network power, the control society, and surveillance assemblages can help reveal the implications of these tools – however, well-meaning they are – for individual privacy. As argues, big data has the capacity to intensify certain surveillance trends that are generally associated with information technologies and networks, and is therefore implicated in configurations of power and influence.

Notes
1. www.sickweather.com/
7. www.sickweather.com/privacy/
8. www.healthmap.org/site/about
10. www.healthmap.org/site/about/termsofuse

References


Corresponding author
Scott S.D. Mitchell can be contacted at: scott.dobson.mitchell@gmail.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
The compliant environment
Conformity, data processing and increasing inequality in UK higher education
Penny Andrews
School of Information, University of Sheffield, Sheffield, UK

Abstract
Purpose – The purpose of this paper is to present the concept of institutions as compliant environments, using data to monitor and enforce compliance with a range of external policies and initiatives, using the particular example of UK higher education (HE) institutions. The paper differs from previous studies by bringing together a range of policies and uses of data covering different areas of HE and demonstrating how they contribute to the common goal of compliance.
Design/methodology/approach – The compliant environment is defined in this context and the author has applied the preliminary model to a range of policies and cases that use and reuse data from staff and students in HE.
Findings – The findings show that the focus on compliance with these policies and initiatives has resulted in a high level of surveillance of staff and students and a lack of resistance towards policies that work against the goals of education and academia.
Research limitations/implications – This is the first study to bring together the range of areas in which policy compliance and data processing are entwined in HE. The study contributes to the academic literature on data and surveillance and on academic institutions as organisations.
Practical implications – The paper offers suggestions for resistance to compliance and data processing initiatives in HE.
Originality/value – This is the first study to bring together the range of areas in which policy compliance and data processing are entwined in HE. The study contributes to the academic literature on data and surveillance and on academic institutions as organisations.
Keywords Higher education, Policy, Immigration, Dataveillance, Surveillance, Data
Paper type Conceptual paper

Introduction
The “compliant environment” at the Home Office (Home Office, 2017a) is a rebranding of then Home Secretary Theresa May’s “hostile environment” approach to immigration (Travis, 2013), which involves the reuse and processing of data from a variety of sources (including the National Health Service, employers, housing providers, educational institutions and social media) and the promotion of unwelcoming messages aimed at migrants to the UK to support immigration enforcement. This paper argues that a form of “compliant environment” is what we now see in UK higher education (HE), perpetuated by a number of different initiatives aimed at staff and students, both at the institutional and national level. The compliant environment in HE is heavily reliant on the collection and processing of multiple sources of the data for the monitoring of this compliance, and also to create new forms of compliance and conformity via metrics and analytics. While other articles have considered these initiatives separately, this paper is original in rigorously examining their collective impact inside and outside universities, and their relationship to other everyday uses of data to monitor and evaluate citizens. This paper explains the various ways in which data is used in UK HE to comply with outside agendas and conform with various social and sectoral norms, and suggests a different approach informed by the resistance work of NHS workers. If UK HE is important to society and is to remain a public good, this resistance work is needed. Significant claims (Leathwood and Read, 2013; Lynch and Ivancheva, 2016; Spiller et al., 2018; Teelken, 2012) are made about this collective impact of compliance initiatives: the combined effect is to enact more oppression on the most
marginalised and surveilled people in HE – both underrepresented minorities in the staff and student bodies – and to erode trust and public good in HE. Support from the public and finance from the government depends on how the role of HE is viewed: as employment training or as a public good in itself.

The concept of HE as a “public good” is contested. As Nixon (2011) points out in his work on the topic, so is the idea of the “public” itself, and both are often too narrowly defined and need to be more broadly imagined outside the scope of private interests and those with the power to bestow or withdraw public ownership. If the government’s stated desire is to encourage more privatisation and “challenger institutions” in HE (Department for Business Innovation & Skills, 2016), that indicates that they think they have this power and do not consider the public to be the current owners. HE and university are not synonymous or inseparable, but the latter is the main model for delivery of the former in the UK. The experiences of both staff and students have diversified further and grown in complexity since the student population in universities has become bigger and more heterogeneous (Wånggren, 2018), and the policy framework continually changes (Collini, 2017), further exposing the inequalities already present.

