POLICY BRIEF

Why Canada Must Defend Encryption

M.J. Masoodi | Alexander Rand

cybersecure
policy
exchange
Powered by RBC®

t.txt written!
E DECRYPTED TEXT IS
ENDEDTOIMPRESSEMPLOYERSENDUPTIC
PERSGALOREASTUDYHASFOUNDTHESTUD
NTOFTHERANDOMLYSELECTEDRESUMESA
GTHEFUNNYBONEANDSOUNDINGOUTRAGEO
ATICALSPELLINGANDTYPOGRAPHICAL
SOLUTIONSREVEALEDTHATMORETHANP

Mohammed (Joe) Masoodi

Joe has been conducting research and policy analysis at the intersections of surveillance, digital technologies, security and human rights for over six years. He has conducted research at the Surveillance Studies Centre at Queen's University and the Canadian Forces College. He holds an MA in war studies from the Royal Military College of Canada; an MA in sociology from Queen's University; and has studied sociology as a PhD candidate from Queen's University, specializing in digital media, information and surveillance.

Alexander Rand

Alex is interested in disinformation and the ways in which new technologies influence online political discourse. He has worked as a Policy and Research Assistant for the Cybersecure Policy Exchange, a Public Policy Researcher at the Centre for the Future of Democracy, and at the London-based AI think tank Future Advocacy. He holds a Master of Public Policy from Cambridge University, where he conducted statistical analyses of online partisanship and disinformation in the Canadian context, as well as a BA from McGill University in Economics and Music Technology.

How to Cite this Report

Masoodi, M.J. & Rand, A. (2021, September). *Why Canada Must Defend Encryption*. Retrieved from https://www.cybersecurepolicy.ca/policy-brief-encryption

350 Victoria St, Toronto, ON M5B 2K3

Cybersecure Policy Exchange: https://www.cybersecurepolicy.ca/

@cyberpolicyx @cyberpolicyx Cybersecure Policy Exchange

Executive Summary

Apple has recently announced plans to scan customers' mobile devices for pictures uploaded to its iCloud servers as well as texts shared through its messaging app for child sexual exploitation materials, raising significant questions and concerns regarding surveillance and reigniting the debate on encryption. Western law enforcement and intelligence agencies have long warned about their seeming inability to gain access to the content of individuals' private electronic communications due to the widespread use and implementation of encryption technologies in consumer electronics, posing risks to public safety and national security. In particular, these arguments are often linked to threats, including terrorism, domestic violent extremism and, more recently, child sexual exploitation. Police and intelligence agencies believe it will become increasingly difficult to curtail such crimes when unbreakable encryption continues to be widely implemented in everyday electronics. As a result, such agencies are increasingly making calls to tech companies to devise new ways that allow them access to private communications by weakening their encryption systems; and Australia and the UK have gone as far as passing legislation to compel company cooperation in this regard.

On the one hand, such calls by police and intelligence agencies in the West are growing; while, on the other hand, a wide range of public, private and civil society stakeholders — including researchers, experts and even senior government officials within the policing-intelligence apparatus — have staunchly opposed such proposals. Rather, they argue that additional legal powers aimed at circumventing encryption will produce wide-ranging consequences by leaving networks and the people that rely on them more vulnerable to cyberattacks while producing lasting harms including to human rights and civil liberties globally.

While Canada has occasionally voiced mild support for strong forms of encryption, there's an indication that this public position is changing.[1] In its most recent move, the federal government issued a joint statement in October 2020 with its with Five Eyes intelligence counterparts criticizing encryption systems and calling on technology companies to find 'technically feasible solutions' that 'enable law enforcement to [access] content in a readable and usable format'.[2] The joint statement identifies end-to-end encryption — popularly used by messaging apps like WhatsApp and Apple's iMessage — as posing particular challenges to public safety and national security.

In our analysis, **legislative efforts to weaken encryption cannot be sufficiently targeted to achieve the desired policy outcomes without creating disproportionate and wide-ranging risks for Canadian society at large,** including for human rights, civil liberties and national security. This conclusion is in line with the broad technical consensus that proposed government measures in this area are fundamentally unworkable in practice.[3]

This policy brief builds on the excellent research on encryption produced by experts in Canada[4] and extends this knowledge by presenting an alternative policy framework to help guide Canada's policy on encryption. It is developed based on the analysis of the current encryption-policing-security landscape, revealing that, law enforcement and intelligence agencies have the legal and technical capabilities to achieve their objectives without additional powers aimed at breaking encryption; and that tech companies, specifically social media, can be required to apply additional efforts to curtail illegal activities:

1. There is a plethora of **non-encrypted data available** to police and security agencies to lawfully gather and analyze for investigative and intelligence gathering purposes, including for example metadata and open source data (e.g., social media and other online data). Such approaches need to be guided by best practices, given their criticisms and broader worry surrounding their use.[5]

2. At a higher level, the government can require social media companies to **apply greater efforts in identifying and removing illegal materials** on open platforms, disrupting the cross-flow of illegal activities between open platforms and encrypted platforms.

3. Regulatory measures can require social media companies to introduce **changes to software design**, preventing or slowing the spread of illegal activity by creating friction, such as rules and restrictions on encrypted private messages between children and adults.

4. Social media companies can be required to **provide regular and transparent reports** providing data detailing their response in curtailing illegal activities, including metrics on takedowns to help identify specific issues and formulate tailored responses to specific illegal activities.

Such measures are less invasive and more secure than what Western governments, including Canada, are requesting, such as legally mandating that tech companies introduce methods intended for allowing state actors access to encrypted data — often referred to by the metaphor 'backdoor'. There is a high degree of certainty that such methods will not only be exploited by lawful authorities, but by other malicious actors posing risks and implications for all users and wider society — fears shared by many over Apple's recent decision.[6]

This policy brief joins others, including cryptographers, academics, researchers, and privacy experts, in calling on the Government of Canada to **preserve strong encryption** by preventing legislation that systemically weakens it by requiring tech companies to intentionally introduce known vulnerabilities for government surveillance purposes.

It analyzes Canadian and other Western policy responses raised by the perceived challenges of encryption; and is aimed at providing insight for Canadian policymakers on the options available as they review and update their policies on encryption. It also provides results of a national survey on Canadians' views on encryption, conducted in May 2020, revealing a relative lack of public awareness on encryption. Thus, this brief also serves to raise awareness on the broad-ranging social, political and economic benefits of strong and robust encryption among ordinary Canadians. It will be equally beneficial for academics, researchers, advocates and legal professionals, to gain a better understanding on how their online communications, specifically on social media, may be impacted by policy changes.

Introduction

Consumer electronic devices that enable easy access to the internet have become ubiquitous in everyday life. Nearly all Canadians rely on these technologies to facilitate our social, political and economic interactions, many of which contain sensitive personal information. As such, ensuring the privacy of communications carried out on these devices is critical for protecting the privacy rights of Canadians. Trust in the security of one's communications is also a prerequisite for individuals to feel they can safely exercise their basic rights and freedoms of expression, thought, opinion, belief and association. This protection is particularly important for marginalized and vulnerable groups, who are disproportionately targeted and surveilled through technology by industry and state security actors.[7]

In addition to undermining basic rights and trust in democracy, a failure to ensure the privacy of personal data can have immediate consequences for national security — paving the way for malicious actors, including cybercriminals, terrorists, and hackers, to engage in nefarious activities. Foreign intelligence agencies may have an interest in obtaining Canadians' personal data because it can allow them to manipulate public opinion and undermine public confidence in government.[8] Foreign powers can also use Canadians' personal data to identify individuals and their weaknesses, potentially turning them into agents of a foreign power.[9] According to a recent report by the Canadian Centre for Cyber Security, criminal and state-sponsored efforts to seek out data for the purpose of identifying, profiling and tracking individuals are expected to increase.[10]

Encryption is important because it is the primary technical bulwark against these threats to individual rights, democracy and national security. Indeed, these seemingly disparate interests have converged as our communications have moved to digital platforms.[11] As such, the security of communications infrastructure and the contents of personal communications must be an urgent priority for government.[12] The important role for encryption in protecting against these threats has been acknowledged in the past by the Canadian government.[13]

Understanding Encryption: Defining Key Terms and Concepts

Encryption is the process of encoding information so that it can only be understood by its intended recipient.[14] Basic forms of encryption, for instance, simply involve the switching of letters according to a pattern: every time you see the letter 'A', replace it with 'Z'. The many methods used in this process are collectively known as **cryptography** — a process as old as writing itself.[15, 16] Modern cryptography has become vastly more sophisticated through encryption methods that rely on computer algorithms.[17] As a result, patterns used in this process have become highly complex, making it increasingly difficult for non-authorized parties to decipher the content of messages.

Algorithms take information written in a form readable to humans (**plaintext**) and convert it into an unreadable form (**ciphertext**).[18] This is done using a random[19] string of information consisting of 0s and 1s, or 'bits', collectively referred to as a **key**. The key is used by the intended recipient to convert the information back into its original readable form in a process called **decryption**.[20] Keeping the key secure is critical in keeping encrypted information away from prying eyes.

