Revisiting public health informatics: patient privacy concerns

David Birnbaum  
*Applied Epidemiology, North Saanich, Canada*

Kathryn Gretzinger  
*School of Journalism, University of British Columbia, Vancouver, Canada*

Marcy G. Antonio and Elizabeth Loewen  
*University of Victoria, Victoria, Canada, and*

Paulette Lacroix  
*PC Lacroix Consulting Inc., Vancouver, Canada*

**Abstract**

**Purpose** – Expanding networks of data portals and repositories linked to electronic patient record systems, along with advances in information technology, have created both new opportunities in improving public health and new challenges in protecting patient privacy. The purpose of this paper is to review stakeholder perspectives and provide a framework for promoting implementation of current privacy protection improvement recommendations.

**Design/methodology/approach** – This paper summarizes a workshop session discussion stemming from the 2017 Information Technology and Communication in Health (ITCH) biennial international conference in Victoria, British Columbia, Canada. The perspectives within health service research, journalism, informatics and privacy protection were represented.

**Findings** – Problems underlying gaps in privacy protection in the USA and Canada, along with then-current changes recommended by public health leaders as well as Information and Privacy Commissioners, were identified in a session of the 2015 ITCH conference. During the 2017 conference, a workshop outlined the current situation, identifying ongoing challenges and a lack of significant progress. This paper summarizes that 2017 discussion identifying political climate as the major impediment to progress on this issue. It concludes with a framework to guide the path forward.

**Originality/value** – This paper provides an international perspective to problems, resources and solution pathways with links useful to readers in all countries.

**Keywords** Public health, Knowledge management, Information technology, Risk management, Health law or regulation, Informatics

**Paper type** Viewpoint

The case for a new data sharing policy framework

Electronic patient record (EPR) systems store detailed patient information and serve to communicate a patient’s longitudinal clinical data across multiple clinical care sites (Häyrinen *et al.*, 2008). They have become increasingly linked through data portals in wide networks so that authorized entities can add laboratory and other diagnostic test results; automate required public health case reporting; facilitate insurance billing and reimbursement; permit patients to view their own records, make appointments and refill prescriptions, etc. Additionally, “de-identified” data sets (containing pertinent case details of individuals without revealing patient identity) and public information summaries (giving only aggregated overviews) have research application. It is not surprising that many different professions and perspectives are involved in creating, maintaining and improving the ability to share such data in a responsible way.

Throughout the evolution of these systems, there have been ongoing calls to examine the legal, ethical and practical considerations for data sharing (Greenhalgh *et al.*, 2009;
Gummadi et al., 2014; Hodge et al., 1999). Greenhalgh et al. (2009) note that it has long been realized that “[...] a systematic review of the ethics and practicalities of data sharing is needed [...]”. Such a review should cover topics like the balance between technical security and accessibility; the nature of the trust relationship among the individual, the clinician, and the EPR; the desire (or not) of patients and citizens to view data concerning them; the changing dynamics of the clinical relationship as information inequality is redressed; and the involvement of patients, citizens, and civil liberties groups in influencing policy in this area.” An internationally harmonized conceptual framework, consistent with ethical and privacy principles for data access and information sharing, would indeed be helpful to guide development and implementation of networked information systems. The logical source of such guidance would be an organization, such as the World Health Organization (WHO), which has indeed published a Framework and Standards for Country Health Information Systems as part of the Health Metrics Network, that document provides guidance on how countries should implement healthcare information systems generally (World Health Organization, 2012). As we will discuss in this paper, despite documents like the WHO guidance, responses even among leading individual countries (e.g. Ramanathan et al., 2015) have not been consistent between nations and despite compliance current practices have recognized shortcomings.

It is well recognized that in addition to clinical, laboratory and administrative internal users of EPR systems, EPR data flow into external systems, such as for public health reporting, and there are at least three external groups (academic researchers, journalists and lawyers) who seek information contained in such systems (some as identifiable raw data, others as de-identified data sets). Further, laws and regulations have not kept pace with advances in technology to ensure adequate protection of patient privacy especially as more sophisticated probes and multiple database linkages became possible (Birnbaum et al., 2015). Table IV, in that paper, from a panel discussion at the 2015 international Information Technology and Communications in Health conference outlines current methods for protected data sharing, along with their perceived strengths and weaknesses; its text describes prima facae evidence that current methods used by American public health departments to produce de-identified data sets fail to prevent patient re-identification; and it identifies changes recommended in several countries by leading Information and Privacy Commissioners, public health professionals and informaticians. For an update at the 2017 Information Technology and Communication in Health (ITCH) conference, we were unable to find progress on moving those recommended changes forward in North America. What will it take to improve timely dialogue and co-operation between healthcare practitioners, academic researchers, journalists, regulators in government agencies, legislators and the public to maintain a reasonable balance between legitimate beneficial information access vs essential protection of privacy?