Increased professionalisation and privatisation has led some academics to leave their jobs (Morrish, 2016), finding the demands of “the general distortions required to turn a university into a for-profit business” (Warner, 2014) intolerable. Others such as Les Back (2016) have chosen to stay, deploying strategies of non-envious generosity and developing an intellectual hinterland to survive and thrive. However, academics can be argued to have been actively complicit in the auditing and marketisation measures their colleagues find so oppressive, and at research-intensive universities may have sought protection for their funding and place in middle class society at the price of the public status of the university (Holmwood, 2017, 2018).

The branding of UK universities, via distinctive design and differentiation of the “student experience” (Barkas et al., 2019; Lomer et al., 2018), has intensified since the 1990s formation of groupings like the Russell Group and Million+, which signal both the institution’s position within the elite hierarchy and their intended focuses and audiences (Furey et al., 2014) to undergraduate applicants and the wider world. Prestige at institutional and individual level became more important as the sector became more marketised and forced into competition by government policy, and the number of qualified academics applying for jobs increased (Blackmore and Kandiko, 2011; Holmwood, 2018; Tregoning, 2016). To market themselves, academics and universities too are drawn into the data-driven world of benchmarked data, metrics and indicators of esteem (Coate and Kandiko Howson, 2016) and into conforming with others’ ideas of what a successful or high quality brand might be. Marketing literature from UK universities demonstrates a high level of homogeneity in UK HE, and institutional expectations are high but explanations of what e.g. “quality” or “the student experience” really mean are scarce (Huisman and Mampaey, 2018). Equally, what makes an academic employable is not any distinctive factors but high scores in standardised metrics (Hall and Page, 2015; Smeyers and Burbules, 2011) and exercises such internal audits for the Research Excellency Framework (Grant and Elizabeth, 2015; Marcella et al., 2017; Shore and Wright, 2015) and a high score on a competency framework that often cannot allow for contextual information or individual circumstances. The “good” or “successful” academic (Archer, 2008; Van den Brink and Benshop, 2014) and “good” university or institution (Brown and Mazzarol, 2009; Mountz et al., 2015; Olssen, 2016) are judged by rankings, research income and prestige, and a very particular idea of what students need and want (EY Parthenon, 2018).

This paper outlines the concept of the compliant environment in HE. It then explains how data are used and combined in HE, including for purposes of border control and othering of staff and students, the reasons why compliance occurs and offers some ideas for resisting compliance.
A compliant environment

The Home Office describe their vision of the “compliant environment” as follows:

The Compliant Environment, which deters and prevents immigration offending and protects public and private services from abuse through a rounded package of incentives, interventions and sanctions, is an integral part of the BICS Business Plan. (Home Office, 2017b)

Compliance in UK HE also involves a “rounded package of incentives, interventions and sanctions”. The purposes of creating such an environment are different from those of the Home Office, outside of the legal requirements to support immigration and anti-terrorism (Prevent) initiatives, but the impact on staff and students is still considerable. The compliant environment in HE presents in two connected ways:

1. HE acts as an arm of the UK government’s policy on immigration. This is the compliant environment as border control.
2. HE has adopted the compliant environment in and of itself, as extension of audit culture connected with the marketization of UK HE.

Why is everyone so focussed on compliance in these different situations – with the government (understandable, but resistible), with funders, with vendors (NDAs etc), with certain ideas of success and excellence, with the norms of STEM (Science, Technology, Engineering and Mathematics)? Where is the governance of this form of governance? The compliant environment is the best way to understand what is happening, as it demonstrates the consequences of succumbing to the branding and marketization of HE in the UK and the influence of external stakeholders in the sector – all monitored and controlled by data products and services. This is important because it helps to take a holistic view of where HE sits within wider trends of data use in education and the UK government’s interventions around immigration and “excellence” in universities (Moore et al., 2017) and who suffers most from the implementation of compliance across all areas of HE.

