National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

# STRONG ENCRYPTION AND THE PRIVACY VS SECURITY DEBATE

**Lieutenant-Colonel Nakul Nayyar**

## JCSP 46

## Solo Flight

**Disclaimer**



## PCEMI 46

## Solo Flight

**Avertissement**



Canada

CANADIAN FORCES COLLEGE – COLLÈGE DES FORCES CANADIENNES

JCSP 46 – PCEMI 46
2019 - 2020

SOLO FLIGHT

# STRONG ENCRYPTION AND THE PRIVACY VS SECURITY DEBATE

By Lieutenant-Colonel Nakul Nayyar



Word Count: 4,642

Nombre de mots : 4.642

# STRONG ENCRYPTION AND THE DIGITAL PRIVACY VS SECURITY DEBATE

## INTRODUCTION

The subject of digital privacy has been hotly debated over the last three decades ever since governments recognized that their citizens could actually hide their personal communications from them. Digital communications have become more secure as a result of stronger encryption technology that began to emerge in the 1990s and made available to the masses for free by technology companies. The encryption available in the 1990s was much stronger than what the FBIs of the world were routinely used to breaking. The encryption was rendered even more uncompromisable by the virtue of its design that did not include any backdoor access, not even for the technology providers themselves. After decades of being able to 'snoop in' when authorized, the world had suddenly gone 'dark' for these government agencies. Ever since, government agencies such as the FBI and CSIS have repeatedly engaged the technology companies to build backdoors or deliberately weaken the encryption so it could be broken. In many cases, the technology companies have chosen not to cooperate and in fact pushed back and won. Though we live in an era when a majority of our communications have shifted to the digital realm, the laws of the lands haven't caught up to the realities of today especially concerning the privacy of an individual's digital communications weighed against the needs of the state to conduct surveillance or investigate crime.

Though anonymity and encryption are both part of the digital privacy debate, this paper is focused on the rights of the individuals to strong encryption and how confidence in strong encryption enables the exchange of ideas on the internet and powers e-commerce. This paper illustrates the history of manipulation by the governments in developing tools and backdoors to decipher encryption to enable investigative work until corporate technology companies like

Apple stood up and challenged such ongoing compromise of encryption algorithm in favor of individual privacy. This paper argues that digital privacy is a basic human right and any efforts to weaken encryption in the name of lawful access will only introduce vulnerabilities that can and will be exploited by criminal actors.

**Encryption enables fundamental rights and freedoms**

Strong uncompromisable encryption enables individuals to express their thoughts and opinions with an assurance of preserving their identity as well as the security of their communications. This is accomplished by utilizing a system of encryption keys that are only known to the sender and receiver. These keys are used to encrypt the message in transit and convert it into a cipher which can then only be unlocked by the key of the receiver. A digital signature on the sender's message applied by the sender's key is proof for the receiver that the message was in fact sent by that person and not tampered in transit. Encryption enables the integrity of the communications by preventing any tampering of the information while the message is in storage and transit. It also ensures that the message is only read by the intended recipient. Moreover, the receiver of the information is assured that the message was in fact sent by the sender.

In certain countries where freedom of expression is under threat by the ruling oppressive government, this can mean a difference between communication and censure. Secure online communications offer a way for marginalized ethnic groups or for those who are prosecuted for their sexual orientation or religious beliefs to browse the web, exchange emails and share ideas without fear of persecution. Journalists around the world utilize strong encryption to protect the identity of their informants and sources. Since secure uncompromisable encryption makes it much harder for state-run algorithms to automatically filter out certain messages on the internet,

it enables discourse and discussion on certain taboo subjects that an authoritarian government would otherwise censure. Permitting backdoors for states to access such secure encrypted communications can take away this online freedom of expression and stifle democracy.

Even in western liberal democracies, persons have a right to digital privacy even if they are not being persecuted or otherwise being targeted by the government. Both the 'Universal Declaration of Human Rights' proclaimed by the United Nations General Assembly in 1948 and the International Covenant on Civil and Political Rights (ICPR) adopted by General Assembly (1976) assert that 'no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence'[1]. Even though the 'Universal Declaration of Human Rights' is not legally binding on the member nations, it has provided a collective expression of fundamental values that all nations aspire to. The ICPR on the other hand, is a treaty among the member nations and hence all nations that ratified the treaty are compelled, though not bindingly obligated to take appropriate judicial and legislative measures to uphold the rights of the citizens as stipulated in the treaty.[2]

**Encryption enables Digital privacy**

In December 2013, the United Nations General Assembly adopted resolution 68/167 that reaffirmed that privacy was a human right and that all individuals had a right to protection of their privacy by the legal authorities. [3] It also recognized the importance of the right to privacy as an enabler of the right of freedom of expression. In 2015, a special report was commissioned by

[1]The United Nations. *International Covenant on Civil and Political Rights*. (U.N.: New York. 1976). https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx

[2] Ibid.

