Office of the
Privacy Commissioner
of Canada

Privacy and Cyber Security

Emphasizing privacy protection in cyber security activities

December 2014

Table of Contents

Abstract

This research report examines the common interests and tensions between privacy and cyber security. It explores how challenges for cyber security are also challenges for privacy and data protection, considers how cyber security policy can affect privacy, and notes how cyberspace governance and security is a global issue. Finally, it sets out key policy directions with a view to generating dialogue on cyber security as an important element of online privacy protection.

Introduction

As "cyberspace" has become central to the global information and communication infrastructure, the security of cyberspace has now become a more urgent priority for corporations and governments around the world.[1] In fact, the *Digital Canada 150* strategy, launched in April 2014, complements Canada's cyber security strategy by making Protecting Canadians one of its five pillars.[2] According to the 2010 document *Canada's Cyber Security Strategy* (the "*Strategy*"), *cyberspace* is "the electronic world created by interconnected networks of information technology and the information on those networks. It is a global commons where more than 1.7 billion people are linked together to exchange ideas, services and friendship."[3] The term "cyber security," though not defined in the *Strategy*, is generally understood to encompass any measures taken to protect online information and secure the infrastructure on which it resides.[4]

Technologies that are ubiquitous, interconnected, and allow easy access to the Internet have become deeply integrated in everyday life. As a result, we increasingly depend on cyberspace for social, economic and political interactions. The web provides a platform for a whole range of critical infrastructure sectors and services, such as health care, food and water, finance, information and communication technology, public safety, energy and utilities, manufacturing, transportation and government.[5] Cyberspace connectivity augments all of these critical infrastructure sectors and is therefore vital to Canada's future economic growth.[6]

At the same time, the online environment has increasingly been subjected to sophisticated and targeted threats; our ever-increasing reliance on cyberspace is creating new and significant vulnerabilities.[7] This risk is magnified by a number of factors: more valuable electronic data is being stored and processed on a massive scale, much of it in the cloud; powerful and portable computing devices such as smartphones, tablets and laptops are increasingly integrated into every aspect of our lives; information is shared, combined and linked with other information with greater frequency; and third-party relationships (e.g.: outsourcing to a cloud provider) are the norm. Unless all components are equally secure, the entire system is vulnerable as cyber criminals are often skilled at exploiting weaknesses in cyberspace.

For example, in 2011, Canada suffered a significant security breach when the computer systems of three key federal government departments were penetrated.[8] Although no personal information was known to have been compromised in the attack, the hackers were able to steal highly sensitive documents and force the departments offline for months.[9] In 2012, the Auditor General of Canada observed that the Government's response to the 2011 breach revealed that systems were clearly vulnerable and good information security practices were not being consistently followed.[10] The Auditor General also commented that implementation of the *Strategy* had been slow to date, leaving the nation's capacity to secure cyberspace extremely underdeveloped.[11] More recently, in 2014 much of the cyber world had to deal with "Heartbleed", a security bug which revealed a vulnerability in commonly-used encryption. This bug opened the door to possible compromise of usernames, passwords and other sensitive content from a variety of websites, including popular social media sites, web-based e-mail providers and a number of e-commerce sites.[12] In addition, the recent malware "Blackshade" allowed for the capture of information on a victim's computer, including

keystrokes, photographs, documents and passwords to access online accounts. These events were sobering reminders of the fragility of the Internet, and reinforced the importance of cyber security.

The *Action Plan 2010-2015 for Canada's Cyber Security Strategy* (the *"Action Plan"*), released in April 2013, outlined the progress to date as well as the Government's ongoing plans to implement the *Strategy* which has been augmented by the April 2014 release of *Digital Canada 150,* focusing on five pillars: connecting Canadians, protecting Canadians, economic opportunities, digital government and Canadian content.[13] Since 2010, the Government of Canada has structured its *Strategy* and *Action Plan* around three pillars: 1) securing federal government systems, 2) partnering to safeguard vital cyber systems outside the federal government and 3) helping Canadians to be secure online.[14] The public awareness component of the *Strategy* has received the highest profile to date. Since its launch, the Government of Canada has made public awareness and outreach efforts a priority, informing Canadians about ways to protect and safeguard their personal information in the digital sphere.[15]

For example, as the private sector carries significant responsibility for cyber security, much of the information generated and stored in cyberspace is not within the control of individual users, but rather is in the hands of many private sector and third party providers. Given that the private sector is also largely responsible for the critical infrastructures in Canada,[16] the second pillar of the *Strategy* and *Action Plan* recognizes that many of the risks and impacts of cyber incidents are shared between public and private sectors.

Privacy protection and cyber security should be thought of as interconnected: as more and more personal information is processed or stored online, privacy protection increasingly relies on effective cyber security implementation by organizations to secure personal data both when it is in transit and at rest.[17] In some cases, cyber security measures underpin critical infrastructure that protects data, thereby safeguarding personal information.

However, as with many security measures, certain cyber security efforts can also threaten privacy; the relationship between cyber security and privacy is not a completely harmonious one. Cyber security activities can require up-to-the-second monitoring of activities on a network in order to detect anomalies and threats, and in some cases, monitoring of this nature could involve capture and analysis of massive amounts of personal information.