The “compliant environment” is a way to draw together and extend other, often related, concepts already in use in the sociologies of HE and work: audit culture, managerialism (over-reliance on professional managers), marketization (turning the university sector into a competitive market), quantified work (work reduced to what can be measured, e.g. targets or rankings), New Public Management (making public services more business-like), attainment gaps (between groups of learners) and the performative university (one where the challenges are seen as individual, rather than structural – Pereira and do, 2015). All of these issues have to be seen together to understand and resist their effects on students and staff. They are part of the same problem, where universities are not sites of resistance to policies and ideologies imposed by the government and business but are compliant with its demands.

Data use in HE

Just because a situation can be framed as a problem, in order that a product or service can be offered as a solution, does not mean that this problem can or should be solved. In the case of what Andrews calls data foam products (Andrews, 2018), products of dubious value such as new research metrics that are created by combining multiple sources of data, they are often sold to administrators as part of bigger workflow and analytics packages, but the individual products are marketed as answers to specific questions that were not posed by the purchaser. Comparing researchers across fields is not something that is of great benefit to researchers or their disciplines, and human expertise and robust processes have traditionally been advocated, if not always used, in sensitive situations where researchers must be individually evaluated. However, a product like Field Weighted Citation Index is a
A metric designed to enable this sort of comparison without knowledge or context, enabling a worker with less domain knowledge and/or fewer relevant skills to create automated reports and make recommendations to decision-makers. It is an example of automated discrimination (Lyon, 2003).

Reducing costs and increasing the productivity of staff are problems many organisations are keen to solve. When accompany (RELX/Elsevier) tells you that part of their business (LexisNexis) is risk management, believe them. Their products, created via control of multiple data flows (LexisNexis, 2016, 2017), have the potential to enhance employee surveillance and employment risk management. Arguably, the internal and external use of Elsevier products such as Scopus (an index of citations) and SciVal (a reporting system for research metrics) in rankings and evaluation improve a “high performing” university’s success in attracting income in the form of research grants and student numbers.

The networks and the flows are most important in relating to the data, not the individual. Discussions about data ownership, downloading data held by an organisation or platform or calls for “transparency” do not address the issues raised by combining and processing data, nor tell the whole story. Commoditised networks, knowledge and prosocial behaviour can only be understood through consideration of the control of networks and flows, and the impact of this on society, not the data and the individual alone.

The current President of Ireland gave his opinion on the use of academic metrics in a 2018 speech:

Within the universities [...] resources are increasingly channelled towards areas which, it is suggested, will yield a return, at least in the short-term, to the university in terms of increased funding. Much of this is facilitated by an abuse of metrics; an ideological fad that views the use of metrics of academic work, not as a contribution or an instrument of knowledge but as a conforming bending of the knee to an insufficiently contested neo-utilitarian mediocrity. (Higgins, 2018)

Higgins is being provocative here; but talk of the abuse and effects on workers of metrics is not new, either inside or outside HE (Burrows, 2012; Moore, 2015; Pereira and do, 2015). The understandable response of managers and workers alike is conformity with the expectations of the metric or target, if they are disciplined or experience loss of status or income as a result of non-compliance.

Under the General Data Protection Regulations (GDPR), an organisation processing data needs to consider whether the individual whose data is being processed expects this specific use case to happen (Information Commissioner’s Office, 2012, 2018) and if they actively consented to this just by doing their job (teaching, writing, publishing, applying for grants). An individual researcher may not really have control over who they are associated with in the various data sets or who uses or does not use their work, leading to greater or fewer citations of their research outputs. If researchers do not expect this processing to happen, and feel they have little agency over how they are presented in the data product nor how they are judged by it, this should lead institutions to be more careful both legally and ethically in how processed data such as metrics are used.