There are two types of encryption in widespread use today, known as **symmetric** and **asymmetric encryption**.[21] In the former, the same key is used to encrypt and decrypt data. Here, it is critical that a secure method is established to transfer the key between sender and recipient. Of course, one can see how this may raise issues in securely distributing the key between parties. To address this problem, **asymmetric encryption**, often referred to as *public key cryptography,* was developed in the 1970s.[22] In such a system, an algorithm generates two keys: a *public key* to encrypt a message and a *private key* to decrypt the message that has been encrypted using the corresponding public key. In many systems, this kind of exchange takes place without the active participation or even awareness of users. Public key cryptography, such as Pretty Good Privacy (PGP) and Transport Layer Security (TLS), underpins a vast range of our modern communications security systems, including email, online web traffic and banking.[23, 24]

An encryption key is meant to be unique and unpredictable and is often formulated in ways to prevent it from being cracked by '**brute force**'; that is, an attacker would need to try and guess every possible key until they stumble upon the right one. Longer keys are harder to crack than shorter ones with each added bit to a key increasing its difficulty to break exponentially.[25] For instance, the popular 128 bit AES encryption algorithm would take 2^{128} guesses (or more than a decillion guesses) to arrive at the correct key — an unfathomably large number of guesses, making it almost impossible even for supercomputers.[26] Underpinning the security of modern encryption systems is Kerckhoff's Principle: that they remain secure even when everything about how they work is known — except for the private key. An encryption private key can be derived through several forms, including for instance a password, pin, or biometric data like a fingerprint, facial or iris scan, making it generally easier for the intended recipient to gain access to encrypted systems, rather than memorizing a lengthy 128-bit string of random characters.[27]

Applying Encryption: In Transit, At Rest and End-to-End

Encryption can be applied to data while it travels through networks, including for example from one's browser to a social media site, and is known as encryption **in transit**.[28] When the data are stored and encrypted on a physical device, it's known as being **at rest**. Different parties are involved in applying encryption and controlling the private key, or the mechanisms in which it's been derived (e.g., password, passcode, etc.), producing different legal and practical implications.[29] Service providers may, for instance, keep the private key to decrypt user data for various purposes, including the improvement of 'quality and services', for data monetization or to provide lawful access to authorities. In doing so, the secrecy of user keys, and therefore information, is left within the hands of the service provider, despite encrypting data both in transit and at rest. Many communications systems, however, are increasingly deploying **end-to-end encryption**, where only the sender and the intended recipient can view the contents of the message in plaintext. This leaves the service provider or any third party, including law enforcement and intelligence agencies, unable to access the message. End-to-end encryption has become increasingly popular over the years, deployed by many messaging applications such as WhatsApp, Signal and iMessage. In such a system, the encryption and decryption take place on the respective devices of users, while the private keys used to decrypt messages never leave the devices.

Strength by Numbers: Encryption’s Growing Use

Today, encryption is commercially deployed on a large scale, becoming a standard in securing hardware, software and networks such as mobile phones and instant messaging services — and becoming a perceived problem for law enforcement and intelligence agencies. More than just keeping information ‘private,’ encryption ensures the confidentiality, integrity, and authenticity of data.

Innovations in modern cryptography have made it practically impossible to reveal the plaintext contents of a file, message, or device on a properly encrypted system without the right key. Although, on the one hand, encryption ensures the confidentiality, integrity, and authenticity of data; on the other hand, it raises concerns for the state, as it allows for information to exist out of the reach of law enforcement and intelligence agencies. While the state does and can exploit other vulnerabilities, such as design and implementation, to circumvent encryption systems as well as the humans who work within them, it cannot do so using brute force alone.[30] The sheer volume of possible keys makes it practically impossible to do so. Rapid technological change has increased the perceived problems of encryption and renewed interest among state actors to circumvent such systems.

Distinct Roles of Intelligence Agencies and Law Enforcement

While the perceived challenges posed by encryption are mainly framed by law enforcement and intelligence agencies, both face different issues. Intelligence agencies identify what are ostensibly seen as threats to national security, determined through risk assessments,[31] while these threats change over time.[32] Included in the course of intelligence gathering is signals intelligence, performed by agencies like the U.S. National Security Agency (NSA) and the Canadian Communications Security Establishment (CSE), which systematically perform bulk collection of communications data, which in the case of the CSE, takes place outside of Canada. These agencies are mainly involved in intercepting and eavesdropping on *data in transit*.[33] Among the methods used to circumvent encryption, these agencies cooperate closely with tech companies to gather and analyze data *before* they become encrypted.[34] Changes to Canada's national security legislation in 2017 also explicitly permit CSE offensive cyber operations to "degrade, disrupt, influence, respond to or interfere with the capabilities, intentions or activities of a foreign individual, state, organization or terrorist group as they relate to international affairs, defence or security."[35]

Although there are some overlapping areas of concern and objective, law enforcement agencies are limited to specific investigations that are justified on some basic grounds, and mainly deal with seizing and gathering evidence including *data* in rest on devices.[36] Law enforcement rarely has the type of technological sophistication, resources or expertise that would be available to an intelligence agency like CSE, which is able to engage in much more intrusive activities, including overcoming encryption. In some cases, law enforcement may seek the assistance of CSE.[37]

A Brief History of the Encryption Debate

Restricting Access: Government Surveillance and Encryption Technologies

Encryption is not a new phenomenon. Ancient societies employed basic forms of encryption to protect and conceal military and political secrets, including notably the Romans through the use of the Caesar Cipher.[38] Although the methods changed significantly, encryption technologies continued to be mainly used by governments to securely share military and intelligence communications, even for much of the 20th century. However, with the invention and commercialization of the internet, encryption systems have taken on new roles, moving beyond protecting military and state secrets, to increasingly being seen as essential in securing the growing commercial activities taking place online. Today, encryption is responsible for protecting and securing the myriad facets of day-to-day life that now rely on networked technologies.[39] It is estimated that encryption technologies are used to protect 87% of all internet traffic, ranging from credit card transactions, to emails and private messages.[40, 41]

The rapid proliferation and expansion of encryption systems, however, has not been without controversy. Over the past four decades, the use and implementation of encryption technologies, particularly within the commercial sphere, has sparked debate on the appropriate role of public policy in this area. Throughout these years, Canada and its Western allies have adopted a range of measures to control the use, implementation and even research on encryption technologies. Researchers often describe these four decades as more precise historical periods.[42] Since the immediate post-WWII period and early days of the Cold War, governments exercised strict control over the availability, control and use of cryptography, with encryption becoming almost exclusively the domain of the military-industrial complex.[43] When commercial encryption applications began to emerge, government agencies in the United States moved to limit and weaken their availability, including by applying export controls on encryption technologies.[44]

By the 1990s, data security began to play a more prominent role as the public began to increasingly adopt the internet, spurred by the growth of e-commerce, adding pressure on governments to reduce restrictions on encryption systems.[45] While government intelligence agencies acknowledged the need to keep online data secure, they were unwilling to allow a reduction of their surveillance capabilities. The state began to wade in with efforts to control the spread of encryption systems, eventually leading to the dawning of the so-called 'Crypto Wars'; and proposals intended to reconcile data security and state surveillance objectives were forwarded. The 'Clipper chip,' introduced in 1993 by the Clinton administration, seemingly enabled the encryption of commercial electronic devices while their secret keys were registered with a government database in an escrow system to allow state actors access to data in plaintext.[46] Like their American counterparts, law enforcement agencies in Canada made similar calls to bypass encryption.[47] Plans for the Clipper chip eventually faltered mainly as a result of significant pressure by activists and privacy advocates.

In the absence of effective government efforts to curtail its proliferation, encryption technologies spread especially quickly. The 2000s saw the encryption debate begin to cool off, with government agencies starting to exploit the growing volume of open source and unencrypted data generated by increasing web activities, including social media, location data and cloud-based storage.[48] Although the Crypto Wars subsided, the underlying tensions never truly went away.

Renewed calls by police and state security actors to circumvent encryption have particularly increased in frequency since 2014, when technology companies began to adopt more sophisticated encryption measures following Snowden's revelations on global state surveillance which, among other disclosures, revealed Western intelligence agencies collaborating with tech and online service providers to bypass encryption systems.[49,50] Public outcry led many tech companies to reorient themselves toward a more pro-encryption stance in efforts to regain public trust, such as enabling encryption by default on mobile operating systems, enabling full-disk encryption on personal computers, and implementing end-to-end encryption on online messaging services.[51] Apple, for example, deployed end-to-end encryption for its iMessage service and later introduced a function that allowed users to delete their phone's data after several unsuccessful login attempts. End-to-end encryption was also implemented by WhatsApp across all devices in 2016. This was followed by Facebook Messenger, which added end-to-end encryption as an opt-in option (called Secret conversations). In March 2019, Facebook announced its intention to integrate WhatsApp, Facebook Messenger and Instagram direct messages, and extend default end-to-end encryption across three platforms.[52,53]

The "Going Dark" Narrative: State Perceptions and Shifts in Discourse

Since then, senior officials from law enforcement and intelligence agencies have introduced the phrase 'going dark' to describe how the growing use of encryption has impeded their investigative and intelligence gathering capacities, essentially reintroducing the encryption debate of the 1990s.[54] Some have argued that the rhetorical shorthand perpetuates a discourse of fear and — like words in general — shapes public understanding in powerful ways,[55] including improperly analogizing how encryption systems work to serve a specific legal or policy response.[56]

In 2015, the fight against strong encryption was taken to new heights following the San Bernardino attack, unleashing a legal battle between the FBI and Apple, with Apple refusing FBI demands to unlock the attacker's iPhone by creating a separate operating system that would be able to bypass certain security features and gain access to the phone's contents (see section on 'backdoors' discussed in the following section). Apple CEO Tim Cook issued a statement that such a move would set a dangerous precedent, and would be equivalent to creating a 'master key' with the potential to unlock millions of other iPhones.[57] The dominant security narrative mainly revolved around the presumption that terrorists were using encryption systems to communicate and plot attacks, undermining the efforts of police and intelligence agencies.

Soon after, child exploitation was linked to end-to-end encryption in a high-profile conference in 2019 hosted by the U.S. Department of Justice. The department sent an open letter to Facebook, signed by its Australian and UK counterparts, requesting that the company stop its implementation of end-to-end encryption across its messaging service, citing child safety.[58] The security narrative on the impacts of encryption shifted its focus from preventing and investigating terrorism to focusing on law enforcement's ability to investigate child sexual abuse material.[59] Following the U.S. Capitol riots in January 2021, law enforcement again shifted focus to domestic violent extremism and the far-right after it was revealed that insurrectionists used encrypted messaging apps like Signal and Telegram to communicate and coordinate — reigniting calls to grant law enforcement special access to encrypted data.[60] Critics, however, argue that the attacks were not a surveillance or intelligence failure, and were planned and orchestrated days before, with ample evidence in plain sight. Instead, they blame police and intelligence unwillingness to take the threat of white supremacist violence seriously.[61] Nonetheless, the narrative on the implications of 'going dark' appear to be shifting, with some governments now using the spread of disinformation on encrypted messaging apps to justify legislative proposals allowing state access to encrypted data, including notably in Brazil and India.[62]