1. Cyber Security Challenges

A report from the World Economic Forum released in January 2014 examines the need for new approaches to increase resilience against cyber attacks and suggests that the failure to effectively secure cyberspace could result in an aggregate impact of approximately US$ 3 trillion by 2020.[18] However, many of the challenges for cyber security are also challenges for privacy and data protection. Cyber security is by no means a static issue with a permanent solution. Threats to information in cyberspace evolve quickly and, more recently, have expanded into new channels such as social media and mobile technologies. As organizations strive to keep pace with the changing landscape created by innovative technologies, social practices and ever-changing threats, data produced, collected and collated on a massive scale can be left vulnerable to those cyber threats. The following are some of the emerging challenges for data protection and cyber security.

a) Complexity of the connected environment

The continuing evolution of cyberspace, as a fully electronic world created by interconnected networks in parallel with our physical environment, is characterized by an enormous amount of data. The modern economy increasingly depends on vast quantities of digital data that are generated through financial transactions, communications, entertainment, travel, shopping, online browsing, and hundreds of other

routine activities.[19] Data elements are continually being combined, connected, compared and linked to other information as organizations try to capitalize on its value and to offer new and improved services to their users. The electronic systems and digital networks that facilitate these transactions and communications also capture our preferences and other personal details, and track our online and, increasingly, physical movements. The volume of data generated in cyberspace can only increase exponentially once the "Internet of things" becomes a reality, and sensors within devices autonomously report on location, status, surrounding environment, provide real-time updates or help monitor and control devices remotely.[20]

Cyberspace has become inherently complex to manage and challenging to secure. Increased, persistent connectivity through a greater range of mobile devices and "always on" services, third-party business relationships, cloud computing infrastructures, information sharing agreements, and other "seamless" or automated business processes in cyberspace continue to pose shared risks to cyber security and privacy. Threats in cyberspace will continue to target the weakest links in any complex web of business relationships or government processes, meaning stakeholders in cyber security efforts have a shared role in protecting the infrastructure and the information that flows through it.

b) Growing sophistication of the threat

Online threats may be invisible but their effects are very real, and interconnected systems that are globally accessible are inherently vulnerable. As the scale of information flowing through cyberspace has expanded, so too has its value to corporations, government, and those with malicious intent. Our data trails now leave a larger footprint across cyberspace , leaving us more exposed to threats.[21] Wherever there is an opportunity to profit there is usually a market for criminal activity, but as Gabriella Coleman notes, there has also been a "professionalization" of hacking[22] and cyber-crime, making these activities much more sophisticated.[23] State-sponsored threats, conducted or condoned by a nation state, are also becoming increasingly common.[24] These are sometimes referred to as Advanced Persistent Threats (APTs) and are usually well educated, well-resourced adversaries who focus on the theft of secrets including intellectual property.[25]

Ronald Deibert, Director of the Canada Centre for Global Security Studies and the Citizen Lab at the Munk School of Global Affairs, University of Toronto, explains that cyber-crime is growing in frequency and complexity for several reasons: "First, the number of users coming online, including individuals, businesses, organizations, and governments is growing rapidly, creating a growing baseline of potential targets. Second, the ways in which we communicate and share information online has changed fundamentally over the last several years, with the growth of social networking, cloud computing and mobile forms of connectivity. We share more data with each other, entrust it to third parties outside our immediate control, and click on links and documents over social networking platforms and services with a greater degree of frequency."[26] Third, he argues that because companies rarely disclose security breaches to the public for competitive and reputational reasons, there is limited information about how attacks are carried out, which could ultimately hinder cyber security efforts.[27]

c) Threats are moving to the mobile sphere

In the next three years, the number of cellphones in use will exceed the global population.[28] Our mobile devices can contain a goldmine of personal information. People routinely carry their mobile devices everywhere and use them for almost anything imaginable; people communicate with friends, access email, take photos and video and upload it to the web, play games, track distances, locate nearby stores and restaurants, find directions to specific locations, access their bank accounts, surf the web, monitor their health/physical activity, keep track of appointments or log to-do lists. Organizations are all striving to reach consumers and clients on the devices they use every day, but alongside all of these conveniences for the consumer is the possibility for new vulnerabilities or opportunities for cyber threats.

The International Cyber Security Protection Alliance (ICSPA) recently released a cyber-crime study that highlighted mobile communications and cloud services as today's new targets for the cyber-criminal.[29] The study notes that one of the significant concerns facing the mobile industry is how to address the skyrocketing amount of malware on mobile devices. Malware can easily be distributed to mobile devices through malicious apps within smartphone app stores which appear safe.[30] Furthermore, the use of free public Wi-Fi can also put mobile devices at increased risk of having data intercepted.[31] Malware can target mobile devices used for near-field communications transactions and compromise "tap-and-pay" functionality.[32] ICSPA's study concludes that mobile malware is a key emerging threat in cyberspace. Although it has been argued that cyber criminals are building better malware specifically designed for mobile devices, actual infection rates on devices are low, for the present, since the distribution of malware to mobile devices has not yet been perfected.[33] This can be expected to change in the near future.

