Proposing a Charter of Personal Data Rights

Our personal data is being created, collected, mined, analyzed, monitored, shared, sold, stored, and used for diverse reasons beyond most of our knowledge or control, let alone our willing consent or endorsement. A charter of personal data rights is needed to temper this datafication of people's lives, which compromises personal privacy, confidentiality, trust, and security.

Marc Kosciejew, Ph.D.

In this data-saturated world, many important political, economic, and social activities increasingly provide opportunities for access to and use of *personal data* – that is, information relating to an individual as an identified or an identifiable person. It is being harnessed and exploited by powerful institutions and interests for diverse purposes.

Every day, personal data is given to these institutions and interests or, increasingly, simply taken by them to permit participation in the information ecosystem upon which many aspects of public and private life now depend. Those who want to participate, it is argued, must be willing to hand over their personal data.

It is no wonder why the World Economic Forum declared personal data as a new economic asset class or why analysts and officials were led to describe it as the 21st century's version of oil and the new currency of the digital world.

Types of Data Collected

The kinds, quantities, and values of personal data being given, or taken, are enormous and varied: employment histories, educational backgrounds, familial ties, social connections, professional networks, financial records, medical profiles, personal propensities, daily routines, and other everyday engagements, some of which people may

be unaware, are being collected and analyzed.

Personal data regarding who people are, who they know, who they are connected to, where they are, where they have been, and even where they may be going is being aggregated. It is consequently under threat by those who are able to harness and exploit it for their own benefit, usually to the detriment of those whose personal data it is.

For example, personal data is being created or collected

Personal data fundamentally belongs to the person it identifies, stands in for, and represents; it should not be treated as the property of powerful institutions or interests, governmental, corporate, or otherwise.

by powerful commercial enterprises for their own financial profit of which people tend not to receive any share. It also is being monitored by government agencies for their own Big Brother-esque surveillance and security activities, regardless of whether those being watched have ever been suspected of criminal activity.

The Threat of Datafication

These threats to personal data are, in fact, threats to people's physical selves. It is not simply a collection of meaningless bytes about random information abstracted from their lives. It is integral to their very personhoods, an informational extension or a kind of personal appendage that extends their lives into the informational (which increasingly means "digital") realm. This means that it is people – not just data – being exploited.

Personal data fundamentally belongs to the person it identifies, stands in for, and represents; it should not be treated as the property of powerful institutions or interests, governmental, corporate, or otherwise. As such, people have certain rights to their personal data. Indeed, personal data rights are basic human rights that must be recognized, respected, and protected.

There is particular urgency for the recognition of and respect for personal data as human rights because, as many aspects of people's lives continue to migrate online, they are, in turn, being datafied. Every transaction, interaction, connection, and contribution are being transformed into distinct data points to be aggregated with so-called big data sets in order to more effectively surveil individuals for diverse purposes.

Even those individuals who are not connected online are caught up in this digital panopticon as many mundane activities, from walking down a street to riding a bus or making a commercial purchase, are captured and datafied by various information communication technologies (ICTs). This datafication of people's lives seriously compromises personal privacy, confidentiality, trust, prospects, and security.

Balance Needed

Admittedly, there must be an appropriate balance between personal data rights and the legitimate and legal interests of those who may collect and use this information. There are some political and economic interests that are of societal and individual import, such as the refinement and delivery of particular social services, programs, or products.

But, as Aleecia M. McDonald from Stanford Law School's Center for Internet and Society reminds us, "We have learned the hard way that we cannot trust companies or governments to exercise basic decency and restraint in collecting [and managing, storing, using, etc.] our data."

For example, Edward J. Snowden's revelations of the U.S. National Security Agency's widespread surveillance practices, coupled with the complicity by many important players in the ICT and Internet industry, have serious (worldwide) political and economic implications for governments and corporations alike.

A March 21 *New York Times* article, "Revelations of N.S.A. Spying Cost U.S. Tech Companies," examined how these practices and their resulting violations of personal rights have negatively affected the bottom lines of many ICT and Internet companies and eroded much public and commercial trust in them. Indeed, there are substantive political and economic risks for governments, corporations, and other powerful institutions and interests that violate personal data rights.

A Call to Action

There is growing momentum for the recognition of personal data rights. Brazil recently approved the draft bill Marco Civil da Internet, heralded as a Constitution for the Internet that will enshrine individuals' rights to access and use the World Wide Web.

The European Union also recently approved new rules strengthening net neutrality to help ensure equal access to the Internet, and it is working on revised digital privacy regulations.