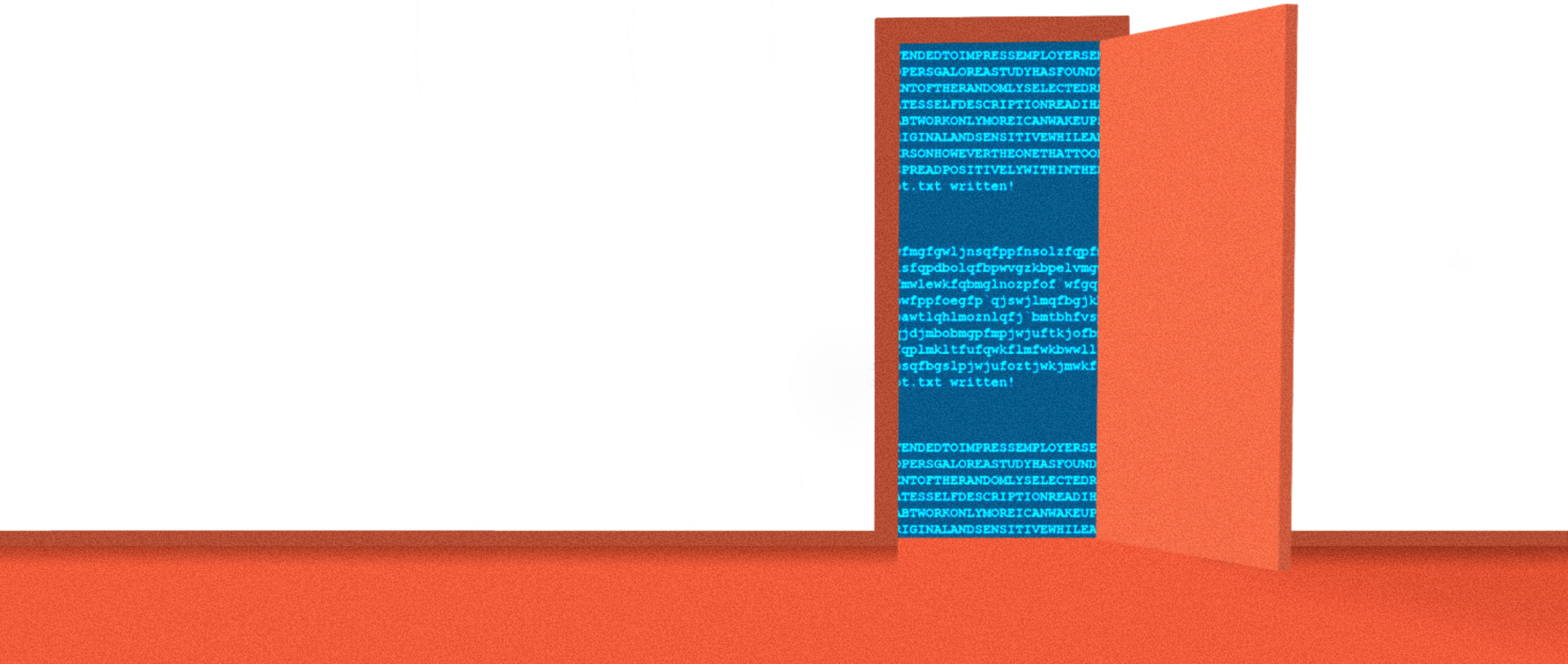
Canadian police and intelligence actors have also been working actively to promote the 'going dark' narrative. In 2016, the Canadian Association of Chiefs of Police highlighted encryption as an investigative challenge and have called for increased powers to compel decryption,[63] echoing the U.S.-based group International Association of Chiefs of Police.[64] In a 2017 report by Public Safety, 'going dark' was explicitly mentioned and went on to blame strong encryption as an impediment to law enforcement's ability to investigate terrorism.[65] As Western countries, including Canada, continue to push calls for increased police powers that grant special access to encrypted data, it is possible for shifts in the encryption narrative to take place, renewing such calls and justifying its circumvention.[66]

"Backdoors": Gaining Access to Encrypted Data, and the Costs to Privacy and Security

To help close the perceived gap between state authority and technical reach, officials have been calling for legislative changes that provide law enforcement and security agencies with what they refer to as 'exceptional access' to encrypted data. Such proposals are centred on compelling companies to create the technical capacity that grants them — when legally authorized — access to what would otherwise be encrypted communications, in plaintext. Essentially, what is being demanded by government is a technical framework commonly known by the metaphor 'backdoor'.[67] Backdoors are inserted into the design of a program or algorithm as a means to bypass the normal method of user authentication, allowing state authorities access to encrypted data without having the correct credentials.[68]

Perhaps the most infamous 'backdoor' system is *key escrow*, where decryption keys are held in escrow and meant to be accessible to state authorities during investigations. This was the approach taken by the Clinton administration in 1993 in its early efforts to create a *'backdoor'* through the Clipper chip, as discussed previously. In the case of the Clipper chip, plans to insert the 'backdoor' were made explicit and immediately resulted in widespread backlash, ultimately leading to it being entirely defunct. However, 'backdoors' are usually inserted covertly, without the wider public's knowledge. For instance, in Canada, the RCMP used what has been described as a 'global master key' to unlock encrypted messages sent using Blackberry devices in a mafia-related investigation between 2010 and 2012.[69] As part of the operation, police were able to intercept over one million messages between those years — details of which only came to light in 2016 through court documents.[70] News of the operation also raised concerns that the communications of ordinary Canadian BlackBerry users have been vulnerable to government surveillance. Many other details of the operation remain unknown, including how the police obtained the key, whether it was subsequently changed, and how long Canadian police forces continued to use the 'backdoor' system after the conclusion of the investigation.

Technologists, including leading cryptographers from industry and academia, argue that forcing companies to weaken their encryption systems by mandating companies to provide communications through 'backdoors' would create widescale vulnerabilities to be exploited by criminal actors and foreign state agents.[71] Even Facebook strongly signaled its intention to resist such a mandate, claiming that any such 'backdoor' would "be a gift to criminals, hackers, and repressive regimes."[72] In other words, there is no guarantee that the backdoors and decryption keys would be exclusively used by state agencies that have the legal authority to do so. Others have described such an approach akin to having the state require that every household keep its backdoors unlocked, just in case first responders need access to people's homes in the event of an emergency.[73] The technical reality is that there is no possibility of introducing weakness into encryption systems without systemically compromising the security and privacy of all users. Security officials nonetheless continue to believe otherwise, arguing that it is possible to grant access to encrypted data only to them and denying it to others.[74]



```
ENDEDTOIMPRESSEMPLOYERSE
PERSGALOREASTUDYHASFOUND
NTOFTHERANDOMLYSELECTEDR
TESSELFDESCRIPTIONREADIH
BTWORKONLYMOREICANWAKEUP
IGINALANDSENSITIVEWHILEA
RSONHOWEVERTHEONETHATTOO
PREADPOSITIVELYWITHINTHE
t.txt written!


fmgfgwljnsqfppfnsolzfqpf
sfqpdbolqfbpwvgzkbpelvmg
mwlewkfqbmglnozpfof`wfgq
wfppfoegfp`qjswjlmqfbgjk
awtlqhlmoznlqfj`bmtbhfvs
jdjmbobmgpfmpjwjuftkjofb
qplmkltfufqwkflmfwkbwwll
sqfbgslpjwjufoztjwkjmwkf
t.txt written!


ENDEDTOIMPRESSEMPLOYERSE
PERSGALOREASTUDYHASFOUND
NTOFTHERANDOMLYSELECTEDR
TESSELFDESCRIPTIONREADIH
BTWORKONLYMOREICANWAKEUP
IGINALANDSENSITIVEWHILEA
```

Going Around Encryption: Digital Forensic Tools

Law enforcement has increasingly been using digital forensic tools to retrieve encrypted data on devices like smartphones. Perhaps the most infamous of these tools are the Israeli-based law enforcement, Cellebrite, which was initially presumed to have unlocked the iPhone belonging to the San Bernardino shooter,[75] as well U.S.-based Grayshift. These tools work by exploiting the vulnerabilities of device operating systems including for example by accessing keys in the quick access memory to decrypt data.[76] In this less secure state, known as "After First Unlock", encryption keys get stored in the quick access memory for applications to quickly and easily decrypt data. This occurs after the user unlocks their phone for the first time after being rebooted. The tools exploit such vulnerabilities at the operating system level, expanding the attack surface for authorities (or malicious actors) and providing more data to access.[77] According to one report, there are nearly 50,000 examples of U.S. police across the country using such tools to get access to smartphone data between 2015 and 2019.[78] Government disclosures suggest that law enforcement in the U.S. currently finds successful workarounds for encrypted devices about half the time.[79] In Canada, the RCMP are known to use Cellebrite though have remained silent on its use refusing to answer questions on 'sensitive investigative techniques.'[80] However, such practices have not been without controversy operating within a legal grey zone. Police agencies that conduct searches on devices often do so lacking policies regulating the practice and are only constrained by nascent and rapidly changing case law, raising concerns over violating individual rights and freedoms.[81] Nonetheless, such practices reveal the success police have in retrieving encrypted data through workarounds.

Online Harms and Content Moderation Proposals

In this section, legislative and technical proposals are outlined that will likely influence the direction of the encryption debate going forward — both of which require careful thought and consideration by Canadian policymakers, as their implementation may carry unintended consequences including expansion of government surveillance, posing risks to rights and freedoms, including to privacy and free expression.

The 'Duty of Care' Model

Governments around the world are increasingly concerned about the role that social media and messaging platforms play in spreading online harms, such as terrorism and child pornography.[82] As a response, several jurisdictions, including the UK, Germany and other European governments, have advanced proposals that place responsibility on the platforms, including the moderation of online content. The UK's Online Safety Bill, also referred to as the 'Duty of Care' model, is among such proposals that are increasingly gaining traction elsewhere including in Canada. The proposed law would require that companies take down and introduce other measures that prevent the spread of 'harmful' user-generated content, even if lawful, based on a government-prescribed 'code of conduct', or otherwise face fines as well criminal charges against senior directors.[83] The laws are set to apply widely and not just to social media, including websites, apps and services that host user-generated content, or allow users to communicate with one another.[84,85] By extension, this would include encrypted messaging apps, which could undermine digital privacy and anonymity by virtue that many such apps and services use end-to-end encryption, with many others, including Facebook Messenger, soon to follow.