As cyber threats increasingly target mobile devices, data protection becomes all the more critical. Communications and transactions using mobile devices are more closely tied with individual users, sensors within mobile devices can be enabled to locate devices with a high degree of precision, and features built into the devices or apps that people download can track, record and store personal information, upload contact lists, communications and transactions. Faced with these mounting risks, the mobile industry, companies and app developers have a heightened responsibility to ensure the safety of the platforms and the backend systems, where so much personal information is collected, handled and stored.

d) The "big data" paradox: is it a bigger risk or a solution?

"Big data" can be defined as vast stores of information gathered from both traditional sources and, increasingly, new collection points (e.g. web data, sensor data, text data, time and location data gleaned from social networks).[34] The insights derived through analysis of big data are often touted as the solution to almost any problem or issue.[35] However, this data-driven approach raises two distinct issues from a cyber security perspective: how to secure information in a big data context and the use of new data analytics to sift through network information including personal information, in order to predict security incidents.[36]

In the same way that data ("big" or not) is considered a valuable commercial asset, it is also likely to be valuable to cyber-attackers. Security breaches will have a potentially serious impact upon "big data" providers, as the use of big data is fairly new to most organizations and the vulnerabilities and risks may not be well understood. Organizations that decide to use big data analytics may introduce new potential security vulnerabilities, or opportunities for malicious data input.[37] An additional concern is that "big data" begets "bigger data"; as the capabilities to collect data increase, so does the temptation to do so.

Proponents of big data analysis have claimed that it could play a key role in helping detect cyber threats at an early stage by using sophisticated pattern analysis and combining and analyzing multiple data sources.[38] Moreover, big data has been touted as a crucial problem-solving tool, capable of improving public safety and security[39], saving energy[40] and improving healthcare.[41] On the other hand, the inherent complexities of those same multiple data points and integration across platforms will also bring more complexity in the safeguards required to protect the information. Certainly, evidence exists which shows privacy concerns arise by virtue of the fact that big data analytics quite often means unrestricted collection of data, and sophisticated analysis that can yield very personal insights about individuals. This is also a process that could potentially motivate secondary uses of personal information that are unreasonable. Peter Wood, Chief Executive Officer of First Base Technologies LLP and a member of the ISACA London Chapter Security Advisory Group, explains that the crux of the issue is that big data's volume and velocity "expands the boundaries of existing information security responsibilities and introduces significant new risks and challenges."[42]

e) For many, breach preparedness is still not a priority

In recent years, reports of privacy breaches have become increasingly common, with potentially significant consequences for affected individuals. Many of the risks and impacts of cyber incidents are shared between governments and the private sector, but it is most often the private sector that is on the front line in confronting these threats, given that they control the vast majority of the telecommunications infrastructure.[43] Several recent reports have indicated that a large number of businesses are unprepared for, and indifferent to, cyber threats, and lack proper contingency plans.[44]

Cyber security issues have plagued Canadian companies in recent years.[45] ICSPA's study of the impact of cyber-crime found considerable gaps in Canadian businesses' preparedness against cyber-crime overall, but stated that generally, large businesses may be better prepared to deal with shifting threats, which are very real, and in constant evolution.[46] The main cyber-crime threats (as perceived by the businesses who responded to the survey) include malware and virus attacks, sabotage of data or networks, financial fraud, phishing/social engineering, theft of laptops/devices, unauthorized access or misuse of website, misuse of social networks by employees, denial of service, telecommunications fraud, and Advanced Persistent Threats.[47] The study revealed that most Canadian businesses that responded (69%) had no procedure in place to follow when cyber-crime is identified, and only 22% reported that they employ a risk assessment process to identify where they were most vulnerable.[48] This is concerning given that the survey revealed the prevalence of cyber-crime among Canadian businesses, with 69% reporting some kind of attack within a twelve-month period.

At the same time as organizations appear to be unprepared for cyber threats and breaches, individuals are expressing their desire to know if and when they may be affected by a breach. The OPC's 2013 survey of Canadians found respondents were uncertain whether they would be notified if the personal information they have given an organization was lost, stolen or unintentionally exposed: 59% thought it unlikely; 41% thought it probable. However, virtually all Canadians (97%) who responded said they would want to be notified,[49] which seems to indicate they would support improvements in how organizations treat information security and breach response. In a business survey commissioned by the OPC in 2014, 58% of respondent businesses indicated that they do not have guidelines in place in the event that personal information of their customers has been breached.[50] Lack of organizational preparedness and low valuation of impact would appear to suggest that breach preparedness has not yet become a business priority.

f) Compliance vs. risk-management

Organizations are required to comply with various laws and regulations in order to operate in particular jurisdictions or across various jurisdictions. When it comes to security, however, a mechanical approach to compliance does not necessarily mean that the organization is secure.[51] In fact, blindly pursuing compliance may actually put an organization at increased risk specifically because it is focused on a "check-the-box" compliance model leading to a false sense of security, whereas performing proper risk management requires organizations to scour and identify areas where additional safeguards are needed.[52] A risk management approach naturally complements compliance obligations. The challenge for organizations is to understand that security is not simply a matter of meeting minimal compliance standards, but rather, a question of engaging in effective risk management and dynamic implementation of security.[53]