Tim Berners-Lee, the creator of the World Wide Web, recently called for a Magna Carta bill of rights for the Internet that should be considered on the same level as human rights. In a March 12 *BBC.com* article, "Tim Bern-

A Charter of Personal Data Rights

In response to the datafication of people's lives, which seriously compromises personal privacy, confidentiality, trust, prospects, and security, this charter of personal data rights is proposed.

Everyone has the following personal data rights:

- The right to own their personal data.
- The right to control and use their personal data.
- The right to privacy regarding their personal data.
- The right to anonymity regarding their personal data.

ers Lee: World wide web needs bill of rights," he challenges us "to make a big communal decision. In front of us are two roads: which way are we going to go? Are we going to continue on the road and just allow the governments [and corporations] to do more and more and more control; more and more surveillance? Or are we going to set up a bunch of values? Are we going to set up something like a Magna Carta for the World Wide Web and say, actually, now it's so important, so much part of our lives that it becomes on a level with human rights?"

He argues that we "have to be constantly aware, constantly looking out for [increasing encroachment on these rights] – constantly making sure through action, protest, that it doesn't happen." At the center of this call to action is personal data. When Internet rights are respected, so are personal data rights, and vice versa.

A Charter of Personal Data Rights

This article responds to Berners-Lee's call to action by proposing a Charter of Personal Data Rights. The aim is to increase awareness and contribute to the momentum towards ensuring that personal data rights are recognized and treated as human rights. This charter proposes four personal data rights, as explained below.

1. Everyone has the right to own their personal data.

As Ann Cavoukian, the Information and Privacy Commissioner of Ontario, Canada, noted in "Personal Data Ecosystem (PDE) – A *Privacy by Design* Approach to an Individual's Pursuit of Radical Control," "When individuals "When individuals go about their daily activities online, it is said that they also release, on average, 700 pieces of personal information a day. It is this stream of data that organizations profit from [that many of which] believe they have the right to control [and ultimately own] this information so that they can extract its value."

Governments and corporations increasingly treat personal data as their proprietary assets that they can collect, store, use, and reuse indefinitely and for whatever purposes they want; indeed, they regard personal data in a similar way to how the energy industry sees untapped reserves of oil and gas. It is theirs to use, distribute, and charge for as they please.

There is a saying that if you are not paying for the product or service, you *are* the product or service. Many online apps, services, and products are, seemingly, free of charge. But as MIT scholar Alex Pentland argues, "You have a right to *possess* your data." In "Reality Mining of Mobile Communications: Toward a New Deal on Data" from the *Global Information Technology Report 2008-2009,* he explains that third parties "should adopt the role of a Swiss bank account for your data. You open an account (anonymously, if possible), and you can remove your data whenever you'd like."

This charter supports this perspective, arguing that while individuals may consent to *share* some kinds of personal data, in limited and specific ways and for limited and specific reasons or functions, this consent does not mean that they have handed over ownership of their personal data. They have the right to both possess and determine how it will be used.

2. Everyone has the right to control and use their personal data.

By virtue of their right to ownership, individuals consequently have the right to determine how their personal data is created, collected, managed, stored, shared, and otherwise manipulated.

Pentland suggests that "if you're not happy with the way a company [or some other third party] uses your data, you can remove it. All of it. Everything must be opt-in, and not only clearly explained in plain language, but with regular reminders that you have the option to opt-out."

Further, individuals have the right to be informed about the processing of their personal data, which must comply with the original specific and limited reasons for which it was created or collected, as well as the right to correct it in cases of mistakes or misinformation.

This right to control and use personal data supports Cavoukian's call for "radical control" of personal data, which she describes as "the level of personal control necessary for an individual to exercise 'informational self-determination.'"

She explains that radical control should be enabled and protected by data protection policies and procedures adopted, and it should be designed and embedded within

ICTs and Internet services. ICTs, for example, should be formatted to enable individuals' control over their personal data when navigating, participating, and interacting within the digital realm.

Personal privacy, in many cases, is becoming a luxury good in this data-saturated world. Privacy comes at a literal and figurative price: those who want privacy have to pay for it through a company or service that claims to protect and ensure it …

3. Everyone has the right to privacy regarding their personal data.

People's personal data privacy is being continually encroached by many parties, from government agencies to ICT and Internet companies, who regard this information as theirs. Many powerful institutions and interests have growing desires for personal data resulting in their disregard for many basic privacy protections. People's privacy is compromised when they lack ownership, control, and use over their personal data.