Metrics and rankings, whether used singly or as part of a “basket of metrics”, only tell the observer what an individual or organisation has done, not what they can – or are even likely to – do. If researcher, departmental or institutional potential is evaluated solely or predominantly via metrics, this is not a responsible use of the numbers (Wilsdon et al, 2015, 2017). To do so is to take a Friedman-like view of personal probability (Friedman, 1976), assigning numerical probabilities to events and arguing for a scientific basis for using metrics for prediction, rather than a Keynes and Knightian approach of risks and uncertainties (Runde, 1998). Academic potential can be argued to be an uncertainty. Studies indicate that journal articles by people of colour are cited less often than those by white authors, with their work receiving less circulation and less attention even as they publish
more outputs (Chakravartty et al., 2018). Novel contributions to the scholarly record receive more variable citation performance and a delay in recognition compared with more traditional or incremental contributions (Wang et al., 2017). Ironically, it is bibliometric analyses that demonstrate why bibliometric analyses should not be used to judge the quality of research or researchers, nor its potential impact. Studies of student evaluations similarly show that those metrics do not correlate with actual learning (Uttl et al., 2017).

The metrics used in the assessment of research and researchers are just part of a trend in UK universities and schools for more and more data collection, processing, analytics and sharing (Perrotta and Williamson, 2018; Williamson, 2016, 2018). Sometimes this is to fulfil legal obligations—some considered by academics to be more legitimate than others (Spiller et al., 2018), given the Conservative Government’s attitudes towards immigration, potential extremism, surveillance, employment rights, liberalism and privacy. Arguments are made for analytics and technology improving staff productivity, student retention and more, when the funding for mental health and pastoral care services are being cut or remain static and the employment prospects of both staff and graduating students are constantly under threat. The idea that people are best motivated and supported by investment in them as individuals and as a society—and in the people who can help them—seems to be outdated.

Quantitative data about student achievements, attendance, activities and engagement levels, amongst other things, is used in further and HE to predict success and pick up potential problems, as well as make claims about cohort groups and refine course and marketing offerings (Jivet et al., 2018; Wintrup, 2017). Data dashboards enable time-pressured staff to have an overview of their students and their progression, and also increase the student’s sense of surveillance (Dear, 2018) and need for conformity within education, especially when targets or indicators are used to denote success or failure with a particular attribute (Burke et al., 2018). Hall and Bowles (2016) provocatively call this a “disciplining gaze”, and their feedback a source for “institutional market gain”. However, a scoping study from the University of Huddersfield (Bennett, 2018) found that some students like being able to see their own data and find a dashboard approach motivates their study, even when they are not achieving what is expected of them. The author does note the need for student training and attention their wellbeing when looking at dashboards, and the study is a small one. There is a government interest in increasing the use of big data and learning analytics in education at all levels, and less positive and positivist approach to understanding how data can be used in this space is needed (Williamson, 2018).

Monitoring and evaluation

University services, including the library and disability services, collect data to measure efficacy and make a case for continued funding. This is understandable at a time of cuts, where capital projects continue to receive funding, but workers are not replaced—or not with full-time, permanent, properly-paid posts. It is a short step from monitoring grades, feedback, attendance, punctuality, engagement with learning management systems or virtual learning environments, legal and health status and so on to passing it between institutions and governments and flagging up risky applications for courses, modules, placements and jobs. Some institutions have piloted tracking of student (Wang, 2018) movement around campus and others are using data to track services staff (Skillweb, 2018; SmartTask, 2018). It would not be difficult to de-anonymise that data, given the other data held on students (including closed circuit television—CCTV—footage, class attendance, WiFi usage and social media accounts) with which it could be triangulated. The university does not have to be collecting all the data itself, but it has fallen into procurement and subscription deals with those who have access to multiple data flows and collect and create more. This is how universities end up contributing to the infrastructure of student surveillance.
An individual has limited capacity to opt out from or resist most of these data-based monitoring and evaluation initiatives, particularly while the prestige economy and competition that enables scholars to advance in their careers (Coate and Kandiko Howson, 2016; Kandiko Howson et al., 2018) causes them to feel anxious and isolated (Loveday, 2017, 2018). The power for that kind of action requires collective responsibility from unions and institutions and political action from elected representatives, who would do better to consider qualitative as well as quantitative evidence for their actions. If, as has been argued, enthusiasm for the use of metrics and data analytics is against the stated values of researchers and librarians (Andrews, 2018), then organisations representing those groups could do more to develop principles for responsible use of data and metrics and the use and procurement of analytics products. This "civic hygiene" (Schneier, 2007) approach would reduce the threat from bad actors. Individuals, even powerful ones, cannot personally remove the incentives for using data to monitor, evaluate and exclude people, so it is up to institutions and policy makers to behave responsibly and protect citizens by creating and supporting new norms around data use and reuse – even as universities continue to blandly conform with institutionalised values (Mampaey, 2018) and fear risk.