2. Cyber Security Policy Developments

Cyber security is an incredibly complex and changing policy issue. No country, organization or individual is ever completely immune to cyber risks, and approaches to protecting against cyber threats can vary greatly depending on the values and decisions that underlie cyber security activities.[54] In fact, the issue of cyber security involves much broader issues of internet governance. Two divergent views of cyber security

regulation have emerged: one favours a harmonized approach to governance which protects openness, privacy and interoperability across regions – the "open commons" approach. The other advocates stronger governmental control and regulatory landscape – the "gated community" approach.[55]

It has been argued that cyber security is more than a technical issue because it pertains to the security of an entire communications ecosystem.[56] In that regard, while cyber security will inevitably require some technical developments, it will also require the development of social norms, global collaboration, and a regulatory framework that includes multiple stakeholders. As stakeholders consider cyber security policy directions, it will be essential to ensure that the dialogue around cyber security includes the acknowledgement of its link to data protection, trust, and privacy. The following section will consider cyber security policy developments and foreign policy considerations.

a) Stewardship vs. securitization[57]

As cyber security policy is developed at a national level, there is a risk that national security and public safety objectives could take a predominant role in formulating responses to cyber threats, at the expense of privacy protection.[58] In this manifestation, cyber security policy could enable what Deibert describes as the "*securitization* of cyberspace – a transformation of the domain into a matter of national security." [59] In an era when national security is so often used to justify extraordinary intrusions on individual privacy, it will be vital to ensure that cyber security strategies and activities do not endorse building massive surveillance regimes for unlimited and unending monitoring and analysis of the personal information of individuals.[60] Cyber security efforts should not expand surveillance to the detriment of individuals' privacy, civil liberties or other democratically held values.[61] Governments must build in the necessary checks and controls to reflect the privacy norms we ascribe to as a society.

As an alternative, Deibert presents an argument for a *stewardship* approach to cyber security, where "governments, NGOs, armed forces, law enforcement and intelligence agencies, private sector companies, programmers, technologists, and average users must all play vital and interdependent roles as stewards of cyberspace."[62] The concept of stewardship in cyber security acknowledges that cyberspace belongs to no one in particular, but that everybody has an influential role to play in shaping its foundation and a stake in its evolution.[63]

This alternative approach recognizes that cyber security is a shared responsibility because of the ways in which cyberspace is interconnected and interdependent, and the role all organizations have to play to ensure that their actions do not introduce security risks into cyberspace in general, or fail to uphold privacy principles.[64] A stewardship approach also calls for accountability on all of the stakeholders involved in cyber security: "Securing cyberspace requires a reinforcement, rather than a relaxation, of restraint on power, including checks and balances on governments, law enforcement, intelligence agencies, and on the private sector."[65] As holders of vast amounts of personal information, it is logical to expect that the private sector assume some responsibilities to protect the infrastructure of cyberspace and the personal information that flows through it.

Both approaches, built-in government controls and the broader stewardship model, have their merits and may, in fact, be complementary.

b) Cyberspace governance and security is a global issue

Given that information flowing through cyberspace is not constrained by national borders, "with whom we share data and where it ultimately resides in cyberspace is an inherently international concern."[66] As such, citizens of every country face similar risks in the protection of their privacy rights. Issues of cyber security and privacy protection are global challenges that require a global response.

The *Action Plan* called on the Department of Foreign Affairs, Trade and Development Canada (DFATD) to develop a foreign cyber policy that ensures that activities in cyberspace are aligned with broader foreign policy, international trade and security objectives.[67] International groups such as the G8, the Organization for Security and Co-operation in Europe (OSCE), and Organization for Economic Co-operation and Development (OECD) are developing principles in support of the right to cyberspace access, openness, freedom of expression and user privacy. However, these very principles can be odds with domestic national security or public safety objectives, and also with suppliers, who create cyber security products with built-in capabilities to track users, monitor network traffic, and filter content.[68]

As cyber security policy directions develop, privacy and data protection authorities have a role to play to reinforce privacy values to ensure that cyber security policy respects privacy rights, and prioritizes personal information protection.

As one such data protection authority, the OPC is perceived as a key player engaged in shaping international cyberspace governance due to the Office's efforts to ensure that online service offerings from international companies uphold Canadians' right to privacy in accordance with Canadian standards for privacy protection.[69] International co-operation in the areas of cyber security and privacy protection will continue to be essential to address the transborder and cross-organizational challenges for cyber security and data protection.[70] In 2013, Peter Hustinx, then European Data Protection Supervisor, acknowledged that cyber security issues have to be addressed at an international level through international standards and cooperation.[71] Hustinx also commented that "while measures to ensure cyber security may require the analysis of some personal information of individuals, for instance IP addresses that can be traced back to specific individuals, cyber security can play a fundamental role in ensuring the protection of privacy and data protection rights in the online environment, provided the processing of this data is proportionate, necessary and lawful."[72]

