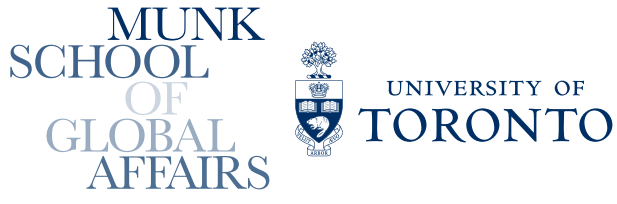
SHINING A LIGHT ON THE ENCRYPTION DEBATE: A CANADIAN FIELD GUIDE

JOINT RESEARCH PUBLICATION, MAY 2018

BY THE CITIZEN LAB AND THE CANADIAN INTERNET POLICY & PUBLIC INTEREST CLINIC

LEX GILL
TAMIR ISRAEL
CHRISTOPHER PARSONS



This page has intentionally been left blank.

COPYRIGHT

Electronic version first published by Citizen Lab and the Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic in 2018. This work can be accessed through https://citizenlab.ca and https://cippic.ca.

Citizen Lab and the Canadian Internet Policy & Public Interest Clinic (CIPPIC) are collaborative research partners. Together, the two groups engage in research that investigates the intersection of digital technologies, law, and human rights. This report is a joint research publication.

Document Version: 1.1 (23 May 2018 — minor revisions)

CITIZEN LAB, MUNK SCHOOL OF GLOBAL AFFAIRS

The Citizen Lab is an interdisciplinary laboratory based at the Munk School of Global Affairs, University of Toronto, focusing on research, development, and high-level strategic policy and legal engagement at the intersection of information and communication technologies, human rights, and global security.

Citizen Lab uses a "mixed methods" approach to research combining practices from political science, law, computer science, and area studies. Its research includes investigating digital espionage against civil society, documenting Internet filtering and other technologies and practices that impact freedom of expression online, analyzing privacy, security, and information controls of popular applications, and examining transparency and accountability mechanisms relevant to the relationship between corporations and state agencies regarding personal data and other surveillance activities.

CANADIAN INTERNET POLICY & PUBLIC INTEREST CLINIC

The Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic (CIPPIC) is a legal clinic based at the Centre for Law, Technology & Society (CLTS) at the University of Ottawa, Faculty of Law. Its core mandate is to ensure that the public interest is accounted for in decision-making on issues that arise at the intersection of law and technology. It has the additional mandate of providing legal assistance to under-represented organizations and individuals on law and technology issues, as well as a teaching mandate focused on providing law students practical training in a law and technology setting.

CIPPIC adopts a multi-lateral approach to advancing its mandate, which involves placing objective and comprehensive research and argumentation before key political, regulatory and legal decision makers. It seeks to ensure a holistic approach to its analysis, which integrates the socio-political, technical and legal dimensions of a particular policy problem. This regularly includes providing expert testimony before parliamentary committees, participating in quasi-judicial regulatory proceedings, strategic intervention at all levels of court and involvement in domestic and international Internet governance fora.

ABOUT THE AUTHORS

Lex Gill is a Citizen Lab Research Fellow. She has also served as the National Security Program Advocate to the Canadian Civil Liberties Association, as a CIPPIC Google Policy Fellow and as a researcher to the Berkman Klein Center for Internet & Society at Harvard University. She holds a B.C.L./LL.B. from McGill University's Faculty of Law.

Tamir Israel is Staff Lawyer at the Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic at the University of Ottawa, Faculty of Law. He leads CIPPIC's privacy, net neutrality, electronic surveillance and telecommunications regulation activities and conducts research and advocacy on a range of other digital rights-related topics.

Christopher Parsons is currently a Research Associate at the Citizen Lab, in the Munk School of Global Affairs with the University of Toronto as well as the Managing Director of the Telecom Transparency Project at the Citizen Lab. He received his Bachelor's and Master's degrees from the University of Guelph, and his Ph.D from the University of Victoria.

ACKNOWLEDGEMENTS

The authors would like to extend their deepest gratitude to a number of individuals who have provided support and feedback in the production of this report, including (in alphabetical order) Bram Abramson, Nate Cardozo, Masashi Crete-Nishihata, Ron Deibert, Mickael E.B., Andrew Hilts, Jeffrey Knockel, Adam Molnar, Christopher Prince, Tina Salameh, Amie Stepanovich, and Mari Jing Zhou. Any errors remain the fault of the authors alone.

We are also grateful to the many individuals and organizations who gave us the opportunity to share early versions of this work, including Lisa Austin at the Faculty of Law (University of Toronto); Vanessa Rhinesmith and David Eaves at digital HKS (Harvard Kennedy School); Ian Goldberg and Erinn Atwater at the Cryptography, Security, and Privacy (CrySP) Research Group (University of Waterloo); Florian Martin-Bariteau at the Centre for Law, Technology and Society (University of Ottawa); and the Citizen Lab Summer Institute (Munk School of Global Affairs, University of Toronto).