[3] The United Nations, *The Right to Privacy in the Digital Age 68/167, (*U.N.: New York, 2014). 1. https://undocs.org/A/RES/68/167

the United Nation's Office of the High Commissioner for Human Rights on the subject of rights and freedom of online expression. The report concluded that "encryption and anonymity enable individuals to exercise their rights to freedom of opinion and expression in the digital age and, as such, deserve strong protection."[4]

The principles embedded in the 'Universal Declaration of Human Rights' were a guiding light for many nations to formulate their own national charter of rights and freedoms. The Canadian Charter of Rights and Freedoms guarantees Canadians under section 8 that they have a right to be secure against unreasonable search or seizure[5]. Under section 273.2 of the National Defense Act (NDA), a government agency trying to utilize encryption breaking mechanisms to 'snoop' into an individual's online transactions without authorization can be found guilty of breaching section 8 of the Canadian Charter of Rights and Freedoms.[6] This section is especially pertinent to ensuring digital privacy protections in Canada as it is built into the laws and policies that govern the actions of Canada's Communications and Security Establishment (CSE).

Access to strong uncompromisable encryption allows Canadians and nationals of other countries to use the internet for not only financial transactions but also to find love on dating sites and purchase marijuana for that matter. Knowing that their transactions are private and secure in the cloud gives peace of mind to an individual that his or her information will not be

---

[4] The United Nations, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*. (United Nations: New York). https://www.un.org/unispal/document/report-of-the-special-rapporteur-on-the-promotion-and-protection-of-the-right-to-freedom-of-opinion-and-expression-a-hrc-41-35-add-2-excerpts/

[5] Department of Justice. *Constitution Act, 1982: Part 1: Canadian Charter of Rights and Freedoms.(*Ottawa: Department of Justice, 1982). https://laws-lois.justice.gc.ca/eng/Const/page-15.html

[6]National Defence Act, RSC 1985, c. N-5: Section 273.2, https://laws-lois.justice.gc.ca/eng/acts/N-5/index.html

'read' through a backdoor by government agencies or hacked into by criminal actors. That peace of mind powers the exchange of ideas and e-commerce on the internet.

**Encryption is a hindrance to government agencies**

Investigative agencies such as the NSA and the FBI have alleged that strong encryption enables criminals to conduct their business without fear of compromise. Even when the agencies obtain a warrant for lawful access, they are unable to crack the encryption to gain access because of a lack of decryption capabilities. This prevents these government agencies to disrupt any ongoing or future criminal activities. On such grounds, they continue to argue the case for technology providers to create decryption mechanisms and backdoors for lawful access.

In September 2018, the five eyes alliance comprising the United States, Canada, United Kingdom, Australia and New Zealand released a 'Statement of Principles on Access to Evidence and Encryption" that highlighted a concern of the 'five-eyes' nations regarding the use of ever stronger encryption by terrorist organizations and organized crime groups to hide their activities from detection and intrusion.[7] The statement reiterates the technological challenges that legal authorities continue to face in accessing (and decrypting) the data even when access has been legally granted due to lack of any 'backdoor' access provisioned by IT companies for legal authorities. It also argues that the lack of such access renders the court order virtually useless and undermines the foundations of the justice system. Through this communique, the five eyes alliance 'encourages' industry partners to cooperate with the governments in voluntarily establishing lawful access for authorized access by investigative agencies and also warn that if

[7] Five Country Ministerial, *Statement of Principles of Access to Evidence and Encryption, (*Australia: Canberra, 2018), Accessed 25 March 2020, https://www.homeaffairs.gov.au/about/national-security/five-country-ministerial-2018/access-evidence-encryption

such cooperation from industry partners is not forthcoming, the authorities "may pursue technological, enforcement, legislative or other measures to achieve lawful access solutions."[8]

This recent five eyes attempt at weakening strong encryption for users is not new. A great example of influence exerted by the US and its western allies in exerting control over encryption standards can be found in the Global System for Mobile Communications (GSM) standard developed for cellular phone communications developed in the 1980s and first deployed in 1991. Though initially designed as a 128-bit encryption system, it was reduced to 64 bits after pressure by the US, France and British governments.[9] The reasoning was that these governments wanted to be able to break the encryption as needed and did not want a stronger standard. Moreover, the last 10 digits of the encryption standard was arbitrarily set to zero so it effectively became a 54-bit system.