**Combining data sources**

Data collected and/or processed for one purpose can end up being used or combined and used for another, increasing risk to those who provide or are measured by the data. Data products, some of which are of dubious value (data foam), are bought or used by institutions, arguably sometimes because they are there rather than out of need (Andrews, 2018). Data can be combined in ways that amplify existing inequalities around gender (Hill et al., 2016), race (Tramer et al., 2017), class (Archer, 2008; Bathmaker et al., 2013), precaritised work (UCU, 2016), first generation students etc and more. Recent statistical reports on UK students from the Sutton Trust (Montacute and Cullinane, 2018) and UK staff and students from Access HE, formerly HESA (Equality Challenge Unit, 2018a, b) show that those existing inequalities, based on protected characteristics data, are not improving and in some cases are worsening. It is no longer the case that “if you are not paying, you are the product”, as part-payment via data is part of the business model for companies inside and outside of academia, and cuts to the HE budget make these kinds of deals more likely.

Comparisons between individuals and organisations and the intensification of the prestige economy are linked to marketization, managerialization and the problems of identity work within organisations. This admittedly difficult identity work, particularly as a precursor to changes to student admissions, has been suggested as a way for academics and managers to resist perpetuating inequalities and address the exclusionary nature of their institutions (Boliver et al., 2018). Researchers and students assert the limited agency they have in a competitive system where they have limited power and their performance is continually monitored and evaluated. When evidence to the government is being provided by QS Solutions, who produce world rankings based on Scopus and other data and student survey reports branded as “enrolment solutions” (QS Enrolment Solutions, 2018a, b), it is clear that the agenda is being shaped by vendors with something to gain from simplification, combined data products, rankings and metricization. Senior managers and research offices are offered these products, such as the full workflow suites from Elsevier and Digital Science, or alternative products from Clarivate, to improve their efficiency and performance. Rank and file academics, students and librarians have little or no say in whether or not they are included in these purchases and pilot schemes.

Young people in some countries may not know a life without tracking, having been subject to dataveillance throughout school, university, their academic or other career (Lupton and Williamson, 2017). Supplier oligopoly in big data means a student or staff member could be at a sensor-loaded football stadium on Saturday, filmed by body-worn
cameras operated by railway station staff and police on their way home on Sunday and tracked across campus on Monday – with all the data stored in the same corporate cloud. The same land grab that happened in other areas of technology has happened here, which increases risk for those who would prefer their data not to be combined. Institutions, government, funders, administrators and librarians need to recognise their roles in perpetuating these problems, instead of just blaming large technology companies. Unethical use of data by academic researchers, e.g. the personality quizzes on Facebook that fed Cambridge Analytica’s political activities and far lesser known examples, may well be the result of pressure on academics to publish quickly, be original, significant and suitably quantified in their research (Hermanowicz, 2016; Loveday, 2018), but contributes to the problem at the macro-level as attitudes towards use of personal data are tainted. Is the “good university” one that fulfils expectations of the sector and the Home Office, or one that puts behaving ethically towards students and staff first? The wellbeing of marginalised staff and students should not be a secondary consideration.

