The rise of cybersecurity and its impact on data protection

Article *in* International Data Privacy Law · May 2017

DOI: 10.1093/idpl/ipx009

5 authors, including:

Dan Jerker B. Svantesson
Bond University
183 PUBLICATIONS **1,454** CITATIONS
SEE PROFILE

Orla Lynskey
The London School of Economics and Political Science
35 PUBLICATIONS **734** CITATIONS
SEE PROFILE

Christopher Millard
Queen Mary, University of London
121 PUBLICATIONS **1,361** CITATIONS
SEE PROFILE

Editorial

The rise of cybersecurity and its impact on data protection

Christopher Kuner*, Dan Jerker B. Svantesson**, Fred H. Cate***, Orla Lynskey*** and Christopher Millard***

Cybersecurity is attracting more attention than ever—not just in headlines, but among policymakers, industry leaders, academics, and the public. Successful cyberattacks are becoming more frequent and threatening as adversaries become more determined, more sophisticated, and more likely to be connected with a nation state. No one and nothing seems safe. The May WannaCry ransomware attack affected more than 300,000 computers in 150 countries. The presidential elections in France and the United States (U.S.) have been the subject of major attacks, followed by strategically timed disclosures. Yahoo, in the midst of its sale to Verizon, reported that information of approximately 1.5 billion user accounts had been stolen. In the United States (U.S.), the NSA and the CIA appear to be haemorrhaging top secret documents apparently stolen by insiders, while the U.S. Office of Personnel Management was unable to protect 21.5 million records on government employees and contractors holding security clearances.

Part of the escalating attention to cybersecurity is the result of society's growing reliance on digital systems to control important infrastructure, such as cars, airplanes, utilities, supply chains, and industrial systems. In 2010, for example, the U.S. and Israel reportedly cooperated in the development and use of Stuxnet, a software program that destroyed centrifuges critical to Iran's nuclear weapons program by inferring with their control systems. Hackers used cyberattacks to temporarily shutter three power distribution companies in western Ukraine and operations at a Venezuelan oil unloading facility. In 2014, cyberattacks on a German iron plant caused widespread damage. In 2015, thieves stole $81 million by exploiting weak security at the Central Bank of Bangladesh to persuade the network that controls international transfers of money between banks to transfer the money from the Federal Reserve Bank of New York to the thieves' accounts. The following year, the Mirai botnet exploited vulnerabilities in the Internet of Things devices to overwhelm the Dyn domain server, causing major Internet platforms and services to be unavailable in the U.S. and Europe. Enterprising security researchers have hacked insulin pumps, drones in flight, and cars on the road.

It is no wonder that cybersecurity is attracting more attention, but such attention raises important issues for personal privacy and the data protection tools we use to protect it. The relationship between security and data privacy has always been complicated. Privacy depends absolutely on security. No obligation to provide privacy, whether entered into voluntarily or compelled by law, will be meaningful if the data to be protected are accessed or stolen by unauthorized third parties. As a result, all modern data protection principles include an obligation to protect security as well. For example, the influential 1980 *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, adopted by the Committee of Ministers of the Organization for Economic Cooperation and Development (OECD) in 1980, included the Security Safeguards Principle as one of the eight foundational principles of data protection: 'Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.' This principle was retained in the 2013 revision of the Guidelines (the OECD Privacy Framework), and supplemented by additional security-related language covering data breaches. And security has been recognized in every significant codification of data protection law since then, including the EU Data Protection Directive, the U.S. Federal Trade Commission's fair information practice principles, the APEC Privacy Framework, and the EU General Data Protection Regulation.

* Editor-in-Chief.
** Managing Editor.
*** Editor.

Data privacy and cybersecurity are often advanced by common tools, such as encryption, data minimization, and limits on collecting, retaining, and transferring personal data. In short, what is good for privacy is often good for security as well.