Though the Five-Eyes community through their recent communique raised their concern regarding the use of strong encryption by criminal elements, what they haven't offered is a technically feasible solution for such exceptional access. Technology companies like Apple have repeatedly pleaded that creating backdoors for lawful access will weaken the encryption for everyone and introduce vulnerabilities that can be exploited by hacktivists, foreign national powers, organized crime syndicates and other criminal elements alike. It is one thing for governments to legalize exceptional access or 'encourage' industry partners to voluntarily establish lawful access to investigative agencies, but it's an entirely different matter to develop a technical solution to implement the intent of such a law or recommendation.

---

[8] Ibid.

[9] Arild Faeraas, "Sources: We Were Pressured to Weaken the Mobile Security in the 80's", Aften Posten (9 January 2014), Accessed 21 April 2020, https://www.aftenposten.no/verden/i/95 Olkl/Sources-We-were-pressured-to-weaken-the-mobile-security-in-the-80s.

**Past efforts at building backdoor access to Encryption and failures**

The 1990s saw the early emergence of encryption in securing internet based communications. In response to the US government's aim to bypass encryption and snoop into communications of suspected criminals or foreign actors, the National Security Agency (NSA) developed a chipset called 'Clipper" that when deployed on communication networks would relay the cryptographic keys to the NSA.[10] In this manner, the NSA or other government agency could then decrypt the communication upon authorization. However, despite pressure by the US government, most telecommunications providers resisted the adoption of the 'Clipper' chipset on the grounds that it impinged on their customers' privacy. The only company to adopt the chipset was AT & T which was eventually publicly heavily criticized when their cooperation was made public.

The Clipper chipset finally met its demise in 1994 when Matt Blaze, a cryptography expert working at A T & T Bell published a paper that revealed significant flaws in the chip's design. The paper discussed several ways in which the transmission of the 'public key' to the government authorities could be compromised thereby compromising the ability of the NSA to 'snoop' into private communications. Matt Blaze's paper was a death sentence for the Clipper chip and it was soon abolished by the NSA. It also supported the technology providers' claim that introducing backdoors will open a pandora's box of complexities in the system that will weaken the security of the communications for everyone.[11]

[10] Electronic Privacy Information Center "The Clipper Chip". Accessed 27 March 2020. https://epic.org/crypto/clipper/

[11]Matt Blaze, "Protocol Failure in the Escrowed Encryption Standard". *Proceedings of the 2nd ACM conference on computer and communications security*. (Nov 1994): 66. https://dl.acm.org/doi/10.1145/191177.191193

The Clipper debacle combined with increasing calls for protection or privacy rights heralded a shift in sentiment in the US government towards strong encryption with the acknowledgement that string uncompromisable encryption did play a key role in maintaining the security of commercially available networks.[12] It also caused a relaxation of US policy on export restrictions related to encryption technology. Until that time, the US government had enacted export control measures. For example, any technology employing greater than 56-bit encryption required special export permissions. The aim was to control the transfer of encryption technology outside the country such as not to impact the NSA's ability to snoop in on foreign communications.

**State Surveillance driving technology companies to make stronger encryption**

The Patriot Act passed on 26 Oct 2001 authorized the NSA and FBI to conduct mass surveillance of Americans and foreign nationals that was unprecedented. The US Patriot Act that came into effect six weeks after 9/11 provided sweeping powers to government agencies to spy on phone conversations, email exchanges and text messages with greatly reduced checks and balances on their power. The FBI, NSA and CIA were no longer required to obtain a warrant to collect data on individuals in certain cases. The lack of judicial oversight resulted in several cases where individuals were targeted without due process or justification as was revealed by the whistleblower, Edward Snowden.

