UNIVERSITY OF TORONTO

munk school
OF GLOBAL AFFAIRS & PUBLIC POLICY

# Standing Committee on Public Safety and National Security

## *Cybersecurity in the Financial Sector as a National Economic Security Issue*


Submission by

Dr. Christopher Parsons

Research Associate

Citizen Lab, Munk School of Global Affairs & Public

Policy at the University of Toronto



munkschool.utoronto.ca

**At Trinity College**
1 Devonshire Place
Toronto, ON
Canada M5S 3K7
T: 416.946.8900 F: 416.946.8915

**At the Observatory**
315 Bloor Street West
Toronto, ON
Canada M5S 0A7
T: 416.946.8929 F: 416.946.8877

**At the Canadiana Gallery**
14 Queen's Park Crescent West
Toronto, ON
Canada M5S 3K9
T: 416.978.5120 F: 416.978.5079

# Introduction

1. I am a research associate at the Citizen Lab, Munk School of Global Affairs & Public Policy at the University of Toronto. My research explores the intersection of law, policy, and technology, with a focus on national security, data security, and data privacy issues. I submit these comments in a professional capacity representing my views and those of the Citizen Lab.

# The State of Computer Insecurity

2. Canadian government agencies, private businesses and financial institutions, and private individuals rely on common computing infrastructures. Apple iPhones and Android-based devices are used for professional and private life alike, just as are Microsoft Windows and MacOS. Vulnerabilities in such mobile and personal computing operating systems can prospectively be leveraged to obtain access to data on the targeted devices themselves, or utilized to move laterally in networked computing environments for reconnaissance, espionage, or attack purposes. Such threats are accentuated in a world where individuals routinely bring their own devices to the workplace, raising the prospect that personal devices can be compromised to obtain access to more securitized professional environments.
3. The applications that we rely on to carry out business, similarly, tend to be used across the economy. Vulnerabilities in customer service applications, such as mobile banking applications, affect all classes of businesses, government departments, and private individuals. Also, underlying many of our commonly used programs are shared libraries, application programming interfaces (API), and random number generators (RNG); vulnerabilities such codebases are shared by all applications incorporating these pieces of code, thus prospectively endangering dozens, hundreds, or thousands of applications and systems. This sharedness of software between the public and private sector, and professional and private life, is becoming more common with the growth of common messaging, database, and storage systems, and will only become more routine over time.

4. Furthermore, all sectors of the economy are increasingly reliant on third-party cloud computing services to process, retain, and analyze data which is essential to business and government operations, as well as personal life. The servers powering these cloud computing infrastructures are routinely found to have serious vulnerabilities either in the code powering them or, alternately, as a result of insufficient isolation of virtual servers from one another. The result is that vulnerabilities or errors in setting up cloud infrastructures prospectively enable third-parties to inappropriately access, modify, or exfiltrate information.
5. In summary, the state of computer insecurity is profound. New vulnerabilities are discovered -- and remediated -- every day. Each week new and significant data breaches are reported on by major media outlets. And such breaches can be used to either engage in spearphishing -- to obtain privileged access to information that is possessed by well-placed executives, employees, or other persons -- or blackmail -- as was threatened in the case of the Ashley Madison disclosures -- or other nefarious activities. Vulnerabilities affecting computer security, writ large, threaten the financial sector and all other sectors of the economy, with the potential for information to be abused to the detriment of Canada's national security interests.

# Responsible Encryption Policies

6. Given the state of computer (in)security, it is imperative that the Government of Canada adopt and advocate for responsible encryption policies. Such policies entail commitments to preserving the right of all groups in Canada -- government, private enterprises, and private individuals -- to use computer software using strong encryption. Strong encryption can be loosely defined as encryption algorithms for which no weakness or vulnerability is known or has been injected, as well as computer applications that do not deliberately contain weaknesses designed to undermine the effectiveness of the aforementioned algorithms.
7. There have been calls in Canada,[1] and by law enforcement agencies in allied countries,[2] to 'backdoor' or otherwise weaken the protections that encryption

[1] RCMP's ability to police digital realm 'rapidly declining,' commissioner warned, https://www.cbc.ca/news/politics/lucki-briefing-binde-cybercrime-1.4831340.
[2] In the dark about 'going dark', https://www.cyberscoop.com/fbi-going-dark-encryption-ari-schwartz-op-ed/.

provides. Succumbing to such calls will fundamentally endanger the security of all users of the affected computer software[3] and, more broadly, threaten the security of any financial transactions which rely upon the affected applications, encryption algorithms, or software libraries.