Advances in information technology have impacted all professions that have a vested interest in balancing individual rights with public interests around health data. Over the past several years, challenges faced by the traditional media have raised concerns both for journalists and about journalism (see Table I) (Kruvand, 2012). These concerns span the very definition and ethical constructs of being identified as a journalist, the purposes of news reporting, as well as practical aspects of obtaining reliable information and selecting the best way(s) to convey a particular story. For academic researchers, the rapid development in computing technology and the internet have opened up new sources of the research data, where databases are an essential part of the global science infrastructure; for example, the international Human Genome Project’s openly accessible information being used by many different researchers all over the world for a great variety of purposes (www.genome.gov/10001772/all-about-the-human-genome-project-hgp/). In 2007, the Organisation for Economic Co-operation and Development (OECD) set out recommendations for collective
standards for member countries to implement in support of global research, realizing that
data, in digital form, are increasingly being used in research endeavors beyond the original
project for which they were gathered, including in other research fields and in industry
(www.oecd.org/sti/sci-tech/38500813.pdf). The administrative data from the institutions of
OECD member countries, such as employment information, are now used extensively in the
social sciences, as well as in policy making. Data from academic, clinical and public health
organizations play a growing role in the advancement of life sciences, for example in
stimulating development of vaccines by identifying disease burdens, causative agents, their
means of transmission, disease-causing mechanisms and specific risk groups (Gordon and
Robertson, 2017). Similarly, the geo-spatial data collected by many different government
organizations are essential for environmental and other types of research (https://
canadiangis.com/data.php). Faced with “big data,” legal professionals, like academic
researchers, also have benefitted by advances in information technology. While the volume
of requested evidence in lawsuits can be overwhelming, technology provides lawyers with
the means to determine patterns and relationships among documents, or among people, that
might otherwise go unnoticed in a traditional, manual review. Using eDiscovery software,
predictive coding and data science, lawyers are able to work quickly and efficiently to
prepare, present and settle cases. Data scientists using the semantic modeling to augment
keyword searches are assisting lawyers to determine what information is most useful or
significant. A great deal of background information about an individual is publicly available
on the internet, and lawyers search social media, LinkedIn and the writings of people in place
of lengthy depositions. Fast access to data during direct examination or cross-examination of
a witness means a document that can be searched for and displayed within the courtroom, not
surprisingly, with powerful effect (www.informationweek.com/big-data/software-platforms/
data-lawyers-and-it-how-theyre-connected/a/d-id/1323314). The types of technologies and
tools described above offer great potential; however, if developed and implemented locally
without guidance from an over-arching international framework there is potential to
create incompatibilities instead of effective interoperability and mistrust by the public as to
the uses of their personal health information. In some sectors, like the public health focus of
this paper, ability to implement novel changes in how healthcare information is collected, used
or disclosed by public health agencies also is governed by legislation; in this era of expanding
global networks automating information sharing (e.g. between healthcare providers and local
or regional public health agencies, then between those and national public health agencies like
the US Centers for Disease Control and Prevention, and eventually national agencies with
global entities like the WHO), the present lack of harmonization between the OECD
recommendations, the European privacy by design approach, Canada’s trust model approach
and America’s balance between Health Insurance Portability and Accountability Act of 1996

<table>
<thead>
<tr>
<th>Roles/responsibilities of the media</th>
<th>Challenges faced by the media</th>
</tr>
</thead>
<tbody>
<tr>
<td>Investigate/research</td>
<td>Industry disruption</td>
</tr>
<tr>
<td>Inquire/question</td>
<td>Barriers to accessing information</td>
</tr>
<tr>
<td>Inform/share/discuss</td>
<td>Consolidation of ownership</td>
</tr>
<tr>
<td>Educate</td>
<td>Declining number of science journalists</td>
</tr>
<tr>
<td>Examine/explain</td>
<td>Rise of &quot;new media&quot;</td>
</tr>
<tr>
<td>Collaborate</td>
<td>Rise of infotainment, social media newsfeeds, false stories, opinion over fact, etc.</td>
</tr>
<tr>
<td>Ethical framework</td>
<td></td>
</tr>
<tr>
<td>Truth (accurate/fair)</td>
<td></td>
</tr>
<tr>
<td>Independent</td>
<td></td>
</tr>
<tr>
<td>Accountable</td>
<td></td>
</tr>
<tr>
<td>Minimize harm</td>
<td></td>
</tr>
</tbody>
</table>