The extent of the mass surveillance was revealed by Edward Snowden in 2013 to the Guardian and Washington Post newspapers. Snowden sent the newspapers classified documents

[12] Lex Gill, Tamir Israel, and Christopher Parsons, "Shining a Light on the Encryption Debate: A Canadian Field Guide," Munk School of Global Affairs and Public Policy, May 2018:25, Accessed 21 April 2020, https://citizenlab.ca/2018/05/shining-light-on-encryption-debate-canadian-field-guide/

revealing the existence of NSA's PRISM computer system that was actively collecting data from the servers of various major internet companies like Microsoft, Yahoo, Google, Facebook, AOL, Skype and Apple. The information collected included chat messages, geolocation, contacts, photos, e-mails, file transfers and social networks. What the Snowden revelations highlighted were that the NSA was not just simply targeting the information of specific persons of interest but instead conducting mass surveillance of Americans and foreign nationals at home and abroad in a gross act of injustice and abuse of privacy.[13]

The Snowden revelations on mass surveillance motivated the technology companies and cryptographic experts to develop stronger encryption standards. The availability of stronger encryption for individuals has made it harder for the western and allied governments' capability to decrypt encrypted transmissions, in what has led to the 'Going Dark' scenario. The term 'Going Dark' refers to this reality in which investigative government agencies such as the FBI are no longer able to 'snoop' into people's communications even when they have been granted such access by a court.

Edward Snowden's public disclosures in 2014 have now shown that the five eyes countries are actively performing electrical and digital surveillance of its citizens and foreign actors. This has led to a more determined effort by commercial encryption providers to strengthen their encryption products.

**Apple vs FBI**

[13] The Guardian, "NSA Files Decoded",. Accessed 28 March 2020. https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/5

Advancements in encryption algorithms and technology have rendered encrypted data opaque to even the smart phone manufacturer or cloud services provider themselves. The encryption algorithm in Apple smartphones for example is designed so that only the user is able to unlock the data. The FBI and Apple encryption dispute of 2015 started when FBI asked Apple to create a software that would enable FBI to unlock the Apple IPhone belonging to one of the terrorists of the December 2015 San Bernandino attack. The terrorist was dead but the FBI wanted access to the IPhone in order to investigate the attack and potentially uncovering clues to other terrorist operations. Apple refused on the grounds that the law did not require them to develop decryption algorithms for their encryption. The law that Apple referred to in their defense was the Communications Assistance for Law Enforcement Act (CALEA) of 1994. Though CALEA requires traditional telecommunications carriers to develop voice and data interception gateways for use by legal authorities such as FBI, it does not prohibit any telecommunications provider to deploy encryption that it cannot decrypt itself.[14]

Despite efforts by the FBI to expand and update CALEA to expand its scope, such efforts have yet remained unsuccessful. As a result, CALEA does not apply to the myriad of IT, hardware software and cloud services companies providing encryption at rest, encryption in transit and end to end encryption services to individuals and companies alike that utilize certain encryption algorithms that only decrypt the data once the user's password is entered. Without the user's password, their communications are opaque to the smart phone manufacturer or the cloud services provider due themselves. As a result, these companies are not similarly bound to develop such interception gateways.

---

[14] United States Congress, *Communications Assistance for Law Enforcement Act,* https://www.congress.gov/bill/103rd-congress/house-bill/4922

In Canada, the law does not require internet service providers to provide decryption mechanisms to the government[15]. Moreover, there is no much stipulation or law in the Canadian criminal code, CSIS Act or otherwise that a person or an organization must reveal the passwords to their encrypted communication.[16] This is not just a matter of preservation of the privacy of an individual but also one of the constitutional rights of an individual.[17] Section 11c of the Canadian Charter of Rights and Freedoms confirms the right of an individual against self-incrimination[18]. If revealing the password to your smartphone would divulge incriminating evidence for an offence that the person had committed, then the charter can uphold the right of that individual to refuse to reveal the password to the investigative agencies.

**The request for backdoors from governments ignores technical realities**

In a letter published on 16 Feb 2016, Apple in defense of its refusal to compromise the security of the Apple iOS as requested by the FBI in the San Bernandino mass shooting. [19] Apple contends that doing so would undo the years of advances that companies like Apple have made in protecting their customers' security and "undermine the very freedoms and liberty our government is meant to protect."[20] Apple also warned that if FBI succeeded in changing the laws to force Apple to comply with its request, it could in the future lead to enhanced government

---

[15] Public Safety Canada, Our Security, Our Rights, National Security Green paper *2016*. (Canada: Public Safety, 2016), 19. Accessed 26 April 2020:59. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-scrt-grn-ppr-2016-bckgrndr/ntnl-scrt-grn-ppr-2016-bckgrndr-en.pdf

[16] Ibid., 61.