3. Conclusion: Emphasizing privacy protection in cyber security activities

As individuals grow more dependent on and connected to the cyberspace, they will become more reliant on organizations' effective implementation of cyber security and sensitivity to privacy. The following are some of the key areas in which an increased emphasis on privacy protection could help support, advance and augment cyber security activities.

a) Building privacy values into cyber security policy directions

We know that certain degrees of monitoring, logging, data mining or surveillance will create tensions or conflicting requirements between privacy and cyber security efforts. As Canada's Interim Privacy Commissioner stated in 2011, "violating people's privacy in the interest of ensuring cyber security would defeat the very purpose of cyber security."[73] While cyber security activities may require some degree of monitoring in order to be able to detect anomalies and protect cyber infrastructure and information, cyber security strategies and activities should not be an excuse for building massive surveillance regimes for unfettered monitoring and analysis of the personal information of individuals. Privacy regulators and advocates have a role to play to ensure that cyber security strategies, principles, action plans and implementation activities promote privacy protection both as a guiding principle and an enduring standard.

In its 2013-2014 Report on Plans and Priorities, the Department of Foreign Affairs, Trade and Development Canada (DFATD) committed to establishing a cyber security foreign policy to promote Canada's Internet-related economic, security and foreign policy interests.[74] This priority stems directly from the *Action Plan* and is part of the Government's overall plan to implementing the *Strategy* as launched in 2010. DFATD has foreign policy responsibilities for coordinating Canada's participation in international undertakings to support cyber

security initiatives, including the Council of Europe *Convention on Cybercrime*, of which Canada is a signatory.[75]

There are clear advantages to building cyber security into programs and activities from the start rather than retroactively mitigating cyber risks after the fact. Undertaking preventative measures to ensure security – and informing consumers of the potential risks and how they have been mitigated – can foster trust in individuals using the internet.

b) Legislative approaches that incentivize cyber security preparedness

The private sector carries a significant responsibility for cyber security because it controls so much of the infrastructure and information in cyberspace. The volume and range of personal information that organizations collect make it a valuable asset for organizations, but also a valuable asset for bad actors. In the competitive rush to innovate and develop new technologies, services and applications, organizations may not be doing enough to adequately assess cyber risk. Too often personal information is treated like a commodity, and is monitored, aggregated, collected, used, disclosed and retained with little regard for the impacts on privacy. Too many organizations leave themselves vulnerable to breaches either through a lack of preparation or an undervaluation of impact, and all too frequently seem to accept data loss as a cost of doing business.

The *Action Plan* commits to improving legislative tools to protect Canadians in cyberspace. This legislative promise includes *Canada's Anti-Spam Legislation* (CASL) [76] which came into force in July 2014, and the data breach notification requirements contained in Bill S-4, the *Digital Privacy Act*, introduced April 2014.

The private sector is unquestionably faced with complex and significant challenges in protecting cyberspace. The web of business relationships, persistent connectivity, and greater range of devices and channels makes cyberspace inherently complex and challenging to secure. Still, as stewards of massive amounts of personal information, the private sector has a responsibility and shared role in protecting the infrastructure of cyberspace and the personal information that flows through it.

There is no simple solution to the persistent and ever-changing threats to privacy in cyberspace. Any legislative solutions need to be carefully considered to ensure they are balanced and that there is accountability for personal information protection. Practical cyber security implementation should involve identifying personal information as a critical asset in need of protection, identifying the vulnerabilities that put personal information at risk, and implementing safeguards to protect against the risks identified without in turn impeding on privacy rights or other values such as openness and freedom of expression. Generating dialogue with the private sector on the vital components of cyber security implementation may uncover areas in their cyber risk assessments and privacy safeguards that still need to be strengthened.

c) Facilitating broader dialogue on cyber security that acknowledges its importance for privacy, trust, and responsible data stewardship

The complexities of cyberspace and the mounting sophistication of threats necessitate that organizations do more about privacy protection, particularly with respect to cyber security efforts. Security safeguards are a key element of the ability to protect personal information and preserve privacy in cyberspace, with technical safeguards being only one aspect of an overall risk management approach to cyber security and personal information protection. It is no longer enough to simply be compliant with privacy requirements or technical safeguards to the minimum extent possible. Protection of personal information requires giving effect to all privacy principles, and practicing privacy compliance throughout the lifespan of the information, including: demonstrating accountability, being transparent, practicing data minimization, ensuring appropriate use and

disclosure, implementing effective access controls, and abiding by reasonable retention periods and safe destruction methods.

Equally, the interconnectivity and shared risks in cyberspace puts responsibility on all stakeholders to shape cyberspace and cyber security on a foundation of enduring trust. Cyber security efforts will require global collaboration and a stewardship approach that ensures there is accountability and checks and balances on all stakeholders involved in cyber security activities. Privacy regulators have a role to play in this broader dialogue about global stewardship to ensure that cyber security efforts are based on a balanced and proportional risk management approach that effectively protects personal information and respects privacy rights.

Notes

[1] Deibert, Ron. *Distributed Security as Cyber Strategy: Outlining a Comprehensive Approach for Canada in Cyberspace*. Prepared for the Canadian Defence & Foreign Affairs Institute, August 2012.

[2] See the Government of Canada's *Digital Canada 150* (2014) at http://www.digitaleconomy.gc.ca.