Although the bill does not ban it, companies that use end-to-end encryption are not exempt and would have to demonstrate how they meet the new requirements or face charges.[86] In a March report, the Centre for Social Justice, a think tank headed by former Home Secretary, Sajid Javid, advised the proposed regulator, Ofcom, to 'treat high-risk design features like end-to-end encryption as breaches of the Duty of Care and sanction should be able to apply retroactively.'[87] It remains unclear how companies that use end-to-end encryption will be able to meet the new requirements; and it also raises questions on whether companies will be implicitly coerced into introducing vulnerabilities in order to comply with the new laws. Some have suggested that such demands aimed at companies that offer end-to-end encrypted messaging are a 'last resort' when alternative approaches have failed.[88] For instance, much of the driving force behind the government's push for the bill's adoption has been calls for tech companies to address child sexual exploitation online.[89] There is indication that such pressure has led companies like Instagram to make changes to their software design, including restricting adults from privately messaging minors who they don't follow, rather than scrapping their plans to employ end-to-end encryption.[90]

As the duty of care model and other similar legislative proposals continue to be advanced by other jurisdictions, it's possible that such an approach may also be considered in Canada. However, policymakers will need to proceed with the same caution as with any proposal that requires platform monitoring and removal of user-generated content, particularly with respect to how the 'codes of practice' will implicate encryption systems, including end-to-end encryption.[91]

Client-Side Scanning

Among the technical proposals aimed at addressing the perceived concerns of state actors with encryption includes client-side scanning. In this approach, videos and images are scanned and matched against a database of prohibited content either before or after it is transmitted to the recipient.[92] In some proposals, if the message matches the content of prohibited material, the full message would be barred from being sent or sent to a third party for manual review. This the approach taken by Apple in its recent decision to scan photographs on mobile devices prior to being uploaded to Apple's iCloud servers for purposes of identifying child sexual abuse materials.[93] Although the principle use of the technology is for preventing the dissemination of child sexual exploitation materials in the form of photos and videos, it is theoretically possible to repurpose the technology to monitor various other kinds of information – a very likely risk that many have raised in response to Apple's decision.[94]

In its most common proposed form, client-side scanning technology works by comparing a 'hash'[95] of a photograph intended for distribution with a database containing hashes of known illegal materials. PhotoDNA is a popular client-side scanning program in use today and works by comparing unencrypted information on a sender's personal device with a file containing the hashes of illegal materials that has been added to the database by an authoritative source. If the system identifies a match, some sort of alert can be established by the system, including preventing the material from being shared. PhotoDNA is currently being used by Facebook Messenger, Instagram and WhatsApp on unencrypted information to identify and remove child sexual exploitation materials.[96] WhatsApp on unencrypted information to identify and remove child sexual exploitation materials. Apple's plan, on the other hand, goes further by using the technology on encrypted materials on device; Apple says it plans to manually review each report after an account uploads a certain threshold of identified materials before disabling the account and sending a report to authorities. In addition, Apple announced its intention to scan text messages sent or received by children on Apple's messaging app for sexually explicit photos, adding warnings to users and notifications to parents if such materials have been identified.[97]

Although client-side scanning has been presented by some jurisdictions[98] as a solution to the encryption challenge, it is seen by many experts and privacy advocates as a form of 'backdoor access'[99] that can be exploited by third-party adversaries.[100] Deeper examination reveals there are many technical, legal and policy challenges for client-side scanning to be ready for adoption. The technique has been mostly advanced to identify and reduce the distribution of child sexual abuse materials, and not other public safety or national security risks such as countering far-right and domestic violent extremism. So long as these threats are seen as viable by state security actors, the spectre of legislatively weakening encryption will continue to remain. Further, the impact of client-side scanning technology on the performance of individual devices is unclear. And it is also uncertain whether such an approach would take place at an operating system level or application (the former creating more significant cybersecurity implications); who determines what 'harmful' content is included in the database; who would be in control of the database; and how other jurisdictions may use the technology, including those that don't share the same democratic principles and values.[101] This is in addition to the technology's disruption of Western society's notions of privacy and control; and would create an impression of over surveillance, leading to an inevitable chilling effect.

Recent and Ongoing Policy Developments in the West

Over the past forty years, governments around the world have been introducing legal and policy responses to the challenges raised by encryption, including legal and covert measures.[102] State practices have included applying *regulations to the exports* of encryption to control its use and distribution; *directing efforts to various actors*, such as commercial and academics, to weaken encryption tools and standards and consumer software; *directly compelling service providers* to provide unencrypted information, including through secret keys or passwords; and *compelling individuals* to provide the key or password to decrypt information themselves.[103,104] More recently, several legislative proposals and discussions have taken place in the West, seeking to circumvent encryption and introduce new exceptional access powers. Although not meant to be an exhaustive list, this section provides a current snapshot of some of these recent and ongoing policy developments.

The United Kingdom

In 2016, the UK passed the *Investigatory Powers Act*. Dubbed by some the ‘snoopers charter,’[105] this law granted the Secretary of State a new power to issue “technical capability notices”, which could include “obligations relating to the removal… of electronic protection applied by or on behalf of [the service provider] to any communications or data”.[106] After much pushback from tech companies, the bill was amended to specify that any such order must be ‘technically feasible’ for the company in question.[107] Although the provision can compel companies to re-engineer their platforms in fundamental ways, including removing end-to-end encryption, some experts believe the government avoids doing so as the implications can be significant, including the migration of users to other platforms with less cordial government relationships or no corporate presence at all.[108] However, the government’s stance has been explicitly in favour of inserting backdoors. Former Home Secretary Rudd advanced the view that end-to-end encryption is not for 'real people' and should be banned, a position which gained tacit support from then-Prime Minister May.[109] The UK government has only used these powers once, with a non-binding request that WhatsApp "build a way to give [the Government] access to encrypted messages." However, WhatsApp opted to not comply with this request. It has been suggested that even if the new powers afforded by this law included the power to force companies to weaken their encryption, the UK government would avoid doing so for fear of enforcement challenges.[110]

Australia

In 2018, Australia enacted a controversial new law, the *Assistance and Access Act*, allowing law enforcement and intelligence agencies to compel designated communications providers, including social media platforms, to provide technical assistance for investigations.[111,112] The Australian government, like the UK, has specifically cited end-to-end encryption as the specific problem. As with the *Investigatory Powers Act* in the UK, there is some ambiguity regarding the scope of these powers. In the case of Australia, this ambiguity stems from the language used. For example, the legislation specifies that state authorities *cannot* require companies to develop new decryption features that 'render systemic methods of authentication or encryption less effective'; however, they *can* require those same companies to 'selectively [introduce such features] to one or more target technologies that are connected with a particular person.' Many technology companies and privacy advocates have questioned whether this 'selective' weakening of encryption is possible from a technical perspective without creating broader vulnerabilities. Some have suggested that platforms may be able insert spyware that enables agencies to read encrypted messages on particular devices, rather than introducing structural changes to their broader encryption methods.[113,114] If the companies do not have the tools to intercept encrypted data for authorities, they can be required to create new tools to do so. Companies failing to comply could face fines of up to $7.2 million USD.[115] Despite the unresolved ambiguity, the legislation has reportedly already been used by police investigating drug trafficking and child exploitation. The legislation has come under scrutiny for its lack of clarity and oversight and has also been criticized for creating a negative reputation to Australia's technology sector affecting growth and innovation.[116]

The United States

In 2019, the U.S. Attorney General and Secretary of Homeland Security, along with the UK Home Secretary and Australian Minister for Home Affairs, wrote to Facebook to request that it “not proceed with its plan to implement end-to-end encryption across its messaging services without ensuring that there is no reduction to user safety and without including a means for lawful access to the content of communications to protect our citizens.”[117] Shortly thereafter, the U.S. Senate took up the issue as well, threatening to legislate backdoor access if Apple and Facebook did not comply.[118] Most recently, the *EARN IT Act* has been proposed, giving state legislatures the power to threaten internet companies with civil litigation forcing them to break encryption. Under the proposed bill, internet companies must abide by a set of ‘best practices’ in order to ‘earn’ the continuation of the legal protections they enjoy with regard to the moderation of the content hosted on their platforms.[119,120,121,122] Some have suggested that these ‘best practices’ may include a hard mandate to ban end-to-end encryption, with the Stanford University Center for Internet and Society stating that the goal of the bill is ‘to ban end-to-end encryption without actually banning.’[123] Similarly, the proposed *Lawful Access to Encrypted Data Act*, introduced in 2020, would require tech companies to assist state authorities in decrypting data, including by requiring them to provide ‘any technical capabilities that [are] necessary to implement and comply with anticipated court orders’, as well as establish ‘prize competition’ and ‘incentivize and encourage research and innovation into solutions providing law enforcement access to encrypted data pursuant to legal process.’[124] It’s important to note that there has been a change in tone on the encryption debate, with newly installed Biden administration appearing largely dormant on the issue, despite police and intelligence actors continuing to maintain their positions.[125]

The European Union

The European Commissioner launched its ‘Delivering on the security union’ in July 2020, with an industry consultation to “map and preliminarily assess, by the end of 2020, possible technical solutions to detect and report child sexual abuse in end-to-end encrypted electronic communications, and to address regulatory and operational challenges and opportunities in the fight against these crimes.”[126] In a subsequent non-legally binding resolution adopted in December 2020, the Council of the European Union expressed support for robust encryption while arguing for ‘targeted, lawful access to encrypted data.’ Though it is not clear how EU lawmakers will achieve this, discussions will take place with the tech industry on solutions to gain access to encrypted data, making it clear that it will not include backdoors.[127]

Encryption in Canada: Shifts in Policy

Canada has generally avoided imposing legal obligations on tech companies that would require them to decrypt or establish 'backdoor' access to encrypted data.[128] Canada did, however, come close in 2012 by introducing Bill C-30, which would have imposed decryption requirements on telecommunications service providers, which was eventually withdrawn after considerable opposition.[129] Although there is currently no specific power to compel third-party decryption in the Criminal Code, courts may compel third parties to assist with investigations.[130] Nonetheless, rapid changes in technology, including the proliferation of strong encryption to secure communications, has reignited the perceived urgency in the encryption debate and renewed calls in Canada for government 'backdoor' schemes.[131]

Although Canada has remained relatively quiet on the encryption debate,[132] while occasionally voicing support for strong encryption,[133] recent developments indicate a shift in policy. In October 2020, the Government of Canada issued a joint statement with its Five Eyes counterparts — the United States, the United Kingdom, Australia and New Zealand — calling on technology companies to find 'technically feasible solutions' that "enable law enforcement to [access] content in a readable and usable format."[134] Prior to this, Canada had issued a joint communiqué in July 2019, again along with the Five Eyes, directing companies to introduce ways to allow government access to encrypted technologies.[135] At the moment, Canada and its allies have left questions of *how* to achieve this to the tech companies themselves.