Table I.
Balancing individual vs public interest in journalism

Revisiting public health informatics
(HIPAA) covered entity, Safe Harbor redaction conventions and “sunshine” laws approach to privacy protection law underscores the urgency to craft internationally-compatible national laws and standards. Countries like Australia explicitly prohibit attempts at re-identification from de-identified health data sets, other countries do not. Failure of each nation to craft and maintain the best possible information access and privacy protection legislation will undermine public trust, an issue we discuss further below, and the loss of public trust will impede courageous legislative leadership. As Greenhalgh et al. noted in 2009, a unifying harmonized conceptual framework consistent with ethical principles is urgently needed.

The magnitude of benefits from increased data access empowered by advancing data sharing technologies in various sectors of the economy, the value of stolen healthcare data on the black market and the need to safeguard individual privacy are all well recognized (Nelson, 2015).

However, there has been minimal progression in policy to address the evolving access and utilization of personal data originally collected in an EPR. By 2014, it was recognized in Washington State and other American jurisdictions that the American “Safe Harbor” criteria approach for de-identifying individuals in public use data sets were not adequate, and the US “sunshine” laws also prevented sufficient redaction by public health agencies to protect patient privacy (Birnbaum et al., 2015). In the same year, it was formally recognized that the Canada’s trust model approach to privacy also required changes to better protect personal health information (Office of the BC Information and Privacy Commissioner, 2014).

The case for faster progress
Three years later, in 2017, little progress seems to have been made to update privacy legislation in British Columbia (FIPPA & PIPA)[1], and in Canada. The Federal Privacy Act, which covers the personal information-handling practices of federal government departments and agencies, has had minimal substantive updates since it was first introduced in 1983 (www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-privacy-act/parl/ref_rec_161101/). Since 2001, PIPEDA[2], the federal private-sector privacy law, has only been updated in minor ways and now needs to be modernized (www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-privacy-act/parl/20170216; www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-privacy-act/parl/). Similarly in Washington State, no new data sharing legislation has been introduced during this time.

The problem of legislative inaction may be more acute in the USA than in Canada. America’s funded incentives through its HIPAA meaningful use policy initiative have advanced implementation of EPR systems and their linkage through health information exchanges to support electronic reporting networks. These networks have been promoted to serve billing and reimbursement between providers and the Centers for Medicare and Medicaid Services, delivery of laboratory results and health records to authorized providers of healthcare services without redundant rekeying of information, and automation of the legally required public health case reports. While numerous states in the USA have enacted laws that provide various forms of incentives for healthcare industries to use HIEs, this broad sharing of sensitive personal information, potentially without a patient’s knowledge or consent, has raised privacy concerns. Adjerid et al. (2015) found that among all of the states with laws creating HIE incentives, only states that combined incentives with privacy regulatory consent requirements saw a net increase in operational HIEs. When compared to states that did not include requirements for patient consent, those states that addressed consent requirements reported an overall decrease in privacy concerns with their HIEs, resulting in an overall positive impact. Patient portals are being tethered into these systems, with the aim of enabling patients to take a greater role in their healthcare process by accessing records of their own treatment without major security breach concerns (Wang et al, 2004). However, it is noteworthy that successive stages of meaningful use
implementation have steadily been pushed back, hampered by various technological, political and business case conflicts.

Providing patient access with associated education and navigation assistance, in ways that maintain privacy and confidentiality along with strategies to support institutional change, spurred discussion through a 2006 Canadian national survey and workshop on issues, risks and benefits (Wiljer et al., 2008). Five recommendations were made in recognition that patients should have this access but that it will require alignment of international as well as national changes:

1. National infrastructure: there is a need for national standards and guidelines that will ensure that patient-centered care is delivered nationally. The infrastructure will include not only the required IT networks, but also the infrastructure to support the development and dissemination of policies, procedures, security protocols and educational standards. In addition, the infrastructure should engage the public, raise awareness and promote knowledge sharing and patient advocacy.