[3] Government of Canada Cyber Security Strategy (2010) http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/cbr-scrt-strtgy-eng.pdf.

[4] There is no commonly recognized definition for cyber security. ISO/IEC 27032/2012 defines cyber security as the "preservation of confidentiality, integrity and availability of information in the Cyberspace."

[5] See Public Safety Canada's website for list of critical infrastructure sectors. http://www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/index-eng.aspx.

[6] '*Canada and Cyberspace: Key Issues and Challenges*' (2012) a report prepared by The SecDev Group, commissioned by the Department of Foreign Affairs and International Trade Canada (DFAIT).

[7] This is acknowledged in the *Action Plan 2010-2015 for Canada's Cyber Security Strategy* (the Action Plan). Released April 2013.

[8] The departments affected were Department of Finance, Treasury Board of Canada Secretariat, and Defense Research and Development Canada. This reference comes from '*Canada and Cyberspace: Key Issues and Challenges*' (2012) a report prepared by The SecDev Group, commissioned by the Department of Foreign Affairs and International Trade Canada (DFAIT).

[9] '*Canada and Cyberspace: Key Issues and Challenges*' (2012) a report prepared by The SecDev Group, commissioned by the Department of Foreign Affairs and International Trade Canada (DFAIT).

[10] Fall Report of the Office of the Auditor General (2012), Chapter 3 - Protecting Canadian Critical Infrastructure Against Cyber Threats.

[11] See Fall Report of the Office of the Auditor General (2012), Chapter 3 - Protecting Canadian Critical Infrastructure Against Cyber Threats and '*Canada and Cyberspace: Key Issues and Challenges*' (2012) a report prepared by The SecDev Group, commissioned by the Department of Foreign Affairs and International Trade Canada (DFAIT).

[12] The Heartbleed Hit List: the passwords you need to change right now. Accessed online at http://mashable.com/2014/04/09/heartbleed-bug-websites-affected/.

[13] Government of Canada's *Digital Canada 150* (2014) at http://www.digitaleconomy.gc.ca.

[14] *Action Plan 2010-2015 for Canada's Cyber Security Strategy* http://www.publicsafety.gc.ca/prg/ns/cybr-scrty/_fl/ccss-ctn-eng.pdf.

[15] The OPC has already been involved in projects that helped to raise awareness among Canadian citizens and small businesses across Canada about cyber security and its importance to personal information protection. In 2010, the OPC launched the *Privacy for Small Business online tool* designed to help SMEs build customized privacy plans. In 2011, the OPC developed an article series offering cyber security advice and tips for small business. The OPC also worked collaboratively with Public Safety to review the section of its Cybersafe web site providing information to individuals on how to protect themselves. See: GetCyberSafe.gc.ca. Also related is OPC Guidance on Apps, and Fact Sheets on protecting personal information on mobile devices: Privacy on the Go: 10 Tips for Individuals on Protecting Personal

Information on Mobile Devices and Privacy on the Go: 10 Workplace Tips for Protecting Personal Information on Mobile Devices.

[16] See Public Safety Canada's *Get Cyber Safe* Blog, October 29, 2013. "So… what is critical infrastructure anyways?" http://www.getcybersafe.gc.ca/cnt/blg/pst-20131029-eng.aspx.

[17] OPC Speech: New Platforms, New Safeguards: Protecting Privacy in Cyberspace (February 23, 2011).

[18] World Economic Forum report on *Risk and Responsibility in a Hyperconnected World,* released January 20, 2014.

[19] Center for Applied Cybersecurity Research, Indiana University. *Roundtable on Cyber Threats, Objectives, and Responses: A Report*. December 2012.

[20] Business Insider "Everything You Need To Know About The New Internet—The 'Internet Of Things', Julie Bort, Published March 29, 2013. Accessed online October 7, 2013 at: http://www.businessinsider.com/what-you-need-to-know-about-the-internet-of-things-2013-3?op=1#ixzz2h3ge4p7R.

[21] Discussed in an Interview with Ron Deibert, found at: http://ww3.tvo.org/video/193823/ron-deibert-surveilling-cyberspace.

[22] "Hacking" is the commonly used term, however the technically correct term is "cracking" - a shortened form of "criminal hacking". Hacking, in the original sense of the word, is figuring out how things work. Where the term "hacking" is used throughout the paper, it is meant to refer to criminal hacking activities, aka "cracking". For more on hacking, see the work of Gabriella Coleman; in particular, Politics and Publics http://gabriellacoleman.org/wp-content/uploads/2012/08/Coleman-hacker-politics-publics.pdf or Hacker Practice: Moral Genres and the Cultural Articulation of Liberalism at http://steinhardt.nyu.edu/scmsAdmin/uploads/003/679/255.pdf.

[23] Google Big Tent Canada 2013, *Google Demonstration: Cyber security in Action*. May 30, 2013.

[24] Ibid.

[25] 'Study of the Impact of Cyber Crime on Businesses in Canada.' *International Cyber Security Protection Alliance* (May 2013) p. 33.