Bordering, othering and immigration
Marginalised students and staff experience more surveillance by systems and society and feel under more pressure to perform successfully, as in the experience of Femi Nylander, a black Oxford alumnus who was tracked via CCTV and his image circulated to staff and students (Joseph-Salisbury, 2019), the racist treatment by colleagues of academic Priyamvada Gopal (Mirsky, 2018) and the support for the “free speech” of senior academics making statements and writing articles that are perceived by transgender staff and students and their supporters as discriminatory and hurtful (Kennedy, 2018; t philosopher, 2019). While the junior researchers, such as the anonymous trans woman “t philosopher”, leave academia due to transphobia, the senior academics who erroneously claim from their platforms to be “silenced” (Phipps, 2019) – critiqued by Sara Ahmed as an abuse of unrecognised privilege (Ahmed, 2015, 2016) – are rewarded with promotion. The tendency of the university is to distrust both workers and students, requiring endless paperwork providing proof of disability (Dong and Lucas, 2013; Hughes et al., 2016; Seale et al., 2015), illness, fitness to return to work/study and more. The experience of difference and an inability to conform and comply with the norms of their peers is felt by academic parents (Harris et al., 2017), trans academics (Pitcher, 2017), working class students and academics (Bathmaker et al., 2013; Black, 2005) and more – and all feel watched and judged.

University workers have a duty under UK counter-terrorism law to prevent people from being drawn into extremism, and the requirement for monitoring and reporting of suspected radicalism brings them into conflict with their need to support academic freedom and the welfare of their students (Spiller et al., 2018). This is often called the “Prevent duty” or “PREVENT strategy” and universities must report any incidents immediately to the government (previously to the Higher Education Council for England, HEFCE, now to the Office for Students) and also supply details of their compliance with their duty to protect “British values” and identify people at risk of radicalisation (HEFCE, 2017; HM Government, 2015; Morrice, 2018) on a regular basis. Some of these reports are published online (Queen Mary University of London, 2017). The binaries between migrant/non-migrant and interested in extremism/at risk of radicalisation are more porous than accounted for by the law, in a multicultural and international society with 24/7 access to the news and online sources, or by the general approach to the reporting duty or the data generated from reports. Muslim students in particular experience life as part of a surveillant assemblage of policies, rhetoric and security measures that distrust them and set them apart from their peers, without the data gathered on them significantly improving the intelligence gathered on terrorism either from radical Islamist sources or the UK far right (Sharma and Nijjar, 2018). In the latest update to the counter-terrorism strategy,
Prime Minister Theresa May made this statement: “Because the threat we face is large and multi-faceted, this Strategy has a much greater focus on systemic co-ordination across the public sector” (Home Office, 2018a). Universities are neither set apart in an ivory tower, nor neutrally situated within a community – they are part of this public sector infrastructure of compliance.

It is argued by many that HE is a public good as well as a successful export in international trade (Marginson, 2011; Tilak, 2009), but the UK Government views working and studying in HE as an opportunity for immigration irregularities and requires a large amount of compliance work from institutions that sponsor international students (Home Office, 2018b; UCEA, 2014; University of Chester, 2018; University of Liverpool, 2017; University of Strathclyde, 2018). Checking whereabouts information for international staff (Grove, 2016) and students (Grove, 2012; University of Edinburgh, 2017) can begin as a way of fulfilling obligations to the UK Visa and Immigration (UKVI) inspectors that then normalises requests from a vendor, the Estates department and others for checking academic and student space usage via sensors (FlexibleBoss, 2016; Strydom, 2014; The University of Edinburgh, 2017), tracking other activities online and making a lack of trust the default. The ubiquity of this can help gain support from “home” staff and trades unions for resisting what they dub “xenophobia” (Grove, 2016); however, disgruntled non-international academics may take another view and grow to resent the monitoring of all in service of a minority group. Academics have been co-opted into not only complying with the requirements of UKVI, but effectively becoming border control agents when they collect and report attendance and other data on international staff and students, and there has been limited resistance to this use of soft power and institutionalisation of this compliance as a sectoral norm (Dear, 2018):