8. Some of Canada's closest allies, such as Australia, have adopted irresponsible encryption policies which run the risk of introducing systemic vulnerabilities into the software used by the financial sector, as well as other elements of the economy and government functions.[4] Once introduced, these vulnerabilities might be exploited by Australian intelligence, security, or law enforcement agencies in the course of their activities but, also, by actors holding adversarial interests towards Canada or the Canadian economy. Threats activities might be carried out against the SWIFT network, as just one example.[5]
9. It is important to note that even Canada's closest allies monitor Canadian banking information, often in excess of agreed upon surveillance mechanisms such as FINTRAC. As one example, information which was publicly disclosed by the Globe and Mail revealed that the United States of America's National Security Agency (NSA) was monitoring Royal Bank of Canada's Virtual Private Network (VPN) tunnels. The story suggested that the NSA's activities could be a preliminary step in broader efforts to "identify, study and, if deemed necessary, "exploit" organizations' internal communications networks."[6]
10. Access to strong, uncompromised encryption technology is critical to the economy. In a technological environment marked by high financial stakes, deep interdependence, and extraordinary complexity, ensuring digital security is of critical importance and extremely difficult. Encryption helps to ensure the security of financial transactions

[3] See: Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications, https://dspace.mit.edu/handle/1721.1/97690; Shining A Light On The Encryption Debate: A Canadian Field Guide, https://citizenlab.ca/2018/05/shining-light-on-encryption-debate-canadian-field-guide/.
[4] Civil Society Letter to Australian Government, February 21, 2019, https://newamericadotorg.s3.amazonaws.com/documents/Coalition_comments_Australia_Assistance_and_Access_Law_2018_Feb_21_2019.pdf;
Australia's Encryption Law Deals a Serious Blow to Privacy and Security, https://nationalinterest.org/feature/australia's-encryption-law-deals-serious-blow-privacy-and-security-39212.
[5] That Insane, $81M Bangladesh Bank Heist? Here's What We Know, https://www.wired.com/2016/05/insane-81m-bangladesh-bank-heist-heres-know/.
[6] NSA trying to map Rogers, RBC communications traffic, leak shows, https://www.theglobeandmail.com/news/national/nsa-trying-to-map-rogers-rbc-communications-traffic-leak-shows/article23491118/.

and preserves public trust in the digital marketplace. The cost of a security breach, theft, or loss of customer or corporate data can have devastating impacts for private sector interests and individuals' rights. Any weakening of the very systems that protect against these threats would represent irresponsible policymaking. Access to strong encryption encourages consumer confidence that the technology they use is safe.

11. Given the aforementioned threats, I **recommend** that the Government of Canada adopt a responsible encryption policy. Such a policy would entail a firm and perhaps legislative commitment to require that all sectors of the economy have access to strong encryption products, and would stand in opposition to irresponsible encryption policies, such as those calling for 'backdoors'.

# Vulnerabilities Equities Program

12. The Canadian government presently has a process in place, whereby the Communications Security Establishment (CSE) obtains computer vulnerabilities and ascertains whether to retain them or disclose them to private companies or software maintainers to remediate the vulnerabilities. The CSE is motivated to retain vulnerabilities to obtain access to foreign systems as part of its signals intelligence mandate and, also, to disclose certain vulnerabilities to better secure government systems. To date, the CSE has declined to make public the specific process by which it weighs the equities in retaining or disclosing these vulnerabilities.[7] It remains unclear if other government agencies have their own equities processes. The Canadian government's current policy stands in contrast to that of the United States of America, where the White House has published how all federal government agencies evaluate whether or retain or disclose the existence of a vulnerability.[8]
13. When agencies such as the CSE keep discovered vulnerabilities secret to later use them against specific targets, the unpatched vulnerabilities leave critical systems open to exploitation by other malicious actors who discover them. Vulnerability