[26] Deibert, Ron. *Distributed Security as Cyber Strategy: Outlining a Comprehensive Approach for Canada in Cyberspace*. Prepared for the Canadian Defence & Foreign Affairs Institute, August 2012. Page 11-12.

[27] Ibid.

[28] '*Canada and Cyberspace: Key Issues and Challenges*' (2012) a report prepared by The SecDev Group, commissioned by the Department of Foreign Affairs and International Trade Canada (DFAIT).

[29] Study of the Impact of Cyber Crime on Businesses in Canada.' *International Cyber Security Protection Alliance* (May 2013) The study was sponsored by Above Security, Blackberry, Lockheed Martin and McAfee.

[30] 'Study of the Impact of Cyber Crime on Businesses in Canada.' *International Cyber Security Protection Alliance* (May 2013) page 28.

[31] Ibid, page 36.

[32] McAfee 2013 Threats Predictions Report, McAfee Labs. http://www.mcafee.com/ca/resources/reports/rp-threat-predictions-2013.pdf.

[33] This argument is based on the view that most Android malware is found hidden in apps sold or given away for free in online stores other than the official Google Play store, which scans for malicious code. See Computerworld 'Windows malware finds its way to Android', by Antone Gonsalves, published August 16, 2013. Accessed online October 4, 2013 at http://blogs.computerworld.com/mobile-security/22662/windows-malware-finds-its-way-android?source=CTWNLE_nlt_security_2013-08-19.

[34] "Big Data and Analytics: Seeking Foundations for Effective Privacy Guidance," *Centre for Information Policy Leadership*, February 2013.

[35] "Why Data Analytics is the Future of Everything," *Bloomberg TV*, November 21, 2013. Google Executive Chairman Eric Schmidt and Civis Analytics Chief Executive Officer Dan Wagner discuss the way big data can change everything from corporate strategy to the way people vote. They spoke with Trish Regan at Bloomberg's The Year Ahead: 2014 conference at the Art Institute of Chicago. http://www.bloomberg.com/video/why-data-analytics-is-the-future-of-everything-WeneeY4LQzKJ4khYdMi9uw.html.

[36] Peter Wood. "How to tackle big data from a security point of view," *Computer Weekly,* March 4, 2013. Accessed online September 5, 2013 at http://www.computerweekly.com/feature/How-to-tackle-big-data-from-a-security-point-of-view.

[37] Ibid.

[38] There are a multitude of products available, see for example IBM and SAS.

[39] See "Yes, Big Data Can Solve Real World Problems" *Forbes*, December 2013 at http://www.forbes.com/sites/gregsatell/2013/12/03/yes-big-data-can-solve-real-world-problems/.

[40] Michael Bendewald, How Energy Managers can Leverage Big Data Right Now, FacilitiesNet, April 2013; http://www.facilitiesnet.com/energyefficiency/article/How-Energy-Managers-Can-Leverage-Big-Data-Right-Now--13976#.

[41] Rebecca Walberg, Value of big data in health care is measured not just in dollars, but in lives, Financial Post, February 2014; http://business.financialpost.com/2014/02/05/value-of-big-data-in-health-care-is-measured-not-just-in-dollars-but-in-lives/?__lsa=dd3e-6a53.

[42] Peter Wood. "How to tackle big data from a security point of view," *Computer Weekly,* March 4, 2013. Accessed online September 5, 2013 at http://www.computerweekly.com/feature/How-to-tackle-big-data-from-a-security-point-of-view

[43] Deibert, Ron. *Distributed Security as Cyber Strategy: Outlining a Comprehensive Approach for Canada in Cyberspace*. Prepared for the Canadian Defence & Foreign Affairs Institute, August 2012.

[44] See, for example, Symantec "New Survey Shows U.S. Small Business Owners Not Concerned About Cybersecurity; Majority Have No Policies or Contingency Plans" (Oct 2012); "Canadian businesses unprepared for cyber attacks: Queen's University expert" (May 2013); Computerworld.au "Companies still unprepared for cyber attacks: Deloitte" (February 2013); CBC "Canadian companies open to cyber attacks, says federal agency" (July 2013).

[45] This has been noted in several sources including: Deibert, Ron. *Distributed Security as Cyber Strategy: Outlining a Comprehensive Approach for Canada in Cyberspace*; Misha Glenny "Canada's weakling Web defences" *Globe and Mail*, May 18, 2011; Fall Report of the Office of the Auditor General (2012), Chapter 3 - Protecting Canadian Critical Infrastructure Against Cyber Threats; Alexandra Posadzki "Cyber security in private sector a 'significant' problem: Public Safety records" The Canadian Press, July 14, 2013. Matthew Braga "Canada must ramp up cyber security in wake of alleged China-led attacks, experts say" *Financial Post,* February 19, 2013.

[46] 'Study of the Impact of Cyber Crime on Businesses in Canada.' *International Cyber Security Protection Alliance* (May 2013).

[47] Ibid.

[48] Ibid.

[49] *Survey of Canadians on Privacy Related Issues*. Prepared for the Office of the Privacy Commissioner of Canada by Phoenix Strategic Perspectives Inc. 2013.

[50] Survey of Canadians on Privacy Related Issues. Prepared for the Office of the Privacy Commissioner of Canada by Phoenix Strategic Perspectives Inc. 2014.