Sponsors must […] demonstrate that they are compliant with their sponsorship duties, by passing a Basic Compliance Assessment (BCA) every 12 months. (Home Office, 2018b)

The UK has for some time had a government that wishes to make the country less attractive to outsiders (Gower, 2015) and has enacted legislation that supports their ideology (Bales, 2017; Gower, 2015; Home Office, 2017b; Partos and Bale, 2015). Different institutions take different approaches to working with international staff, with some paying the relevant fees every year for their staff and providing significant advice and support with immigration issues and others viewing it solely as the financial and administrative responsibility of the employee and their fault if full compliance with all the legalities is not achieved. A review article about the use of health data in the NHS in immigration control (Hiam et al., 2018) and a study of university lecturers’ understanding of Prevent duties (Spiller et al., 2018) offer in different ways some hope for resistance work, encouraging workers to look to their collective ethics and values and take an approach that resists neoliberal discourses around terrorism prevention and immigration control. The university does not have to be part of the iBorder (Pötzsch, 2015) or the breaking down of pluralist, accepting society (Yuval-Davis et al., 2018). The university should contribute to work around belonging, and not bordering.

Reasons for compliance
UK universities have been criticised for their limited compliance with the Equality Act 2010, particularly with reference to supporting staff and students with disabilities (Department for Education, 2017). There are limited consequences for failing to make classrooms accessible or have sufficient independently-operating lifts, even with trades unions support for staff members, in part because the numbers of affected workers and students are relatively small. However, compliance with other forms of legislation and social norms, as has been shown throughout this paper, is much higher, and therefore the either the inducements to comply or punishments for non-compliance for these other forms must hold
significantly more weight for senior managers. The tactics of social influence, fear of ostracism within the sector and the network effects of other institutions add to the pressure to comply and conform with border control, metrics, analytics and branding imperatives (Carter-Sowell et al., 2008; Pratkanis, 2007).

A key factor in institutional support for research metrics is the corporate capture of metrics, data analytics and the various products that support them, which are sold to administrators as a solution to multiple problems they may or may not face in their role (Andrews, 2018). These products are often available as part of an information and analytics suite, offering end to end data management. Data dashboards can combine school data, admissions data, Office for Students data, data held and sold on academic outputs and their funders and more. There are internal and external pressures to improve scores in national, international and subject rankings, student numbers, grant income and industry funding and so on and all these scores are benchmarked against other institutions. The high numbers of applicants for academic jobs also makes it tempting for universities to use individual and journal metrics in the recruitment process. It is possible that the companies marketing these metrics are playing a similar game to Cambridge Analytica, in that their publicity makes persuasive promises the products cannot fulfil.

Resisting compliance

Academic freedom and the “student voice” are never out of the media on both sides of the Atlantic Ocean, and yet there is not a sustained effort in the HE sector to resist the rhetoric, policies and behaviours of compliance. The workforce and the student body have become individualised, precaritised and fragmented. Politically, there is a tendency towards polarised discussions and “digital dissensus” (Andrews in Mina, 2018), which makes it difficult to take a position that is more nuanced than discourses of utopia or refusal. The sector has arguably had to accept neoliberalism and managerialism to survive government cuts (Department for Business Innovation & Skills, 2016) and departments and individuals suffer if they do not comply with audit culture. Resistance therefore has to be collective and work with and extend the available structures, such as the trades unions and lobbying policy makers.