Finally, the authors would like to offer our sincere thanks to the John D. and Catherine T. MacArthur Foundation and the Ford Foundation, whose generous funding made this report possible.

CORRECTIONS AND QUESTIONS

Please send all questions and corrections to the authors directly, at:

lex@citizenlab.ca
christopher@christopher-parsons.com
tisrael@cippic.ca

SUGGESTED CITATION

Lex Gill, Tamir Israel, and Christopher Parsons (May 2018), “Shining a Light on the Encryption Debate: A Canadian Field Guide,” Citizen Lab and the Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic.

TABLE OF ACRONYMS

AANDC	Aboriginal Affairs and Northern Development Canada
ACLU	American Civil Liberties Union (US)
AES	Advanced Encryption Standard
BCCLA	British Columbia Civil Liberties Association
CACP	Canadian Association of Chiefs of Police
CALEA	Communications Assistance for Law Enforcement Act (US)
CBSA	Canada Border Services Agency
CCTV	Closed-Circuit Television
CIA	Central Intelligence Agency (US)
CIPPIC	Canadian Internet Policy and Public Interest Clinic
CoE	Council of Europe
CSE(C)	Communications Security Establishment (Canada)
CSIS	Canadian Security Intelligence Service
DES	Data Encryption Standard
ECL	Export Control List
EFF	Electronic Frontier Foundation (US)
ENISA	European Network and Information Security Agency (EU)
FBI	Federal Bureau of Investigation (US)
FELEG	Five Eyes Law Enforcement Group
FFU	Free File Upload
FINRA	Financial Industry Regulatory Authority (US)
FISC	Foreign Intelligence Surveillance Court (US)
FOI	Freedom of Information
G8	Group of Eight
G20	Group of Twenty
GCHQ	Government Communications Headquarters (UK)
GPG	GNU Privacy Guard
GSM	Global System for Mobile Communications
GSN	General Software Note (Wassenaar Arrangement)
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol (Secure)
IACP	International Association of Chiefs of Police
ICCPR	International Covenant on Civil and Political Rights
IMSI	International Mobile Subscriber Identifier
IP	Internet Protocol

IPA	Investigatory Powers Act (UK)
ISP	Internet Service Provider
ISO	International Organization for Standardization
LEAF	Law Enforcement Access Field (Clipper Chip)
MI5	Military Intelligence, Section 5 (UK)
NATO	North Atlantic Treaty Organization
NIST	National Institute of Standards and Technology (US)
NSA	National Security Agency (US)
OECD	Organisation for Economic Co-operation and Development
OSINT	Open Source Intelligence
OTR	Off-the-Record
PGP	Pretty Good Privacy
RCMP	Royal Canadian Mounted Police
RIM	Research in Motion
RSA	Rivest–Shamir–Adleman (Cryptosystem *or* Company)
SGES	Solicitor General's Enforcement Standards
SIM	Subscriber Identity Module
SSL	Secure Sockets Layer
TSL	Transport Layer Security
TSP	Telecommunications Service Provider
UDHR	Universal Declaration of Human Rights
UN	United Nations
UNESCO	United Nations Educational, Scientific and Cultural Organisation
URL	Uniform Resource Locator
VPN	Virtual Private Network
W3C	World Wide Web Consortium

TABLE OF CONTENTS

FIGURES

INFORMATION BOXES

EXECUTIVE SUMMARY AND INTRODUCTION

Access to strong encryption technology is integral to the defense of human rights in the twenty-first century. This technology is also essential for securing digital transactions, ensuring public safety, and protecting national security interests. Yet many state agencies have continued to argue that encryption poses an unacceptable barrier to their investigative and intelligence-gathering activities. In response, some governments have called for limits on the public availability and use of secure, uncompromised encryption technology. This report examines the parameters of this debate, paying particular attention to the Canadian context. It provides critical insight and analysis for policymakers, legal professionals, academics, journalists, and advocates who are trying to navigate the complex implications of this technology. The report proceeds in five sections.

Proposed policy responses to the challenges raised by encryption are sometimes rooted in technical misunderstandings or overconfident rhetoric rather than an accurate view of the technology. **Section One** provides a brief primer on key technical principles and concepts associated with encryption in the service of improving policy outcomes and enhancing technical literacy. In particular, we review the distinction between encryption at rest and in transit, the difference between symmetric and asymmetric encryption systems, the issue of end-to-end encryption, and the concept of forward secrecy. We also identify some of the limits of encryption in restricting the investigative or intelligence-gathering objectives of the state, including in particular the relationship between encryption and metadata.