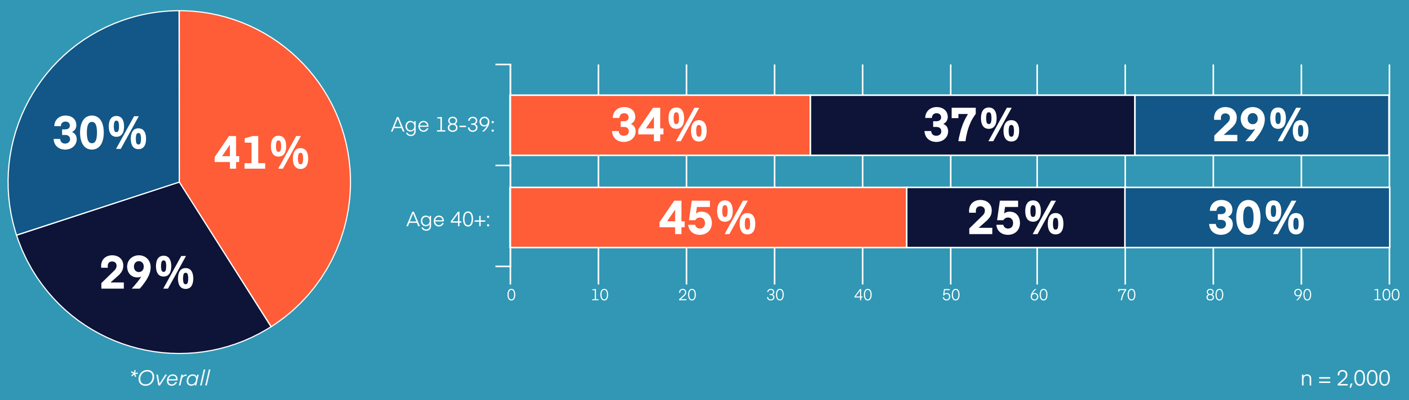
These most recent statements highlight a broader shift in government posture toward encryption in Canada, and among Western countries broadly. Indeed, this change in Canada's posture may be the result of increasing pressure from strategic allies, particularly from then U.S. Attorney General William Barr.[136] The U.S. Capitol Hill riots and the growing threat of domestic violent extremism have also been leveraged by security officials to further push proposals compelling tech companies to create 'backdoors', citing the growing use of end-to-end encrypted messaging apps as a national security challenge.[137] It appears that Canada has recanted its historical support for strong encryption calling on tech companies to intentionally introduce weaknesses into the design of encryption systems to facilitate government surveillance.[138]

Canadians' Opinions on Encryption

The following figure provides the results of our representative online survey with 2,000 adult Canadian residents and 20 follow-up semi-structured interviews with survey participants in May 2020 asking Canadians to share their views on encryption. Our question introduced Facebook's plan to roll out end-to-end encryption to its other services, including Messenger and Instagram, and the concerns law enforcement have regarding the subsequent impact on preventing certain types of crime. This was followed up with a question on whether respondents believed that the prevention of crime was more or less important than the privacy and security of their communications. Although 41% believe that preventing crime is more important, a combined majority are either unsure (30%), or believe that the privacy and security of their communications are more important (29%). While mindful of not imparting any naivety on the part of survey respondents, the relative lack of public awareness of the issue (30%) is high; and may be an indication that Canadians need more information on the topic, including on the wide-ranging benefits of encryption and the costs for undermining or deliberately weakening it.

Canadians Divided on Encryption

"Some online messaging services, such as Facebook's WhatsApp and Apple's iMessage, offer end-to-end encryption. This technology means only the sender and receiver can read or see the messages. Facebook has announced plans to implement end-to-end encryption across its direct messaging services, including Messenger and Instagram. Law enforcement in several countries have raised concerns with this technology. They argue that encryption makes it more difficult to prevent and stop criminal activity, such as terrorism, organized crime, sex trafficking and child sexual exploitation. Which of the following do you most agree with?"



🟧 Law enforcement's ability to prevent and stop criminal activity is more important than the security and privacy of direct messaging

■ The security and privacy of direct messaging is more important than law enforcement's ability to prevent and stop criminal activity

🟦 Not sure/don't know

"I think it depends on which crimes are being targeted, like, what exactly are people doing that requires invading their privacy. I feel there's definitely some actions out there that can be more intimidating than others. So, if they're looking for a murderer, I would be more in favour of breaching other people's privacy."
Man, 18-29

"I feel like I'm kind of more 50/50. I guess if people aren't doing anything wrong, then why would they be worried about anyone looking? On the other hand, I feel like privacy is really important, and I don't do anything illegal, but I just want people to respect privacy."
Woman, 18-29

"I think it depends on what types of crimes. Are we talking about threats against society or are we talking about individual crimes? So, it is a question of who has that information and how are they using it? Sort that out and I might support it. And the police have recently gotten a difficult rap with overreaching on some things, so that is on the back of my mind."
Man, 50-59

Moving Forward: An Alternative Framework to Guide Policy-Making on Encryption

Apple's recent decision to scan photographs and text messages for child sexual exploitation materials has sprung the encryption debate to the forefront, yet again. Although it can be argued that Apple's move represents a preemptive decision on the part of Big Tech — and no doubt greatly influenced by state security actors — the spectre of legislatively weakening encryption technologies continue to remain, especially when other public safety and national security risks, such as terrorism and far-right extremism, continue to exist. However, such legislative moves can and should be avoided as the consequences disproportionately outweigh the potential benefits that may be achieved.

This policy brief reveals that the encryption debate needs to be seen within a broader framework. It is hoped that the alternative lens presented here can help guide policy-making on questions of encryption. This framework emphasizes that law enforcement and intelligence agencies have other options to cope with challenges in encryption. This includes gathering other **non-encrypted data that is accessible**, such as metadata and open source information (e.g. social media, information online, etc.). Depending on the platform's business model and application, non-encrypted metadata can be examined on encrypted platforms, which can potentially reveal insights about content that includes, for example, the sharing of child sexual abuse materials. WhatsApp uses PhotoDNA (as discussed earlier) to proactively scan unencrypted information, to identify groups suspected of sharing child sexual exploitation materials. If any matches are made to known illegal materials, the image is prevented from being shared and the suspected accounts are blocked. Although Facebook claims the approach shows promise[139], there is a need for independent experts to verify such claims through access to company reports and data (discussed below). Of course, there is a need for independent experts to verify these claims and thus would require access to reports and data from companies (discussed below).

Although Apple's underlying technology for its proposed client-side scanning system is similar to PhotoDNA, as mentioned above, Apple's plans go further by not focusing solely on unencrypted materials. In addition to raising tensions in a democracy, the plan also raises critical questions related to privacy and security, moving beyond those encountered through the use of PhotoDNA, making Apple's approach far more controversial. This is not to say that WhatsApp's use of unencrypted information (i.e. metadata) is perfect. There are also criticisms and broader worry surrounding WhatsApp's use of metadata, and thus third-party evaluations of such approaches are needed to guide best practices for use on other social media platforms.[140]

Other non-encrypted sources of information can also be corroborated, including open-source information from social media in what is popularly known as OSINT (open-source intelligence). Experts have long argued that law enforcement and intelligence agencies are becoming increasingly data-driven and have access to more data than ever before to aid investigations and intelligence gathering.[141,142] However, the collection and analysis of even non-encrypted data raises significant concerns to democratic rights and civil liberties, and constitute issues that include the expansion of surveillance and disproportionately targeting people of colour and other members of vulnerable communities. Although these concerns extend beyond the scope of this brief, such practices reveal the investigative potential for Canadian agencies without the need for additional legal powers. Any proposed legislation or policy aimed at further extending police and intelligence powers through 'backdoors' would be far more damaging and irresponsible.[143]

At a higher level, the government can **require tech companies to apply greater efforts in identifying and removing unencrypted illegal materials,** particularly where content remains open and accessible to the wider public. Research shows that there is a cross-flow of information between these 'open' platforms and 'closed' encrypted messaging apps. For instance, open platforms such as Facebook and Twitter may be used by individuals and groups to amplify extremist content by exploiting functions like hashtags; or be used to 'groom' children before migrating to more 'closed' environments like encrypted messaging apps.

Disrupting this cycle is therefore key and can be done by requiring or incentivizing platforms to introduce **safer design features**. For instance, design mechanisms can be put in place to prevent connections between minors and adult strangers, or those adults not on the minor's contact list, as in the case of Instagram.

Finally, governments can **require tech companies to provide regular and transparent reports** providing data detailing their response in curtailing illegal activities, including metrics on takedowns categorized by time periods and reasons for takedown, user reporting, and user bans and suspensions. Such detailed reports can help law enforcement, researchers, civil society and governments identify and home in on specific issues, and identify patterns and trends on criminal activities, evaluate the effectiveness of policies, and formulate tailored responses that are ethical and meet the threshold of necessity and proportionality.

A number of factors have been used in this brief to evaluate whether government proposals that require tech companies to provide them with access to encrypted data are appropriate. As with other surveillance and data gathering practices, the principles of necessity and proportionality should be used as a guiding mechanism in evaluating surveillance and data gathering measures. This helps determine whether the response lowers privacy and security protections; and if it's proportionate to the risk posed and not large enough in scale to encroach the rights of uninvolved parties.[144] Although domestic violent extremism and child sexual exploitation are clearly legitimate threats requiring a government and criminal justice response, the consequences of weakening encryption systems by introducing 'backdoors' may be far more damaging to national security and the safety of children.[145] Thus, Canada should avoid introducing any legislative proposals that require tech companies to weaken encryption by inserting vulnerabilities in order to facilitate government surveillance. Rather, Canada can and should be leading by example, by advocating for strong encryption. Our cyber systems and infrastructures, and the people who rely on them, depend on it.