If it is accepted that some levels of data-driven monitoring and surveillance is inevitable, it is not inevitable that all power over the data needs to be ceded to profit-making corporates. This could be seen as an opportunity to enforce cooperative responsibility in platform governance (Helberger et al., 2018), where the workers whose data are processed or passed through a platform could have an important role in its governance and preservation. Data analytics in HE does not need to be wholly the purview of instrumental technocrats (Kitchin et al., 2017; Ottinger, 2013), but involve the whole academic community. One challenge of resistance is the lack of voice and status for people who are actually oppressed in comparison with people who feel they are being silenced, despite in most ways conforming with middle class professional norms. There’s only one class they are interested in, and it is their own. Recent anti-transgender discourses in academic philosophy have led to tensions between the academic freedom of full professors and the safety and dignity of minority students (Kennedy, 2018). There is a need for data governance models in HE that take power analyses into account (Bates, 2018), and a need for regulatory friction that slows the abuse of data that creates a harmful compliant environment. GDPR, mentioned earlier in this paper, could be argued to cause much friction as it is very complex. High complexity can favour large companies and institutions who can manage compliance, leading to monopolies and oligopolies in data handling. However, as seen earlier in the response to the Equality Act and the lack of consequences for non-compliance, policy and legislation itself is not enough to protect marginalised people.
The responsible research and metrics movements (Stahl, 2013; Wilsdon et al., 2017) offer some glimmers of hope towards a code of practice that could be accepted by multiple stakeholders and avoid the worst abuses, as universities sign up to the San Francisco DORA (declaration on research assessment) principles (DORA, 2012) and avoid using specific metrics seen as inappropriate, such as the journal Impact Factor, for assessing individuals. However, research is only one part of the university. Teaching metrics and analytics, markers of engagement with student-facing systems, strike-breaking uses of lecture recording and employee surveillance (Edwards et al., 2018) and other forms of technology-enabled management and control are not covered by these initiatives. The modern university is so siloed that changing one group’s minds such as academics or librarians may have little impact on the wider sector, and collaborative resistance working across roles and institutions offers a greater chance of success, from rank and file academics and professional services staff to the highest levels of management. Those who choose to resist, who struggle to meet the norms of the sector or stand in solidarity with those who cannot meet those norms, can make themselves visible to others through the struggle and become a community. The systems can be queered (Ahmed, 2018).

Conclusions
As this paper makes clear, when it comes to compliance in UK HE, it is not just metrics, or learning analytics, it is not just border control or surveillance or the undermining of industrial action. It is all those things creating an infrastructure of compliance with policies and assimilation with the norms of a certain kind of student or staff member. There is a strong “narrative investment” (Ahmed, 2015) in the idea and the identity of being a “good university”; and being a “good academic”, or at least a successful one, involves some forms of compliance and conformity to ensure certain ideas of quality assurance and brand reputation are maintained. In this house, we handle immigration well, we avoid trouble and bad press, we score well on all the metrics and rankings, we defend the boundaries of our discipline, we defend what it means to be people like us with our values and we are not the university or the academics your parents or politicians worry about. Data collection and monitoring (and surveillance) are too often used as the tools of reinforcing this narrative and set of institutional values and proving that the sector is right, not finding new stories to tell.

One off acts of resistance will struggle to work, in a time of political and social fragmentation, so it is important to take a civic hygiene (Schneier, 2007) approach to data use, data abuse and compliance as a sector. If we all wash our hands, fewer people get ill. Ongoing small actions that contribute to more than our own health can have a big impact (Raza et al., 1997). Other studies focus on single areas such as immigration, metrics, space monitoring or performance management – but this paper demonstrates how compliance with them all is all part of the same drive. Brand management, prestige and a cautious approach to competition leads to conformity. The people academic and liberal values tell us we are supposed to care about most are getting hurt, and we need to see the problems structurally and act collectively to resist it. Future work in this area would link the data agenda and brand management empirically. Until then, workers and students in UK HE must collectively agree to use data for the benefit of our communities and not merely to serve other agendas.

References


DORA (2012), San Francisco Declaration on Research Assessment, DORA, San Francisco, CA, available at: https://sfdora.org/read/


Friedman, M. (1976), *Price Theory*, Aldine, Chicago, IL.


Further reading


Corresponding author
Penny Andrews can be contacted at: pennyb@gmail.com