[7] When do Canadian spies disclose the software flaws they find? There's a policy, but few details, https://www.cbc.ca/news/technology/canada-cse-spies-zero-day-software-vulnerabilities-1.4276007.
[8] Vulnerabilities Equities Policy and Process for the United States Government (November 15, 2017), https://www.whitehouse.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF.

stockpiles kept by our agencies can be uncovered and used by adversaries. The NSA's and Central Intelligence Agency's (CIA) vulnerabilities have been leaked in recent years,[9] with one of the NSA vulnerabilities used by malicious actors to cause at least $10B in commercial harm.[10]

14. As it stands, it is not clear what considerations guide Canada's intelligence agencies' decision-making process when they decide whether to keep a discovered vulnerability for future use or to disclose it so that it is fixed. There is also no indication that potentially impacted entities such as private companies or civil society organizations are involved in the decision-making process.
15. To reassure Canadian businesses, and make evident that Canadian intelligence and security agencies are not retaining vulnerabilities which could be used by non-government actors to endanger Canada's financial sector by way of exploiting such vulnerabilities, I would **recommend** that the Government of Canada publicize its existing vulnerabilities equities program(s) and hold consultations on its effectiveness in protecting Canadian software and hardware that is used in the course of financial activities, amongst other economic activities.
16. Furthermore, I would **recommend** that the Government of Canada include the business community and civil society stakeholders in the existing, or reformed, vulnerabilities equities program. Such stakeholders would be able to identify the risks of retaining certain vulnerabilities for the Canadian economy, such as prospectively facilitating ransomware, data deletion, data modification, identify theft for commercial or espionage purposes, or data access and exfiltration to the advantage of other nation-states' advantage.

# Vulnerability Disclosure Programs

17. Security researchers routinely discover vulnerabilities in systems and software that are used in all walks of life, including in the financial sector. Such vulnerabilities can,

[9] Who Are the Shadow Brokers?, https://www.theatlantic.com/technology/archive/2017/05/shadow-brokers/527778/; WikiLeaks Starts Releasing Source Code For Alleged CIA Spying Tools, https://motherboard.vice.com/en_us/article/qv3xxm/wikileaks-vault-7-vault-8-cia-source-code.
[10] The Untold Story of NotPetya, the Most Devastating Cyberattack in History, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

in some cases, be used to inappropriately obtain access to data, modify data, exfiltrate data, or otherwise tamper with computer systems in ways which are detrimental to the parties controlling the systems and associated computer information. Relatively few organizations, however, have explicit procedures that guide researchers in how to responsibly disclose such vulnerabilities to the affected companies. Disclosing vulnerabilities absent a disclosure program can lead companies to inappropriately threaten litigation to whitehat security researchers, and such potentials reduce the willingness of researchers to disclose vulnerabilities absent a vulnerability disclosure program.[11]

18. Responsible disclosure of vulnerabilities typically involves the following. First, companies make clear to whom vulnerabilities can be reported, assure researchers they will not be legally threatened for disclosing vulnerabilities, and explains the approximate period of time a company will take to remediate the vulnerability reported. Second, researchers commit to not publicly disclosing the vulnerability until either a certain period of time (e.g. 30-90 days) have elapsed since the reporting, or until the vulnerability is patched, whichever event occurs once. The delimitation of a time period before the vulnerability is publicly reported is designed to encourage companies to quickly remediate reported vulnerabilities, as opposed to waiting for excessive periods of time before doing so.
19. I would **recommend** that the Government of Canada undertake, first, to establish a draft policy that financial sector companies, along with other sector companies, could adopt and which would establish the terms under which computer security researchers could report vulnerabilities to financial sector companies. Such a disclosure policy should establish to whom vulnerabilities are reported, how reports are treated internally, how long it will take for a vulnerability to be remediated, and insulate the security researchers from legal liability so long as they do not publicly disclose the vulnerability ahead of the established delimited period of time.
20. I would also **recommend** that the Government of Canada ultimately move to mandate the adoption of vulnerability disclosure programs for its own departments given that they could be targeted by adversaries for the purposes of financially advantaging themselves to Canada's detriment. Such policies have been adopted by

[11] Vulnerability Disclosure Policies (VDP): Guidance for Financial Services, https://www.hackerone.com/sites/default/files/2018-07/VDP%20for%20Financial%20Services_Guide%20%281%29.pdf.

the United States of America's Department of Defense[12] and explored by the State Departments,[13] to the effect of having hundreds of vulnerabilities reported and subsequently remediated. Encouraging persons to report vulnerabilities to the Government of Canada will reduce the likelihood that the government's own infrastructures are successfully exploited to the detriment of Canada's national interests.