References

[1] Parson, C. (2019, August 21). Canada's new and irresponsible encryption policy: How the government of Canada's new policy threatens, charter rights, cybersecurity, economic growth, and foreign policy. *Citizen Lab*. Retrieved from https://citizenlab.ca/2019/08/canadas-new-and-irresponsible-encryption-policy-how-the-government-of-canadas-new-policy-threatens-charter-rights-cybersecurity-economic-growth-and-foreign-policy/

[2] United States Department of Justice. (2020, October 11). International Statement: End-to-End Encryption and Public Safety. Retrieved from https://www.justice.gov/opa/pr/international-statement-end-end-encryption-and-public-safety

[3] Abelson, H. et al. (2015, July 6). Keys under doormats: mandating insecurity by requiring government access to all data and communications. Retrieved from https://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf

[4] In particular, the works of Christopher Parsons, Tamir Israel and Lex Gill, in Canada, have been instrumental in building and mobilizing knowledge on encryption. See for instance: Gill, L., Israel, T., and Parsons, C. (2018, May). Shining a light on the encryption debate: A Canadian field guide. *Citizen Lab*. Retrieved from https://citizenlab.ca/wp-content/uploads/2018/05/Shining-A-Light-Encryption-CitLab-CIPPIC.pdf

[5] Gursky, J and Wooley, S. (2021). Countering disinformation and protecting democratic communication on encrypted messaging applications. *Brookings*. Retrieved from https://www.brookings.edu/wp-content/uploads/2021/06/FP_20210611_encryption_gursky_woolley.pdf

[6] Apple privacy letter. (2021, August 6). An open letter against Apple's privacy-invasive content scanning technology. Retrieved from https://appleprivacyletter.com/

[7] For example, in November 2020, it was revealed that members of the Black and Muslim communities in the U.S. had their personal data gathered from innocuous-seeming apps and funneled into a complex web of data exchanges, being ultimately sold to bidders, including the U.S. government. See for e.g. Cox, J. (2020, November 16). How the US Military Buys Location Data from Ordinary Apps. *Motherboard*. Retrieved from https://www.vice.com/en/article/jgqm5x/us-military-location-data-xmode-locate-x

[8] United States Department of State. (2020, August). Pillars of Russia's Disinformation and Propaganda Ecosystem. Retrieved from https://www.state.gov/wp-content/uploads/2020/08/Pillars-of-Russia%E2%80%99s-Disinformation-and-Propaganda-Ecosystem_08-04-20.pdf

[9] Parsons, C. [caparsons]. (2018, November 18). Chris: left unstated, this information can also be leveraged by foreign intelligence services to identify weaknesses to capitalize on and potentially turn individuals into agents of a foreign power. Keeping this data secure is *really* important. Private businesses... [Tweet]. Retrieved from https://twitter.com/caparsons/status/1329174083242762243

[10] Government of Canada. (2020). National cyber threat assessment 2020. Communications Security Establishment. Retrieved from https://cyber.gc.ca/sites/default/files/publications/ncta-2020-e-web.pdf

[11] Burt, A. (2019, January 3). Privacy and cybersecurity are merging. Here's why that matters for people and companies. *Harvard Business Review*. Retrieved from https://hbr.org/2019/01/privacy-and-cybersecurity-are-converging-heres-why-that-matters-for-people-and-for-companies

[12] Deibert, R (2012, August). Distributed Security as Cyber Strategy: Outlining a Comprehensive Approach for Canada in Cyberspace . Prepared for the Canadian Defence & Foreign Affairs Institute. Retrieved from https://citizenlab.ca/wp-content/uploads/2012/08/CDFAI-Distributed-Security-as-Cyber-Strategy_-outlining-a-comprehensive-approach-for-Canada-in-Cyber.pdf .

[13] Public Safety Canada, ATIP A-2018-00078, page 330. Available at: https://citizenlab.ca/wp-content/uploads/2019/08/A-2018-00078.pdf.

[14] Jean-Guillaume, D, Roch, J., Tannier, E., and Varrette, S. (2015) *Foundations of Coding: Compression, Encryption, Error Correction*. Hoboken, New Jersey : Wiley See also *Surveillance-Self Defence*. (2018, November 14). What should I know about encryption?. Retrieved from https://ssd.eff.org/en/module/what-should-i-know-about-encryption.

[15] In 1587 for instance, Mary Queen of Scots was convicted of treason and then beheaded for her role in an assassination plot against Queen Elizabeth; her participation was revealed through the decryption of private letters among the conspirators see: Kahn. D. (1967). *The Codebreakers: The Story of Secret Writing*. Macmillan: NY

[16] Kerr, O.S., and Schneier, B. (2017, March 20). "Encryption Workarounds," *106 Georgetown Law Journal 989* , Retrieved from https://ssrn.com/abstract=2938033.

[17] Schneier, B. (2009). *Secrets & Lies: Digital Security in a Networked World*. Wiley Publishing: New Jersey

[18] Ibid.

[19] If it is not generated at random, adversaries are provided with an opportunity to predict patterns, reducing the amount of 'guesses' required to decrypt the ciphertext.

[20] Guy, P. (2017, November 27). What is Encryption & How Does it Work? *Medium*. Retrieved from https://medium.com/searchencrypt/what-is-encryption-how-does-it-work-e8f20e340537

[21] UK Information Commissioner's Office. (2021). What types of encryption are there? Retrieved from https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/encryption/what-types-of-encryption-are-there/

[22] The Diffie-Hellman exchange and the development of RSA in the 1970s marked the beginning of public key cryptography, addressing the problems of key distribution. See: Diffie, W. & Hellman, M.E., (1976). New directions in cryptography *IEEE Transactions on Information Theory, 22*(6), 644-54. Rivest, R.L., Shamir, A., &Adleman, L. (1978) A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Communications of the ACM, 21*(2), 120-26

[23] Gill, L. (2018). Law, Metaphor, and the Encrypted Machine. *Osgoode Hall Law Journal* 55(2), 440-477.

[24] Parson, C., and Israel, T. (2015, August 11). Canada's Quiet History of Weakening Communications Encryption. *Citizen Lab*. Retrieved from https://citizenlab.ca/2015/08/canadas-quiet-history-of-weakening-communications-encryption/

[25] Schneier, B. (1996). *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, 2nd ed. John Wiley & Sons: NY

[26] Ibid.

[27] Kerr, O.S., and Schneier, B. (2017, March 20). Encryption Workarounds. *106 Georgetown Law Journal 989*, Retrieved from https://ssrn.com/abstract=2938033.

[28] Parsons, C. (2019).

[29] Gill, L. (2018).

[30] Although many encryption systems are nearly impossible to break using brute force alone, researchers have also pointed out that other types of encryption systems being rather easy to break including 128-bit RSA asymmetric key. Increasing key length to make it more difficult to break an encryption system is generally true for symmetric algorithms and not true for many popular asymmetric algorithms like RSA. For more, see: Knockel, J., Senf, A. & Deibert, R. (2016, March 28). WUP! There It Is: Privacy and Security Issues in QQ Browser, *Citizen Lab*. Retrieved from https://citizenlab.ca/2016/03/privacy-security-issues-qq-browser/ as cited in Gill, L., Israel, T., and Parsons, C. (2018, May). Shining a light on the encryption debate: A Canadian field guide. *Citizen Lab*. Retrieved from https://citizenlab.ca/wp-content/uploads/2018/05/Shining-A-Light-Encryption-CitLab-CIPPIC.pdf

[31] To learn about the intelligence cycle and how intelligence agencies assess risks, see: Gill, P. and Pythian, M. (2018). *Intelligence in An Insecure World*. Polity. London; Andrew, C.M., Aldrich, R.J., and Wark, W.K. (2019). "Introduction: What is intelligence? -- Wanted: A definition of "intelligence"" (Eds.) Christopher M. Andrew, Richard J. Aldrich, Wesley K. Wark. *Secret Intelligence: A Reader*. London: Routledge.

[32] To learn more about how objects of security are constructed by the state see: Buzan, B., Wæver, O., & Wilde, J. . (1998). *Security: A new framework for analysis*. Boulder, Colo: Lynne Rienner Pub.

[33] Lyon, D. (2015). *Surveillance after Snowden*. London: Polity

[34] New York Times. (2013, September 5). Secrets reveal N.S.A campaign against encryption. Retrieved from https://archive.nytimes.com/www.nytimes.com/interactive/2013/09/05/us/documents-reveal-nsa-campaign-against-encryption.html

[35] Bill C-59, An Act respecting national security matters, 1st Sess, 42nd Parl, (21 June 2019) Retrieved from https://www.parl.ca/DocumentViewer/en/42-1/bill/C-59/royal-assent

[36] Gill, L., Israel, T., and Parsons, C. (2018, May). Shining a light on the encryption debate: A Canadian field guide. *Citizen Lab*. Retrieved from https://citizenlab.ca/wp-content/uploads/2018/05/Shining-A-Light-Encryption-CitLab-CIPPIC.pdf

[37] Ibid.

[38] Castro, D. (2020, July 13). Why new calls to subvert commercial encryption are unjustified. *Information Technology & Innovation Foundation*, Retrieved from https://itif.org/publications/2020/07/13/why-new-calls-subvert-commercial-encryption-are-unjustified

[39] Castells, M. (1996). *The Rise of the Network Society*. Wiley: NY

[40] National Academies of Sciences, Engineering, and Medicine. (2018). Decrypting the Encryption Debate: A Framework for Decision Makers. Washington, DC: The National Academies Press. Retrieved from https://www.nap.edu/catalog/25010/decrypting-the-encryption-debate-a-framework-for-decision-makers

[41] Rashid, Y.F. (2019, June 12). Encryption, Privacy in the Internet Trends Report. *Decipher.* Retrieved from https://duo.com/decipher/encryption-privacy-in-the-internet-trends-report

[42] Parsons, C. (2019).

[43] Hellegren, I. (2017). A history of crypto-discourse: encryption as a site of struggles to define internet freedom, *Internet Histories, 1*(4), 285-311

[44] Gill, L., Israel, T., and Parsons, C. (2018, May).

[45] Ranger, S. (2015, March 23). The undercover war on your internet secrets: How online surveillance cracked our trust in the web. *Tech Republic*. Retrieved from https://www.techrepublic.com/article/the-undercover-war-on-your-internet-secrets-how-online-surveillance-cracked-our-trust-in-the-web/

[46] Levy, S. (1994, June 12). Battle of the Clipper Chip. *The New York Times.* Retrieved from https://www.nytimes.com/1994/06/12/magazine/battle-of-the-clipper-chip.html?pagewanted=all

[47] Evenson, B. (1996, August 23), Going Cryptic on the Net, *The Ottawa Citizen.* Archived at: http://www.efc.ca/pages/media/ottawa.citizen.23aug96.html

[48] Gill, L., Israel, T., and Parsons, C. (2018, May).

[49] Nakashima, E. (2013, September 5). NSA has made strides in thwarting encryption used to protect Internet communication. *The Washington Post*. Retrieved from https://www.washingtonpost.com/world/national-security/nsa-has-made-strides-in-thwarting-encryption-used-to-protect-internet-communication/2013/09/05/0ec08efc-1669-11e3-a2ec-b47e45e6f8ef_story.html;

[50] Miller, C.C. (2013, June 7). Tech Companies Concede to Surveillance Program. *The New York Times*. Retrieved from https://www.nytimes.com/2013/06/08/technology/tech-companies-bristling-concede-to-government-surveillance-efforts.html?ref=global-home&_r=1&&pagewanted=all

[51] Castro, D. (2020, July 13).