2. Security and confidentiality: security and confidentiality must be protected according to national standards, but at the same time, a paradigm shift is required so that healthcare organizations create a culture of custodianship, rather than ownership, of patient data. This shift will be achieved by creating models of shared control between healthcare professionals, patients and the public. Healthcare organizations need to be confident they can manage the additional risk exposure in sharing electronic patient information with their users. Patients should have the ability to control the flow of their clinical data and to delegate access to the data.

3. Flexible, interoperable solutions: no solution will fit all of the diverse healthcare settings; therefore, flexibility is required at all levels of the implementation of patient accessible electronic health records (PAEHR), including: first, flexibility for diverse clinical practices; second, flexibility for diverse organizational cultures and approaches to clinical care; third, flexibility for diverse patient groups; fourth, flexibility to accommodate patient choice and promote a patient-centered model of care; and fifth, interoperable solutions to ensure the continuous flow of personal health information.

4. Education: education is required at all levels. Education materials should be developed to support clinicians through the paradigm shifts and cultural changes that are required for patient-centered care models. Public education is required to raise awareness of fundamental rights to access health data. Patient education is also required to help patients understand the nature of the health record itself, including methods of reporting results and tests, and, at the same time, education is required to help patients understand what their clinical data means to them and how they can manage their care to ensure the best possible health outcomes. Healthcare administrators need to be educated on how to deliver and manage PAEHR systems and the costs associated with such practice.

5. Research and evidence-based practice: little is known about the potential risks and benefits of PAEHRs. The research should be a fundamental component of implementing PAEHRs and should focus not only on evaluation research to ensure that the best possible systems are put in place, but also on outcomes research to measure the health benefits in order to identify the real risks and the true benefits.

More recently, Whitt (2016) reminds us of legal precedents in Canada supporting patient access to their health records, increasing complexity in structural relationships between providers and patients, and that “no new ground-breaking court decision has been rendered nor significant new legislation adopting a radically new approach proclaimed.” And even
more recently, a voluntary survey of Canadian physicians (with a notably low response rate of 12 percent) suggests that no more than 10 percent of Canadian patients are now able to view their own health records, book appointments or request prescription renewals online (Leaver, 2017).

Progress toward EPR interoperability has been slower in Canada, where demonstration projects to date in its federal Health Infoway initiative have tended to be insular within specific applications rather than integrated across agencies (www.infoway-inforoute.ca/en/). It should be noted that Canada Health Infoway is only one avenue of digital health in Canada, although a highlighted one. Other pathways provide examples of wider integration (e.g. data holdings of the Canadian Institute for Health Information (www.cihi.ca/en/submit-data-and-view-standards/submission-support-resources) or the Manitoba Centre for Health Policy (http://umanitoba.ca/faculties/health_sciences/medicine/units/chs/departmental_units/mchp/resources/repository/descriptions.html)). Generally, there has been far less progress in Canada than in the USA on creation of patient portals, as well as development in requirements for automating reporting to public health authorities or data format standards to guide vendors in product development. Nevertheless, there is a need to move forward in North America along a path that takes into consideration development of international (not just national) laws and standards to avoid conflict (as illustrated when British Columbia’s Information and Privacy Commissioner raised concerns about the impact of the US Patriot Act on Canadians’ data flowing through internet channels (Information and Privacy Commissioner, 2004)), a concern resurfacing in current trade agreement re-negotiations (Bronskill, 2017). This requires meaningful respect and engagement for all stakeholders and recognition of political inter-agency conflicts. Governments need to engage stakeholders in coordinated processes to produce unifying data dictionaries, record format standards and related guidance so that commercial EPR and EPR-related applications software developers have a common understanding of sufficient functionality, security and interoperability. Last but not least, it is essential for everyone to appreciate a business case for compatible privacy laws and software standards, as well as the marketing reality concerns of the private sector vendors, upon which all other stakeholders rely to develop these new information technology products.