21. Finally, I would **recommend** that our laws around unauthorized access be studied with an eye towards determining if they are too broad in their chill and impact on legitimate security researcher.

# Two Factor Authentication Processes

22. Login and password pairs are routinely exfiltrated from private companies' databases. Given that many individuals either use the same pair across multiple services (e.g. for social media as well as for professional accounts) and, also, that many passwords are trivially guessed, it is imperative that private companies' online accounts incorporate two factor authentication (2FA). 2FA refers to a situation where an individual must be in possession of at least two 'factors' to obtain access to their accounts. The 'factors' most typically used for authentication include something that you know (e.g. a PIN or password), something you have (e.g. hardware token or random token generator), or something that you are (biometric, e.g. fingerprint or iris scan).[14]
23. While many financial sector companies use 2FA before employees can obtain access to their professional systems, the same is less commonly true of customer-facing login systems. It is important for these latter systems to also have strong 2FA to preclude unauthorized third-parties from obtaining access to personal financial accounts; such access can lead to better understandings of whether persons could be targeted by a foreign adversary for espionage recruitment, cause personal financial chaos (e.g. transferring monies to a third-party, cancelling automated bill payments,

[12] he Department of Defense wants more people to 'hack the Pentagon' — and is willing to pay them too, https://www.businessinsider.com/department-defense-wants-people-hack-pentagon-2018-10; DoD Vulnerability Disclosure Policy, https://hackerone.com/deptofdefense.
[13] House panel approves bill to 'hack' the State Department, https://thehill.com/policy/cybersecurity/386897-house-panel-approves-bill-to-hack-the-state-department.
[14] Office of the Privacy Commissioner of Canada Privacy Tech-Know Blog - Your Identity: Ways services can robustly authenticate you, https://www.priv.gc.ca/en/blog/20170105/.

etc) designed to distract a person while a separate cyber activity is undertaken (e.g. distract a systems administrator to deal with personal financial activities, while then attempting to penetrate sensitive systems or accounts the individual administrates), or direct money to parties on terrorist watchlists.

24. Some Canadian financial institutions do offer 2FA but typically default to a weak mode of second factor authentication. This is problematic because SMS is a weak communications medium, and can be easily subverted by a variety of means.[15] This is why entities such as the United States' National Institute of Standards and Technology no longer recommends SMS as a two factor authentication channel.[16]
25. To improve the security of customer-facing accounts, I **recommend** that financial institutions should be required to offer 2FA to all clients and, furthermore, that such authentication utilize hardware or software tokens (e.g. one time password or random token generators). Implementing this recommendation will reduce the likelihood that unauthorized parties will obtain access to accounts for the purposes of recruitment or disruption activities.

# Organizational Information

26. The views I have presented are my own and based out of research that I and my colleagues have carried out at my place of employment, the Citizen Lab. The Citizen Lab is an interdisciplinary laboratory based at the Munk School of Global Affairs and Public Policy, University of Toronto, focusing on research, development, and high-level strategic policy and legal engagement at the intersection of information and communication technologies, human rights, and global security.
27. We use a "mixed methods" approach to research combining practices from political science, law, computer science, and area studies. Our research includes: investigating digital espionage against civil society, documenting Internet filtering and other technologies and practices that impact freedom of expression online, analyzing

[15] Cybercriminals intercept codes used for banking to empty your accounts, https://www.kaspersky.com/blog/ss7-hacked/25529/; AT&T gets sued over two-factor security flaws and $23M cryptocurrency theft, https://www.fastcompany.com/90219499/att-gets-sued-over-two-factor-security-flaws-and-23m-cryptocurrency-theft.
[16] Standards body warned SMS 2FA is insecure and nobody listened, https://www.theregister.co.uk/2016/12/06/2fa_missed_warning/.

privacy, security, and information controls of popular applications, and examining transparency and accountability mechanisms relevant to the relationship between corporations and state agencies regarding personal data and other surveillance activities.