[17] Lex Gill, Tamir Israel, and Christopher Parsons, "Shining a Light on the Encryption Debate: A Canadian Field Guide," Munk School of Global Affairs and Public Policy, May 2018:66, Accessed 21 April 2020, https://citizenlab.ca/2018/05/shining-light-on-encryption-debate-canadian-field-guide/

[18] Department of Justice. *Constitution Act, 1982: Part 1: Canadian Charter of Rights and Freedoms.(*Ottawa: Department of Justice, 1982). https://laws-lois.justice.gc.ca/eng/Const/page-15.html

[19] Apple. "A Message to our Customers", 16 Feb 2016. Accessed 26 April 2020. https://www.apple.com/customer-letter/

[20] Ibid.

surveillance of an individual's locations, bank accounts, medical records and private communications. The FBI eventually withdrew its case against Apple after it managed to find a third party to 'hack' the phone in question.

A 2015 report by a group of leading cryptographic experts summarized that such an 'exceptional access' would seriously undermine the security of the internet as a whole and introduce complex unexpected vulnerabilities that would make the internet vulnerable to exploitation by malicious actors. [21] The report summarizes that building such access would do much greater harm than good and not only jeopardize the security and privacy of individuals but also threaten the government networks. In other words, there is no way to provide exceptional access without compromising security for all.

Uncompromisable encryption enables trust in financial institutions and powers e-commerce. It provides confidence and comfort to companies and their stakeholders that their financial transactions are protected from sabotage and theft. Our supply chains are managed on computer networks that connect companies globally. The flow of information and processing of orders is protected by encryption that prevents criminal actors or competitors from disrupting these supply chains. Our hospitals and medical offices use encryption to protect our medical records so they remain confidential. Our nuclear power stations rely on encrypted networks that protect their operations from hacking and criminal intent. If we weaken encryption, e-commerce, supply chains, nuclear power stations; they all stand to become compromised.

[21] Harold Abelson, Ross Anderson, "Keys under doormats", *Communications of the ACM*, vol 58 iss 10, (September 2015).Accessed 30 March 2020 https://www.schneier.com/academic/paperfiles/paper-keys-under-doormats-CSAIL.pdf

**The government investigative agencies have plenty of other means at their disposal**

According to the FBI, lawful access to personal data continues to get harder for legal authorities with the advent of newer and stronger encryption algorithms available to individuals and organizations.[22]The term, 'Going Dark' refers to this reality in which investigative government agencies such as the FBI are no longer able to 'snoop' into people's communications even when they have been granted such access by a court.

In Canada, Public Safety has also highlighted the 'Going Dark' phenomenon in its 2017 annual report.[23]To combat 'Going Dark', both the FBI and CSIS have strongly suggested that the technology companies engineer backdoors for access by government or use lower encryption standards that can be decrypted. But what these government agencies have not acknowledged is that they are not completely in the 'Dark'. The metadata related to geolocation, text messages, phone conversations, e-mail messages and Voice over IP (VOIP) based communications is often not encrypted. Metadata is the information or dataset about the information that is being communicated. It is not encrypted because of the variety of non-standard networking equipment in use today and the need for speed of communication. Adding encryption to metadata would slow down transmission as the networking equipment would first have to decrypt the metadata related to the destination address before relaying the message. In the case of an e-mail message, metadata includes the subject line and the size of any attachments as well as the time that the message was sent. In case of a mobile phone conversation, the SIM card identifier and receiver is

[22] Federal Bureau of Investigation. *Going Dark* (Washington, D.C.: U.S, n.d.). Accessed 25 March 2020. https://www.fbi.gov/services/operational-technology/going-dark

[23] Public Safety Canada, *2017 Public Report on the Terrorist Threat to Canada: Building A Safe and Resilient Canada*. (Canada: Public Safety, 21 December 2017), 19. Accessed 26 April 2020. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/pblc-rprt-trrrst-thrt-cnd-2017/index-en.aspx

also contained within the metadata. Metadata is not encrypted and accessible to government agencies to collect and analyze.