What framework might help guide the path forward?
The OECD Privacy Framework with its ten principles has, since 1980, been foundational in the global development of privacy legislation, regulations, policy and practice. Recognizing the significant changes to the collection, use and movement of personal information over the past 30 years, the Organization for Economic Co-operation and Development revised the Framework in 2013 to reflect the role of technological advancements in the frequency and complexity of interactions involving personal data. Regulators and privacy professionals faced challenges in applying the traditional privacy principles in an environment that was more globally connected than ever before, for example:

- an increased volume of personal data being collected, used and stored;
- a wider range and types of analytics used for personal data, providing insights into individual and group trends, movements, interests and activities;
- the value of societal and economic benefits enabled by new technologies and responsible uses of personal data;
- the extent of threats to the privacy of personal information;
- the number and variety of actors capable of either putting privacy at risk or protecting privacy;
the frequency and complexity of interactions involving personal data that individuals are expected to understand and negotiate; and

- the global availability of personal data, supported by communications networks and platforms that permit continuous, multipoint data flows.

Regulators proposed three main strategies as the most effective way to meet these challenges in balancing legitimately timely access to information and protecting personal information:

1. develop a national privacy strategy that is multifaceted and coordinated at the highest levels of government;

2. require all entities that collect personal information, private or public and big or small, to develop and maintain a privacy management program through which the organization would be expected to implement privacy protection activities; and

3. revise privacy legislation to include data security breach notification to regulators and to the individuals affected, and to provide the actual and potential risk of harm to the individual caused by the breach (Organization for Economic Co-operation and Development, 2013).

It is understandable that progress cannot be rushed on something so complex as seamlessly shifting healthcare from its traditional paper-based records and face-to-face interactions into a predominantly digital world. This requires major changes not only in providing appropriate technology, but also changes in many laws, remuneration policies, cultural norms, and convincing assurance of safety and security. However, given the ever-evolving nature of threats to enshrined rights and expectations of patient privacy and confidentiality, it is not understandable that progress is not steadily made as a priority in this aspect.

What would be required in a national privacy strategy that would meet the needs of the clinical, journalistic, legal and research communities and also be acceptable to information-sharing preferences of patients and their proxies when patients themselves are unable to make decisions (Caine and Hanania, 2013; Brown et al., 2016)? And how should funders and legislators be engaged to ensure that resulting frameworks are truly implementable? How do we define these needs in specific terms? And how do we ensure that a cadre of information access and privacy specialists are appropriately educated, credentialed and kept current so that privacy legislation will be applied and interpreted properly instead of misinterpreted in practice? These questions presumably fall under the purview of congressional and parliamentary committees, as well as state and provincial legislatures. However, the legislative climate has been described as not being conducive for introducing new bills to address serious security weaknesses, we discussed at the previous biennial international ITCH conference (Birnbaum et al., 2015). The regulatory authority in public health informatics therefore remains hampered, but not for lack of comprehensive example solutions. How should legislation address the issue of re-identification? For example, Australia provides one approach which involves the introduction of legislation that prohibits the intended re-identification of de-identified government data (see www.mondaq.com/australia/x/537580/data+protection/Reidentification+of+deidentified+government+data+to+be+criminalised). A second example is the privacy management program model supported by regulators and privacy commissioners, which includes an accountability framework, risk assessment tools, security controls and reporting requirements for monitoring progress (www.oipc.bc.ca/guidance-documents/1435). Third, the concept of “privacy by design” encompasses the development of IT systems, accountable business practices and physical design including networked infrastructure, with its proactive rather than reactive foundational principle, an important consideration for EPRs (Cavoukian, 2011).
Impetus for legislative change

What factors will contribute to reverse the current climate of legislative reluctance and propel us forward toward more responsible data sharing? We believe the drivers for change will come from two extremely important factors: the digital economy and individual data ownership.

In every area of society, it can be stated new technologies hold promise of important benefits. Future economic growth will come in large part from a digital economy, and North America is well placed to become a world leader in technological advancement including artificial intelligence, which depends on the collection and use of massive amounts of data. However, in a public opinion poll reported in February 2017 by the Privacy Commissioner of Canada (www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2017/por_201703_consent/), the vast majority of Canadians expressed worry they are losing control of their personal information, with 92 percent of Canadians expressing concern, and 57 percent being very concerned, about a loss of privacy. This lack of trust in the collection, use and disclosure of personal information does not bode well for the digital economy as individual trust is required for and by industry to reap the benefits made possible through innovation. That essential trust may be undermined by recent legislation in the USA that allows internet service providers to sell their users’ personal data without a user's explicit permission (Johnson, 2017), which is contrary to the stronger privacy protections in Canada (Braga, 2017), and the increased attention this contested difference is drawing in current trade agreement re-negotiations (Bronskill, 2017).