[51] Info Security "Gartner Says Risk-Based Approach will Solve the Compliance vs Security Issue," published August 8, 2013.

[52] Ibid.

[53] Ibid.

[54] Deibert, Ron. 'Canada and the Challenges of Cyberspace Governance.' University of Calgary School of Public Policy (SPP) Communique. Vol 5, Issue 3, March 2013.

[55] '*Canada and Cyberspace: Key Issues and Challenges*' (2012) a report prepared by The SecDev Group, commissioned by the Department of Foreign Affairs and International Trade Canada (DFAIT).

[56] See Deibert, Ron. 'Canada and the Challenges of Cyberspace Governance.' University of Calgary School of Public Policy (SPP) Communique. Vol 5, Issue 3, March 2013.

[57] Concepts from Deibert, R. & Rohozinski, R; "Risking Security: Policies and Paradoxes of Cyberspace Security," *International Political Sociology* (2010), as quoted in Deibert, Ron. *Distributed Security as Cyber Strategy: Outlining a Comprehensive Approach for Canada in Cyberspace*. August 2012, and Deibert, Ronald J. (2013) *Black Code: Inside the Battle for Cyberspace*. McClelland & Stewart.

[58] Dupont, Benoit "The proliferation of cyber security strategies and their implications for privacy." *Circulation international de l'information et sécurité.* Karim Benyekhlef and Esther Mijans (eds.) Les Éditions Thémis. Page 67-80, 2013. Accessed online June 17, 2013 at http://www.benoitdupont.net/node/145.

[59] Deibert, R. & Rohozinski, R; "Risking Security: Policies and Paradoxes of Cyberspace Security," *International Political Sociology* (2010), as quoted in Deibert, Ron. *Distributed Security as Cyber Strategy: Outlining a Comprehensive Approach for Canada in Cyberspace*. August 2012.

[60] Deibert, Ronald J. (2013) *Black Code: Inside the Battle for Cyberspace*. McClelland & Stewart.

[61] Ibid.

[62] Ibid.

[63] Ibid.

[64] ISO/IEC 27032:2012(E) Information Technology – Security Techniques – Guidelines for Cybersecurity (published 16 July 2012) http://webstore.iec.ch/preview/info_isoiec27032%7Bed1.0%7Den.pdf.

[65] Deibert, Ronald J. (2013) *Black Code: Inside the Battle for Cyberspace*. McClelland & Stewart.

[66] Deibert, Ron. *Distributed Security as Cyber Strategy: Outlining a Comprehensive Approach for Canada in Cyberspace*. Prepared for the Canadian Defence & Foreign Affairs Institute, August 2012.

[67] *Action Plan 2010-2015 for Canada's Cyber Security Strategy* (the Action Plan). Released April 2013.

[68] See page 35 in '*Canada and Cyberspace: Key Issues and Challenges'* (2012) a report prepared by The SecDev Group, commissioned by the Department of Foreign Affairs and International Trade Canada (DFAIT). Suppliers in the US, Canada and Europe are the main producers of tools that enable deep packet inspection, content filtering, social network mining, cellphone tracking, and computer network attacks.

[69] See page 6 in '*Canada and Cyberspace: Key Issues and Challenges'* (2012) a report prepared by The SecDev Group, commissioned by the Department of Foreign Affairs and International Trade Canada (DFAIT).

[70] Address by Chantal Bernier, "New Platforms, New Safeguards: Protecting Privacy in Cyberspace." Remarks to the Centre for National Security organized by the Conference Board of Canada.

[71] EDPS Opinion. Opinion of the European Data Protection Supervisor on the Joint Communication of the Commission and of the High Representative of the European Union for Foreign Affairs and Security Policy on a 'Cyber Security Strategy of the European Union: an Open, Safe and Secure Cyberspace,' and on the Commission proposal for a Directive concerning measures to ensure a high common level of network and information security across the Union. Brussels, June 17, 2013.

[72] EUROPA News Release: "Credible Cyber Security Strategy in the EU needs to be built on Privacy and Trust." June 17, 2013. http://europa.eu/rapid/press-release_EDPS-13-6_en.htm?locale=en.

[73] Address by Chantal Bernier, "Balancing privacy and law enforcement panel." Remarks at a Conference entitled "Securing the Cyber Commons: A Global Dialogue", organized by the Canada Centre for Global Security Studies, the Munk School of Global Affairs, the University of Toronto and the SecDev Group (March 28, 2011).

[74] Department of Foreign Affairs, Trade and Development Canada (DFATD) Report on Plans and Priorities for 2013-2014 available at http://www.international.gc.ca/department-ministere/assets/pdfs/RPP_2013_2014_ENG.pdf.

[75] Also known as the Budapest Convention, this document is the only binding international instrument designed specifically to combat cybercrime. The Budapest Convention serves as a guideline for developing comprehensive national legislation against cybercrime and as a framework for international cooperation between State Parties. It is available for consultation at http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/default_en.asp.

[76] See *Canada's Anti-Spam Legislation* website at http://fightspam.gc.ca/eic/site/030.nsf/eng/h_00211.html.