The aggregate of such metadata can also reveal a significant amount of data about the individuals. An individual's social media accounts, VOIP messaging accounts like WhatsApp, Gmail messages all reveal metadata about them that is unencrypted and easily collected by the likes of FBI. Snowden's revelations have revealed that the NSA's PRISM program collects metadata from several technology companies. The metadata can reveal who the individual's circle of contacts, the frequency of the contact, the users' opinions and interests depending on what forums they participate in or follow. Though the content of the message itself is encrypted, the metadata is not and it can provide a wealth of information.

Moreover, government agencies have a plethora of other tools in war chest to investigate and prosecute crime. For example, traditional wire-tapping (authorized under CALEA in the US), forensics, physical surveillance, data-mining and many others. So, the notion that strong encryption renders these investigative agencies 'Dark' is exaggerated.

**Bill C-59**

The Communications Security Establishment (CSE) is Canada's national signals intelligence and cybersecurity agency. CSE's mandate coms from the National Defense Act (NDA) and it includes the collection of foreign intelligence and protection of Canada's communications infrastructure[24]. It operates in the cyber domain consisting of electromagnetic emissions (mobile communications), internet transmissions (e-mails, instant messages) and satellite communications. Under the NDA, CSE is strictly prohibited from collecting, analyzing

[24] National Defence Act, RSC 1985, c. N-5. https://laws-lois.justice.gc.ca/eng/acts/N-5/index.html

or storing any information on Canadians in strict adherence of Section 8 of the Canadian Charter of Rights and Freedoms and the Privacy Act.

On 21 June 2019, Bill C-59, the National Security Act 2017 received royal assent.[25] The new Act (CSE Act) provides CSE with two new mandates, Defensive Cyber Operations (DCO) and Active Cyber Operations (ACO). Under its new mandate, CSE can trawl the web collecting data on foreign entities using bulk collection techniques. By expanding CSE's powers into the cyber realm, it increases the potential for CSE to engage in 'inadvertent' collection of data on Canadians because of how interconnected the internet is. A Canadians' data could easily be inter-mingled with the data of persons of other nationalities which might be residing on a Google cloud server in Brazil. Section 34(2)(c) of Bill C-59 states that "information acquired under the authorization that is identified as relating to a Canadian or a person in Canada will be used, analysed or retained only if the information is essential to international affairs, defence or security".[26] In contrast to the NDA that completely prohibited CSE from acquiring or storing data on Canadians, Bill C-59 permits the CSE to do so in certain cases that are only implicitly defined in the Bill leaving it open for interpretation by CSE. In this way, it weakens the privacy rights of Canadians in favor of state's investigative powers.[27]

**Canadians' expectation of digital privacy**

[25] Parliament of Canada, Bill C-59. https://www.parl.ca/DocumentViewer/en/42-1/bill/C-59/royal-assent
[26] Ibid.
[27] Canadian Journalists for Free Expression, "Impacts of Bill C-59 and the New CSE Act on Journalism and Free Expression", February 2018. https://www.ourcommons.ca/Content/HOC/Committee/421/SECU/Brief/BR9688057/br-external/CanadianJournalistsForFreeExpression-e.pdf

A national security green paper, titled 'Our Security Our Rights' was published by the Canadian government in 2016.[28] It highlighted the issue that law enforcement agencies in the country faced when it came to gaining lawful access to encrypted data and how smart phones with their strong encryption were being used by terrorists to conduct terrorist activities. The paper provided the setting for an online questionnaire that was circulated to Canadians that included several questions on the subject of security, privacy and lawful access to data by the government. The questions also asked Canadians whether the technology companies had an obligation to decrypt communications for the government and to make recommendations on how the government could balance privacy and security. The 59,000 responses received clearly established that Canadians were opposed to enabling backdoors or for compelling technology companies from having to decrypt their customers' data.[29]

The survey results also revealed that Canadians felt that the Canadian investigative agencies such as the CSIS and RCMP have sufficient tools at their disposal to investigate and prosecute crime and authorizing further tools such as 'exceptional access' that would only end in compromise of Canadians' privacy. Canadians have an expectation of digital privacy and preferred protection of individual rights to privacy over increased investigative powers to the agencies. New measures or powers must only be enacted with increased provisions of checks and balances. Bill C-59 significantly expands CSE's investigative powers into the cyber space domain from mainly focusing only on the signals intelligence domain. The Canadian government must ensure that Bill C-59 does not compromise the expectation of privacy that Canadians have

---

[28] Department of Public Safety and Emergency Preparedness, *National Security Green paper. (*Ottawa: Public Safety, 2016),5. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-scrt-grn-ppr-2016/ntnl-scrt-grn-ppr-2016-en.pdf

[29] Department of Public Safety and Emergency Preparedness, *National Security Consultations: What We Learned Report*. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2017-nsc-wwlr/index-en.aspx

over their digital communications and that CSE's activities are in line with section 8 of the Canadian Charter of Rights and Freedoms that prohibits unlawful search or seizure of individuals.