The concept of data ownership means that an individual has exclusive domain over their personal information, and must provide meaningful consent for an entity to collect, use and disclose that information in accordance with privacy laws. Meaningful consent is only valid if it is reasonable to expect that the individual understands the nature, purpose and consequences of the collection, use or disclosure of personal information to which they are consenting. Complicating this context is that unlike licensed medical service providers and clinical laboratories, direct-to-consumer commercial genomic services do not operate under the same legal constraints on ownership and privacy, which has raised concerns (e.g. see, www.councilforresponsiblegenetics.org/genewatch/GeneWatchPage.aspx?pageId=285). In the age of “big data,” the Internet of Things, artificial intelligence and robotics, obtaining meaningful consent has become increasingly challenging for organizations. A 2017 study by the Privacy Commissioner of Canada found a strong relationship exists between trustworthiness of an organization and meaningful consent by an individual (www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2017/por_201703_consent/). In an ever-competing digital economy, organizations could enhance their trustworthiness with consumers through the use of privacy by design, demonstrable accountability with a privacy management program and adopt industry codes of best practice. On the other side of the coin, consumers are requesting targeted legislation to prevent specific harms such as cyberbullying and revenge porn, improved education on safe and appropriate use of the internet (especially for vulnerable populations). This will require improving practices for websites and social network platforms, enhancing regulators’ enforcement powers to actively promote organizational compliance with privacy legislation, and proactively conducting more performance audits.

Recognizing the importance of information privacy in a digital economy, the 2016 OECD Ministerial Declaration on the digital economy committed, among other things, to an international effort to protect privacy, establishing its importance for economic and social prosperity, and its criticality for building consumer trust to enable a vibrant, robust and competitive digital economy. In 2018, the General Data Protection Regulation (GDPR) will come into force in the EU and will affect the collection, use and disclosure of personal information on a global scale (https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf). As the GDPR requires reviews of adequacy decisions every four years, the acceptability of privacy
laws (and regulatory enforcement) in the USA and Canada will be continually reviewed for compliance. Currently the Canadian PIPEDA has an adequacy status of “partial” (January 2017 Communication from the European Commission), and all future adequacy decisions will involve a comprehensive assessment of Canada’s privacy regime, including access to personal data by public authorities for law enforcement, national security and other public interest purposes. The US Department of Commerce has implemented the EU-US and Swiss-US Privacy Shield Frameworks (www.privacyshield.gov/Program-Overview) to provide entities on both sides of the Atlantic with a mechanism to comply with data protection requirements when transferring personal data from the European Union and Switzerland to the USA in support of transatlantic commerce. Organizations voluntarily self-certify for Privacy Shield status to benefit from the adequacy determinations. While joining the Privacy Shield is voluntary, once an eligible organization makes the public commitment to comply with the Framework’s requirements, this commitment becomes enforceable under the US law.

Thus, it appears the seeming legislative inertia is time-limited as the needs of a global digital economy and a more privacy-informed public require – no, demand – how information will be used in future. As has been stated by Professor Klaus Schwab (2015), Founder of the World Economic Forum, “we stand on the brink of a technological revolution that will fundamentally alter the way we live, work, and relate to one another. In its scale, scope, and complexity, the transformation will be unlike anything humankind has experienced before.” This Fourth Industrial Revolution is characterized by a blurring of lines between the physical, digital and biological spheres. The transformation, he posits, will occur at exponential speed; and evidence of this dramatic change is already all around us (mobile supercomputing, intelligent robots, self-driving cars, neuro-technological brain enhancements, Genetic editing).

At the heart of his analysis is the conviction that the Fourth Industrial Revolution is within the control of all of us, as long as we are able to collaborate across geographies, sectors and disciplines to grasp the opportunities it presents. One of the greatest individual challenges posed by these new information technologies is privacy. While instinctively, we understand why privacy is essential, a crucial part of this new connectivity is the tracking and sharing of information about us. Given these imperatives, by 2019 at the next international ITCH conference, we hope to be able to report solutions implemented that restore confidence in the balance between legitimate data access, protection of individuals’ information privacy and enhanced security for sensitive databases.

Notes
2. Canada’s Personal Information Privacy and Electronic Documents Act.

References


Corresponding author
Paulette Lacroix can be contacted at: placroix@placroix.ca