[52] Hutchinson, A. (2020, September 30). Facebook Announces Integration of Messenger and Instagram Direct, Adds New Messaging Features. *Social Media Today.* Retrieved from https://www.socialmediatoday.com/news/facebook-announces-integration-of-messenger-and-instagram-direct-adds-new/586180/

[53] According to our survey in May 2020, these three platforms together represent more than 80% of social media messaging in Canada soon making the large majority of social media messages end-to-end encrypted.

[54] Levy, S. (2016, March 11). Why Are We Fighting the Crypto Wars Again? *Wired.* Retrieved from https://www.wired.com/2016/03/why-are-we-fighting-the-crypto-wars-again/

[55] Such views are not new and borrow from speech act theory to describe how words used in speech by political elites and state security actors shape how security threats are framed and how a response is mobilized. See, for example Balzacq, T. (2005). The Three Faces of Securitization: Political Agency, Audience and Context. *European Journal of International Relations*, *11*(2), 171–201

[56] Gill, L. (2018).

[57] Apple. (2016, February 16). A Message to Our Customers. Retrieved from https://www.apple.com/customer-letter/

[58] U.S. Department of Justice. (2019, October 3). Attorney General Barr Signs Letter to Facebook From US, UK, and Australian Leaders Regarding Use of End-To-End Encryption. Retrieved from https://www.justice.gov/opa/pr/attorney-general-barr-signs-letter-facebook-us-uk-and-australian-leaders-regarding-use-end.

[59] U.S. Department of Justice. (2020, June 23). Statement from Attorney General William P. Barr on Introduction of Lawful Access Bill in Senate. Retrieved from https://www.justice.gov/opa/pr/statement-attorney-general-william-p-barr-introduction-lawful-access-bill-senate.

[60] Riley, T. (2021, March 4). The Cybersecurity 202: FBI renews attack on encryption ahead of another possible attack on the Capitol. *The Washington Post*. Retrieved from https://www.washingtonpost.com/politics/2021/03/04/cybersecurity-202-fbi-renews-attack-encryption-ahead-another-possible-attack-capitol/

[61] Riley, T. (2021, Jan 13). The Cybersecurity 202: extremists flocking to encrypted apps could restart debate over law enforcement access. The Washington Post. Retrieved from https://www.washingtonpost.com/politics/2021/01/13/cybersecurity-202-extremists-flocking-encrypted-apps-could-restart-debate-over-law-enforcement-access/

[62] WhatsApp. (n.d.). The threat of traceability in Brazil and how it erodes privacy. Retrieved from https://faq.whatsapp.com/general/security-and-privacy/the-threat-of-traceability-in-brazil-and-how-it-erodes-privacy/?lang=en

[63] Canadian Association of Chiefs of Police. (2016). Resolution 2016-03, "Reasonable Law to Address the Impact of Encrypted and Password-protected Electronic Devices". Retrieved from https://cacp.ca/resolution.html?asst_id=1197 as cited in Gill, L., Israel, T., and Parsons, C. (2018, May).

[64] International Association of Chiefs of Police. (2015). Data, Privacy, and Public Safety: A Law Enforcement Perspective on the Challenges of Gathering Electronic. IACP Summit Report. Retrieved from https://www.theiacp.org/sites/default/files/2019-05/IACPSummitReportGoingDark_0.pdf as cited in Gill, L., Israel, T., and Parsons, C. (2018, May).

[65] Public Safety Canada. (2017, December 21). Public Report on the Terrorist Threat to Canada: Building A Safe and Resilient Canada. Retrieved from https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/pblc-rprt-trrrst-thrt-cnd-2017/pblc-rprt-trrrst-thrt-cnd-2017-en.pdf.

[66] Andrey, S., Rand, A., Masoodi, M.J. & Tran, S. (2021, May). Private Messaging, Public Harms. Retrieved from https://www.cybersecurepolicy.ca/privatemessaging

[67] Comey, J.B. (2015, July 8). Going Dark: Encryption, Technology, and the Balances Between Public Safety and Privacy. *Federal Bureau of Investigation*. Retrieved from https://www.fbi.gov/news/testimony/going-dark-encryption-technology-and-the-balances-between-public-safety-and-privacy

[68] Wu, T., Chung, J., Yamat, J., & Richman, J. (n.d.). The ethics (or not) of massive government surveillance. Retrieved from https://cs.stanford.edu/people/eroberts/cs181/projects/ethics-of-surveillance/tech_encryptionbackdoors.html

[69] Statt, N. (2016, April 14). Canadian police have had master key to BlackBerry's encryption since 2010. *The Verge*. Retrieved from https://www.theverge.com/2016/4/14/11434926/blackberry-encryption-master-key-broken-canada-rcmp-surveillance

[70] Ibid.

[71] Abelson, H. et al. (2015, July 6).

[72] Palmer, A. (2019, December 10). Facebook rejects AG Barr's request to stop encryption plans for messaging apps. *CNBC*. Retrieved from https://www.cnbc.com/2019/12/10/facebook-rejects-ag-barrs-request-to-stop-messaging-encyrption.html

[73] Holland, B. (2019, October 18). Will Canada weaken encryption with backdoors? *Maclean's*. Retrieved from https://www.macleans.ca/opinion/will-canada-weaken-encryption-with-backdoors/

[74] Marshal, P. (2018, Jan 16). When is a back door not a back door?. *GCN*. Retrieved from https://gcn.com/articles/2018/01/16/fbi-encryption-backdoor.aspx

[75] Riley, D. (2021, April 14). Washington Post: Azimuth, not Cellebrite, hacked San Bernardino Shooter's Phone. Silicon Angle. Retrieved from https://siliconangle.com/2021/04/14/washington-post-azimuth-not-cellebrite-hacked-san-bernardino-shooters-phone/

[76] Newman, L. (2021, January 13). How law enforcement gets around your smartphone's encryption. *Wired*. Retrieved May 6, 2021 from https://www.wired.com/story/smartphone-encryption-law-enforcement-tools/

[77] Ibid.

[78] Koepke, L. Weil, E., Janardan, U., Dada, T., Yu, H. (2020, October). Mass Extraction: The widespread power of U.S. law enforcement to search mobile phones. *Upturn*. Retrieved May 5, 2021 https://www.upturn.org/reports/2020/mass-extraction

[79] Ibid.

[80] Ling, J. (2016, December 22). When Canadian cops need to break into encrypted cellphone, they use this technology. *Vice*. Retrieved from https://www.vice.com/en/article/kzgm4n/when-canadian-cops-need-to-break-into-an-encrypted-cellphone-they-use-this-technology

[81] Levinson, J. (2021, May 24). Police in Oregon are searching cellphones daily and straining civil liberties. *OPB*. Retrieved from https://www.opb.org/article/2021/05/24/police-in-oregon-are-searching-cellphones-daily-and-straining-civil-rights/

[82] On disinformation, see our report: Andrey, S., Rand, A., Masoodi, M.J. & Tran, S. (2021, March).

[83] The Editorial Board. (2021, May 16). UK online harms bill misses the fraud's gateway. *Financial Times*. Retrieved from https://www.ft.com/content/239c33ea-8d41-4e79-ab88-e53bf558a2cf

[84] Lomas, N. (2021, May 12). UK Publishes draft online safety bill. Tech Crunch. Retrieved from https://techcrunch.com/2021/05/12/uk-publishes-draft-online-safety-bill/

[85] Earp. M. (2021, May 25). UK online safety bill raises censorship concerns and questions on future of encryption. *CPJ*. Retrieved from https://cpj.org/2021/05/uk-online-safety-bill-raises-censorship-concerns-and-questions-on-future-of-encryption/

[86] Ibid.

[87] The Centre for Social Justice. (2021, March). Unsafe Children: Driving up our country's response to child sexual abuse and exploitation. Retrieved from https://www.centreforsocialjustice.org.uk/wp-content/uploads/2021/03/CSJJ8804-Unsafe-Children-210325-WEB.pdf

[88] Kelion, L. (2020, December 20). Online harms law to let regulator block apps in UK. *BBC*. Retrieved https://www.bbc.com/news/technology-55302431

[89] United Kingdom Government. (2020, December 15). Online Harms White Paper. Retrieved https://www.gov.uk/government/consultations/online-harms-white-paper/online-harms-white-paper

[90] Instagram. (2021, March 17). Continuing to make Instagram safer for the youngest members of our community. Retrieved from https://about.instagram.com/blog/announcements/continuing-to-make-instagram-safer-for-the-youngest-members-of-our-community

[91] In addition to the effects on encryption, a 'duty of care' approach in Canada may also provoke the analysis of the USMCA and Canada's adherence to Section 230 of the United States Digital Communications Act. For more on this see: Tsai, D. (2020, Oct 30). Online platforms must be liable for third party hate content. Retrieved from https://www.thestar.com/business/opinion/2020/10/30/online-platforms-must-be-made-liable-for-third-party-hate-content.html

[92] Gruber, J. (2021, August 6). Apple's new 'child safety' initiatives, and the slippery slope. DaringFireball. Retrieved from https://daringfireball.net/2021/08/apple_child_safety_initiatives_slippery_slope

[93] Internet Society, (2020, November 19). Breaking encryption myths. Retrieved from https://www.internetsociety.org/resources/doc/2020/breaking-the-myths-on-encryption/

[94] Apple privacy letter. (2021, August 6).

[95] A hash is a term used in the computer sciences realm to describe and refer to a computer function that converts one value into another. In the case of client-side scanning, it can be used to take the numerical value of a photograph, and convert it to a smaller value. The same picture would have the same hash, and only that picture coverts to that hash value. See: Rosenzweig, P. (2020, August 20). The law and policy of Client-side scanning. Lawfare Blog. Retrieved from https://www.lawfareblog.com/law-and-policy-client-side-scanning

[96] Facebook. (2020, January 17). Facebook Letter to the U.S. Senate Committee on the Judiciary. Retrieved from https://www.judiciary.senate.gov/imo/media/doc/Sullivan%20Responses%20to%20QFRs2.pdf

[97] Apple. (2021). Expanded Protections for Children. Retrieved from https://www.apple.com/child-safety/

[98] Internet Society, (2020, November 19). Breaking encryption myths. Retrieved from https://www.internetsociety.org/resources/doc/2020/breaking-the-myths-on-encryption/

[99] Opsahl, K. (2021, August 11). If you build it, they will come: Apple has a opened the backdoor to increased surveillance and censorship around the world. EFF. Retrieved from https://www.eff.org/deeplinks/2021/08/if-you-build-it-they-will-come-apple-has-opened-backdoor-increased-surveillance

[100] Abelson, H. et al. (2015, July 6). Keys under doormats: mandating insecurity by requiring government access to all data and communications. Retrieved from https://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf

[101] Rosenzweig, P. (2020, August 20).