But this is not always the case. Despite the foundational importance of information security for modern data protection and the considerable overlap between many tools for protecting privacy and security, privacy and security are often in tension as well. Many measures employed to enhance cybersecurity pose a risk to privacy. For example, proposals to enhance cybersecurity by requiring identity verification, reducing online anonymity, and sharing potentially personal information about cyberattacks all pose risks for personal privacy. This tension is more than theoretical: concerns about the privacy impact of proposed data sharing legislation in the U.S. led to widespread protests online and offline, delayed its passage for more than four years, and resulted in a substantially weakened final law.

Whatever the relationship between the legal tools used for protecting privacy and security, the greatly expanded focus on cybersecurity poses other challenges for privacy and the professionals in public and private sectors who work to protect it, such as the following:

- The commitment of an ever-increasing portion of scarce resources in industry and government to addressing cybersecurity challenges threatens to diminish investment in data protection. This is not just a matter of money. Institutions only have so much bandwidth, and as more time, attention, and resources are focused on enhancing security, privacy runs the risk of being shortchanged.
- Data protection officials and practitioners often face a Hobson's choice of leaving information security (and the resources that go with it) to others or adding information security to their portfolios, at the risk of diminishing their attention to privacy.
- Historically, when security and privacy priorities have competed head-on, privacy is lost. We see evidence of this following major terrorist attacks, when national governments consider and, in many cases, adopt private-restrictive measures based on the premise that it is necessary to sacrifice a little privacy in the cause of greater security. This bargain rarely proves productive, yet we run the risk of repeating it in the context of measures designed to enhance cybersecurity.
- Privacy is deeply rooted in human rights principles and law; cybersecurity historically has not been. A greater focus on cybersecurity runs the risk of diminishing the individual and human rights components of data protection law.
- Many data protection professionals in industry and government have historically lacked training or experience in computer science or other technologies. Fortunately, this is beginning to change. However, pressure to focus more attention on cybersecurity issues runs the risk of concentrating too much on technology and neglecting other important skills, to the detriment of both privacy and security.

These risks are real and growing. However, the intensified attention to cybersecurity also presents opportunities, including these:

- By drawing attention to the challenges of information governance broadly, the growing focus on cybersecurity may lead to increased funding and other resources for privacy work as well. This is especially true because security is so integral to privacy and public acceptance of new security measures often depends, at least in part, on the degree to which those measures protect privacy.
- Enhanced attention to information security, and especially the sense of urgency with which these threats must be addressed, may lead not only to more attention being given to privacy as well, but also to greater insistence that data protection tools, like cybersecurity tools, adapt and change more readily to the challenges of the 21st century. Data protection law has rarely been thought nimble; pressure to deal with cybersecurity may help change that.
- The importance of technological skills for cybersecurity professionals may intensify the movement towards more data protection professionals trained in technologies as well. At the same time, the broader range of disciplines traditionally applied to privacy may help facilitate a much-needed expansion of cybersecurity competencies as well. After all, the vast majority of successful cyberattacks involves human or institutional failures, so greater attention to human and institutional behaviour, training, incentives, and risk management is key to enhancing cybersecurity, being applied to privacy.
- The human rights foundations of data protection law could benefit efforts to improve cybersecurity as well. For years, many institutions calculated the 'cost' of information security breaches only in terms of the losses suffered by the institution. A greater understanding that information security, as a component of data protection, is not just a financial obligation, but a human rights obligation might contribute to a broader accounting of the harms that may be caused

by breaches and the range of parties who may be injured.

Civilization needs better protection for cybersecurity—far better than we have seen to date–urgently, but it also needs better data protection. The significance of the possible effects on data protection—both positive and negative—of the increased attention being paid to cybersecurity suggests that privacy professionals in government, industry, civil society, and academia should, at a minimum, be paying close attention to the emergence of cybersecurity. Even better would be to think constructively and proactively about how to take advantage of this important development to ensure that people everywhere enjoy strong, effective protections for their privacy and for the security of their data.

doi:10.1093/idpl/ipx009