The rights of an individual when it comes to remaining anonymous are unclear in both US and Canada. Anonymity defined as a state that allows individuals to disengage their activities from their identities. [30] Several online forums and discussion boards allow users to anonymously post material as well as browse topics which are considered taboo. Anonymity provides a means for such individuals to freely communicate without fear of ostracism or judgement by others. It remains unclear in Canada whether Anonymity is protected under section 2b of the Freedom of Expression Act (Canada). This is in part because there have been a limited number of cases that have come up that have forced the supreme court to the interpret section 2b when concerning digital anonymity.[31]In many cases, both US and Canadian courts have compelled Internet Service Providers (ISPs) to reveal the names of individuals suspected of cyber-bullying or child pornography. Though anonymity and encryption are both part of the digital privacy debate, this paper is focused on the rights of the individuals to strong encryption.

**Conclusion**

[30] Citizen Lab and the Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic. "Online Anonymity and John/Jane Doe Lawsuits", Accessed 02 April 2020. https://cippic.ca/en/FAQ/online-anonymity-and-doe-lawsuits

[31]Peter Carmichael Keen, "Anonymity and the Supreme Court's Model of Expression: How Should Anonymity be Analysed Under Section 2(b) of the Charter?", *Canadian Journal of Law and Technology* vol 2 number 3 (2013):167. https://digitalcommons.schulichlaw.dal.ca/cjlt/vol2/iss3/2/

Strong uncompromisable encryption enables fundamental rights and freedoms and powers the exchange of ideas. It allows individuals to express their thoughts and opinions without fear of persecution or censure. Journalists around the world utilize strong encryption to protect the identity of their informants and sources. Hospitals and clinics employ strong encryption to secure and protect confidential health records of their patients. It does so because stronger uncompromisable encryption provides confidence and comfort to these individuals and organizations that their confidential communications are protected from sabotage and theft.

Investigative agencies such as the FBI and CSIS continue to reiterate that strong encryption prevents their investigations because of their inability to decrypt it even when they have legal authority to do so. As a result, they have asked technology companies to build backdoors into their encryption algorithms for reasons of 'exceptional access'. Their assertion ignores security and technical realities. It is one thing for governments to legalize exceptional access or 'encourage' industry partners to voluntarily establish lawful access to investigative agencies, but it's an entirely different matter to develop a technical solution to implement the intent of such a law or recommendation. There is resounding agreement among cryptology experts worldwide that creating backdoors for lawful access will weaken the encryption for everyone and introduce vulnerabilities that can be exploited by hacktivists, foreign national powers, organized crime syndicates and other criminal elements alike. Encryption powers classified communications, banking transactions, power utility control centers and supply chains. If we weaken encryption, e-commerce, supply chains, nuclear power stations; they all stand to become compromised. The 'Going Dark' phenomena are exaggerated as the government agencies have a plethora of other tools in war chest to investigate and prosecute crime without compromising encryption for everyone.

**BIBLIOGRAPHY**


Abelson H., Anderson, R. "Keys under doormats". *Communications of the ACM*, vole 58 iss 10, (September 2015).Accessed 30 March 2020 https://www.schneier.com/academic/paperfiles/paper-keys-under-doormats-CSAIL.pdf

Apple. "A Message to our Customers", 16 Feb 2016. Accessed 26 April 2020. https://www.apple.com/customer-letter/

Australia. Five Country Ministerial. *Statement of Principles of Access to Evidence and Encryption.* Australia: Canberra, 2018. Accessed 25 March 2020 https://www.homeaffairs.gov.au/about/national-security/five-country-ministerial-2018/access-evidence-encryption

Blaze,M. "Protocol Failure in the Escrowed Encryption Standard". Proceedings of the 2nd ACM conference on computer and communications security. (Nov 1994): 59–67. https://dl.acm.org/doi/10.1145/191177.191193