[102] Gill, L. (2018); Gill, L., Israel, T., and Parsons, C. (2018, May).

[103] Ibid.

[104] Parsons, C. & Israel, T. (2015, August 7).

[105] Carey, S. (2019, July 31). The Snoopers' Charter: Everything you need to know about the Investigatory Powers Act. *Computerworld*. Retrieved from https://www.computerworld.com/article/3427019/the-snoopers-charter-everything-you-need-to-know-about-the-investigatory-powers-act.html

[106] United Kingdom, Investigatory Powers Act 2016, c. 25 at s 253(5)(c) Retrieved from https://www.legislation.gov.uk/ukpga/2016/25/section/253/enacted as cited in Gill, L., Israel, T., and Parsons, C. (2018, May).

[107] Aron, J. (2016, March 1). New UK Snooper's charter still gives state wide hacking powers. *New Scientist*. Retrieved from https://www.newscientist.com/article/2079252-new-uk-snoopers-charter-still-gives-state-wide-hacking-powers/

[108] Hern, A. (2017, March 29). UK government can force encryption removal, but fears losing, experts say. *The Guardian*. Retrieved from https://www.theguardian.com/technology/2017/mar/29/uk-government-encryption-whatsapp-investigatory-powers-act

[109] Revell, T. (2017, June 5). Theresa May's repeated calls to ban encryption still won't work. *New Scientist*. Retrieved from https://www.newscientist.com/article/2133644-theresa-mays-repeated-calls-to-ban-encryption-still-wont-work/#:~:text=Speaking%20after%20the%20previous%20terrorist,no%20hiding%20place%20for%20terrorists%E2%80%9D.

[110] Price, R. (2017, August 1). UK home secretary Amber Rudd says 'real people' don't need end-to-end encryption. *Business Insider*. Retrieved from https://www.businessinsider.com/home-secretary-amber-rudd-real-people-dont-need-end-to-end-encryption-terrorists-2017-8

[111] Seo, B. (2019, February 25). Five Eyes fears rise over Aussie encryption laws. *Financial Review*. Retrieved from https://www.afr.com/technology/five-eyes-fears-rise-over-aussie-encryption-laws-20190221-h1bj6f#:~:text=Australia%20is%20facing%20increased%20criticism,citizens%E2%80%99%20security%20and%20privacy%20rights.

[112] Hardy, K. (2020). Australia's encryption laws: practical need or political strategy? *Internet Policy Review, 9*(3). https://doi.org/10.14763/2020.3.1493

[113] Blenkin, M. (2019, February 8). Australia using new decryption powers even before planned review. *Phys.org*. Retrieved from https://phys.org/news/2019-02-australia-decryption-powers.html

[114] Canales, S.B. (2020, August 7). Australia's Controversial Encrypted Messaging Laws, Explained. *Pedestrian group*. Retrieved from https://www.gizmodo.com.au/2020/08/assistance-and-access-law-encrypted-messaging-explained/

[115] Bocetta, S. (2019, Feb 14). Australia's new anti-encryption law is unprecedented and undermines global privacy. *Foundation for Economic Education*. Retrieved from https://fee.org/articles/australia-s-unprecedented-encryption-law-is-a-threat-to-global-privacy/

[116] Barbaschow, A. (2020, July 27). Atlassian says encryption-busting law has damaged Australia's tech reputation. *Zdnet*. Retrieved from https://www.zdnet.com/article/atlassian-says-encryption-busting-law-has-damaged-australias-tech-reputation/

[117] United States Department of Justice. (2019, October 4). Open letter to Facebook. Retrieved from https://www.afr.com/technology/five-eyes-fears-rise-over-aussie-encryption-laws-20190221-h1bj6f#:~:text=Australia%20is%20facing%20increased%20criticism,citizens%E2%80%99%20security%20and%20privacy%20rights.

[118] Paul, K. (2019, December 10). U.S. senators threaten Facebook, Apple with encryption regulation. *Reuters*. Retrieved from https://www.reuters.com/article/us-usa-encryption-facebook-idUSKBN1YE2CK

[119] These protections are afforded in the U.S. under Section 230 protections under the *Communications Decency Act* (DCA)

[120] EFF. (n.d.). Deeplinks Blog. Retrieved from https://www.eff.org/deeplinks/2020/07/new-earn-it-bill-still-threatens-encryption-and-free-speechhttps

[121] Newton, C. (2020, March 12). A sneaky attempt to end encryption is working its way through Congress. *The Verge*. Retrieved from www.theverge.com/interface/2020/3/12/21174815/earn-it-act-encryption-killer-lindsay-graham-match-group

[122] Cathcart, W. [wcathcart]. (2020, March 11). Will: This morning the U.S. Senate Judiciary Committee held a hearing on the 'EARN IT' Act. While not directly mandating a backdoor, as written, this act would form a commission that could have the power to require services like @WhatsApp to stop offering end-to-end encryption. [Tweet]. Retrieved from https://twitter.com/wcathcart/status/1237850609170010113

[123] Pfefferkorn, R. (2020, January 30). The EARN IT Act: How to Ban End-to-End Encryption Without Actually Banning It. *Stanford Law School: The Center for Internet and Society*. Retrieved from https://cyberlaw.stanford.edu/blog/2020/01/earn-it-act-how-ban-end-end-encryption-without-actually-banning-it

[124] Anderson, T., Berengaut, A., Garland J., & Goodwin, C. (2020, July 6). Lawful Access to Encrypted Data Act Introduced. *Inside Privacy.* Retrieved from https://www.insideprivacy.com/surveillance-law-enforcement-access/lawful-access-to-encrypted-data-act-introduced/

[125] Additionally, the change in tone is also marked by new moves under Biden's administration that appear to at least recognize the need for strong encryption. Following the Colonial pipeline cyberattack for instance, an executive order was introduced mandating government agencies to encrypt data in transit and at rest, though fall short from mandating the use, or even mention of, end-to-end encryption. Of course, this does not mean that the encryption debate is over. See, for example: The White House. (2021, May 12). Executive Order on Improving the Nation's Cybersecurity. Retrieved from https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

[126] https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_1381

[127] Lomas, N. (2020, December 14). EU Council wants secure encryption and lawful data access. *Tech Crunch.* Retrieved from https://techcrunch.com/2020/12/14/eu-council-wants-secure-encryption-and-lawful-data-access/

[128] Gill, L. (2018).

[129] Bill C-30, Protecting Children from Internet Predators Act, 1st Sess, 41st Parl, 1st Reading (14 February 2012) Retrieved from https://parl.ca/DocumentViewer/en/41-1/bill/C-30/first-reading/page-4

[130] Library of Congress. (n.d.). About this Collection. Retrieved from https://www.loc.gov/law/help/encrypted-communications/canada.php

[131] Gill, L. (2018).

[132] Pearson, J. (2016, April 14) Canada desperately needs to have a public debate about encryption. *Motherboard.* Retrieved from https://www.vice.com/en/article/z43mny/canada-desperately-needs-to-have-a-public-debate-about-encryption

[133] Public Safety Canada, ATIP A-2018-00078, page 330. Available at: https://citizenlab.ca/wp-content/uploads/2019/08/A-2018-00078.pdf. Also, Canada's public support of strong encryption is contrasted with Canada's Communications Security Establishment in deliberately and surreptitiously introducing known vulnerable encryption standards known as DUAL EC DRBG. See: Perlroth, N., Larson, J. and Shane. S. (2013 September 5). NSA Able to Foil Basic Safeguards of Privacy on Web. *The New York Times*. Retrieved from www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html

[134] Department of Justice, United States of America. (2020, October 11). International Statement: End-to-End Encryption and Public Safety. Retrieved from https://www.justice.gov/opa/pr/international-statement-end-end-encryption-and-public-safety

[135] United Kingdom's Attorney General's Office and Home Affairs. (2019). Joint meeting of Five Country Ministerial and quintet of Attorneys-General: communiqué, London 2019. Available at: https://www.homeaffairs.gov.au/news-subsite/Pages/2019-Jul/joint%20meeting%20of%20fcm%20and%20quintet%20of%20attorneys-general.aspx

[136] Holland, B. (2019, October 18). Will Canada weaken encryption with backdoors? *Maclean's*. Retrieved from https://www.macleans.ca/opinion/will-canada-weaken-encryption-with-backdoors/

[137] Riley, T. (2021, March 4). The Cybersecurity 202: FBI renews attach on encryption ahead of another possible attack on the Capitol. *The Washington Post.* Retrieved from https://www.washingtonpost.com/politics/2021/03/04/cybersecurity-202-fbi-renews-attack-encryption-ahead-another-possible-attack-capitol/

[138] Parson, C. (2019).

[139] Facebook. (2020, January 17).

[140] Gursky, J and Wooley, S. (2021, June). Countering disinformation and protecting democratic communication on encrypted messaging applications. *Brookings*. Retrieved from https://www.brookings.edu/wp-content/uploads/2021/06/FP_20210611_encryption_gursky_woolley.pdf

[141] Ferguson, A G. (2017). *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement.* New York, NY: NYU Press; Brayne, S. (2017). Big Data Surveillance: The Case of Policing. *American Sociological Review 82*(5):977- 1008

[142] Lyon, D. & Murakami-Wood, D. (2021). *Big Data Surveillance and Security Intelligence: The Canadian Case*. UBC Press.

[143] Parson, C. (2019, August 21).

[144] Government of Canada. (2010, November). A matter of trust: integrating privacy and public safety in the 21st century. *Office of the Privacy Commissioner of Canada*. Retrieved from https://www.priv.gc.ca/en/privacy-topics/surveillance/police-and-public-safety/gd_sec_201011/

[145] Internet Society. (2020, November 19). Breaking Encryption Myths. Retrieved from https://www.internetsociety.org/resources/doc/2020/breaking-the-myths-on-encryption/