Personal privacy, in many cases, is becoming a luxury good in this data-saturated world. Privacy comes at a literal and figurative price: those who want privacy have to pay for it through a company or service that claims to protect and ensure it; further, those who want to be connected have to give up some of their privacy. Thus, instead of privacy being the default, access to an individual's private life is, indeed, a matter of course.

But the right to privacy is a human right and a core principle of any free society. The right to privacy must be applied to personal data since it is an information extension of individuals.

Cavoukian, for example, proposes the idea of "privacy by design" built within ICTs, digital services and products, and other informational technologies and settings. Privacy by design would ensure that privacy is the default for all such systems and services instead of it being an afterthought or ignored altogether.

When privacy itself is the default, individuals will be able to better exercise their rights to own, control, use, and, of course, keep private their personal data. Privacy should not have any kind of price tag, literal or figurative.

4. Everyone has the right to anonymity regarding their personal data.

Anonymity through obscurity can no longer be assumed. This data-saturated world is achieving a level of surveillance over people's lives through their personal data that would have been the envy of the former East Germany.

As a scholar on digital security, Ron Deibert writes in *Black Code: Inside the Battle for Cyberspace*, "We no longer move about our lives as self-contained beings, but as nodes of information production in a dense network of digital relations involving other nodes of information production. All of the data about us as individuals…is owned, operated, managed, and manipulated by third parties beyond our control."

With personal data being increasingly collected, analyzed, and used, individuals lose their anonymity. Individuals' right to their personal data being and remaining anonymous requires them to be able to: have any or all of it either removed or erased by the party storing or using it; withdraw consent for or opt out of it being collected; and demand abstention from any further dissemination or use.

Applying the Charter

How can this charter be implemented? In a recent *Foreign Affairs* article, "Privacy Pragmatism: Focus on Data Use, Not Data Collection," Craig Mundie, the senior advisor to the CEO of Microsoft, offers five main recommendations that he refers to as "privacy pragmatism" that governments, companies, and individuals can take to protect their personal data.

1. Use metadata for access control.

The first step Mundie proposes is to annotate, or wrap, personal data in metadata at its point of origin. He asserts that this metadata wrapping "would describe the rules governing the use of the data it held [and] any programs that wanted to use the data would have to get approval to 'unwrap' it first."

2. Impose auditing requirements.

Robust legal and industry regulations should be established to "impose a mandatory auditing requirement on all applications that used personal data, allowing authorities to follow and observe applications that collected personal information to make sure that no one misused it and to penalize those who did," Mundie writes.

3. Encrypt data rights.

ICTs, software, etc. can use encryption and further metadata to embed personal data rights within their services, programs, and products, providing "individuals and organizations a simple and manageable way to protect confidential or sensitive information."

4. Connect data with verified identities.

Governments and the appropriate regulators must create and employ systems connecting legally recognized personal data to individuals. If an individual's preferences for his or her personal data are to be respected and enforced, the personal data must be verified to be that person's authoritative and correct information.

Mundie notes, moreover, that even with proper ways "to more rigorously connect individuals with verifiable online identities, three additional kinds of validated 'identities' would need to be created: for applications, for the computers that run them, and for each particular role that people play when they use an application on a computer." Thus, "only specific combinations of identities would be able to access any given piece of personal data."

5. Punish violators.

The final recommendation is to establish substantive penalties for the violation of personal data rights like privacy. Mundie writes that the violation of personal data rights should "be considered serious criminal offenses, akin to fraud and embezzlement – not like the mere 'parking tickets,' which would not deter rogue operators and companies."

Thus, if people believe their personal data has been violated, they could contact the appropriate regulator who, in turn, "would investigate and prosecute the abuse, treating it as a crime like any other."

Momentum for Charter of Personal Data Rights

As illustrated by Berners-Lee's Internet privacy campaign and the national legislation mentioned in this article, there is growing momentum for the right of people to control their personal data to be recognized as a human right.

There may be resistance and ridicule regarding the recognition of such a charter, particularly because it disrupts the current information practices of many government and corporate parties with vested interests in the status quo. Nevertheless, remembering that no one is exempted from the continuing and increasing expropriation of personal data, it is crucial that these rights be recognized and respected. **END**

Editor's Note: This is the first in an occasional series of editorial/opinion articles meant to provoke reader feedback, including comments and counter-point articles. Send your comments or completed article proposal forms (available at *http://archive.arma.org/imm/IM%20Mag%20Proposal%20Form.doc)* to *editor@armaintl.org*.

Marc Kosciejew, Ph.D., *can be contacted at* mkosciej@gmail.com. *See his bio on page 47.*