Canada. Department of Justice. Constitution Act, 1982: Part 1: *Canadian Charter of Rights and Freedoms. Ottawa:* Department of Justice, 1982. https://laws-lois.justice.gc.ca/eng/Const/page-15.html

Canada. Department of Public Safety and Emergency Preparedness. *National Security Green paper.* Ottawa: Public Safety, 2016. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-scrt-grn-ppr-2016/ntnl-scrt-grn-ppr-2016-en.pdf

Canada. Department of Public Safety and Emergency Preparedness. *2017 Public Report on the Terrorist Threat to Canada: Building A Safe and Resilient Canada*. Canada: Public Safety, 21 December 2017. Accessed 26 April 2020. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/pblc-rprt-trrrst-thrt-cnd-2017/index-en.aspx

Canada. Department of Public Safety and Emergency Preparedness. *National Security Consultations: What We Learned Report*. Ottawa: Public Safety, 2017. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2017-nsc-wwlr/index-en.aspx

Canada. Department of Public Safety and Emergency Preparedness. *Our Security Our Rights*. Ottawa: Public Safety, 2016. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-scrt-grn-ppr-2016-bckgrndr/ntnl-scrt-grn-ppr-2016-bckgrndr-en.pdf

Canadian Journalists for Free Expression. "Impacts of Bill C-59 and the New CSE Act on Journalism and Free Expression", February 2018. Accessed 30 April 2020. https://www.ourcommons.ca/Content/HOC/Committee/421/SECU/Brief/BR9688057/br-external/CanadianJournalistsForFreeExpression-e.pdf

Citizen Lab and the Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic. "Online Anonymity and John/Jane Doe Lawsuits." Accessed 02 April 2020. https://cippic.ca/en/FAQ/online-anonymity-and-doe-lawsuits

Electronic Privacy Information Center. “The Clipper Chip”. Accessed 27 March 2020. https://epic.org/crypto/clipper/

Faeraas, Arild. “We Were Pressured to Weaken the Mobile Security in the 80’s”. *Aftenposten,* 9 January 2014. Accessed 26 April 2020. https://www.aftenposten.no/verden/i/95Olkl/Sources-We-were-pressured-to-weaken-the-mobile-security-in-the-80s>

Gill, L., Israel, T., Parsons, P. “Shining a Light on the Encryption Debate: A Canadian Field Guide”. *Munk School of Global Affairs and Public Policy*. Accessed 21 April 2020. https://citizenlab.ca/2018/05/shining-light-on-encryption-debate-canadian-field-guide/

Green, M. “Apple, CALEA and Law Enforcement”. *Lawfare,* 19 Dec 2017. https://www.lawfareblog.com/apple-calea-and-law-enforcement

Keen, P., "Anonymity and the Supreme Court's Model of Expression: How Should Anonymity be Analysed Under Section 2(b) of the Charter?". *Canadian Journal of Law and Technology* vol 2 number 3 (2013):167-186. https://digitalcommons.schulichlaw.dal.ca/cjlt/vol2/iss3/2/

Landau, S. “Statement of Principles of Access to Evidence and Encryption: Things are seldom what they seem.”. *Lawfare*. Accessed 25 March 2020. https://www.lawfareblog.com/five-eyes-statement-encryption-things-are-seldom-what-they-seem

Swire, Peter and Ahmad, Kenesa. “Encryption and Globalization”. *Columbia Science and Technology Law Review* Vol. 23, (2012):439-441. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1960602

The United Nations. *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*. United Nations: New York. Accessed 31 March 2020. https://www.un.org/unispal/document/report-of-the-special-rapporteur-on-the-promotion-and-protection-of-the-right-to-freedom-of-opinion-and-expression-a-hrc-41-35-add-2-excerpts/

The United Nations. *The Right to Privacy in the Digital Age 68/167*. U.N: New York. Accessed 31 March 2020. https://undocs.org/A/RES/68/167

The United Nations. *International Covenant on Civil and Political Rights*. U.N.: New York. 1976. https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx

The United States of America. Federal Bureau of Investigation. *Going Dark*. Washington, D.C., n.d. Accessed 25 March 2020. https://www.fbi.gov/services/operational-technology/going-dark

The United States of America. Central Investigative Agency. *The Evolution of US Government Restrictions on Using and Exporting Encryption Technologies*. Washington, D.C. 2014. https://www.cia.gov/library/readingroom/docs/DOC_0006231614.pdf