Section Two explains how access to strong, uncompromised encryption technology serves critical public interest objectives. Encryption is intimately connected to the constitutional protections guaranteed by the Canadian *Charter of Rights and Freedoms* as well as those rights enshrined in international human rights law. In particular, encryption enables the right to privacy, the right to freedom of expression, and related rights to freedom of opinion and belief. In an era where signals intelligence agencies operate with minimal restrictions on their foreign facing activities, encryption remains one of the few practical limits on mass surveillance. Encryption also helps to guarantee privacy in our personal lives, shielding individuals from abusive partners, exploitative employers, and online harassment. The mere awareness of mass surveillance exerts a significant chilling effect on freedom of expression. Vulnerable and marginalized groups are both disproportionately subject to state scrutiny, and may be particularly vulnerable to these chilling effects. Democracies pay a particularly high price when minority voices and dissenting views are pressured to self-censor or refrain from participating in public life. The same is true when human rights activists, journalists, lawyers, and others whose work demands the ability to call attention to injustice, often at some personal risk, are deterred from leveraging digital networks in pursuit of their activities. Unrestricted public access to reliable encryption technology can help to shield individuals from these threats. Efforts to undermine the security of encryption in order to facilitate state access, by contrast, are likely to magnify these risks. Uncompromised encryption systems can thus foster the security necessary for meaningful inclusion, democratic engagement, and equal access in the digital sphere.

The nexus between strong encryption and free expression is particularly strong. For example, encryption is an integral component of anonymity and censorship circumvention tools. Encryption also limits the effectiveness of automated content filtering systems used by states to control access to news, political speech, cultural expression, health information, and art. Similarly, a free press depends on the ability to receive documents securely and to communicate anonymously with sources. In many parts of the world, the physical safety of individuals relies on access to secure communications technology. This may be particularly true for political dissidents, human rights workers, and journalists. In authoritarian countries and conflict zones, access to effective encryption tools can sometimes mark the difference between safety and imprisonment.

Access to strong, uncompromised encryption technology is also critical to the economy. In a technological environment marked by high financial stakes, deep interdependence, and extraordinary complexity, ensuring digital security is of critical importance and extremely difficult. Encryption helps to ensure the security of financial transactions and preserves public trust in the digital marketplace. From sensitive financial information to dating sites to health records, technology companies hold the key to the most intimate details of our lives. The cost of a security breach, theft, or loss of customer or corporate data can have devastating impacts for both private sector interests and individuals' rights. Weakening the very systems that protect against these threats in order to facilitate government access would constitute irresponsible policymaking. Access to strong encryption encourages consumer confidence that the technology they use is safe, and that the companies they entrust with their data will not be improperly deputized by the state.

Finally, encryption is vital to protecting public safety and national security. Public access to effective digital security technology prevents countless forms of digitally mediated crime: from identity fraud, theft, and extortion to larger scale intrusions of networks and infrastructure. Encryption is also necessary for the work of law enforcement and intelligence agencies, which must be able to carry out their activities securely and, at times, anonymously. Effective encryption maintains the confidentiality of undercover investigations, preserves state secrets, and protects the sensitive work of judges, civil servants, and diplomats alike.

Section Three explores the history of encryption policy across four somewhat distinct eras, with a focus on Canada to the extent the Canadian government played an active role in addressing encryption. The first era is characterized by the efforts of intelligence agencies such as the United States National Security Agency (NSA) to limit the public availability of secure encryption technology. These agencies applied pressure covertly in the development of cryptographic standards and exerted direct influence within the technical community. Export controls were also used to prohibit and limit the dissemination of strong encryption software, often through restrictions on key length. If emerging technology firms hoped to operate in a global marketplace, these controls deterred them from designing their tools securely.

In the second era of the 1990s, encryption emerged as a vital tool for securing electronic trust on the emerging web. Traditional mechanisms relied upon by the state to limit the spread of encryption technology, including export controls and informal pressure, became less effective. Law enforcement began to raise alarms over the potential for encryption to limit the efficiency of investigations. Cryptographic policy became a hotly contested issue, to the point that the debates during this era are often referred to as the "Crypto Wars." While acknowledging that improved digital security provided benefits to businesses and consumers, governments also insisted on the ability to access these new electronic records. They demanded that technology companies insert "backdoor" access to their software or retain decryption keys in escrow to facilitate state access. These efforts crystallized in an American proposal called the "Clipper Chip." This proposal, and other proposals like it, were ultimately defeated following sustained opposition from civil liberties groups (which argued the proposed technology threatened human rights) and the technical community (which argued that the proposal posed an unacceptable risk to security). In the third era—between 2000 and 2010—the development and proliferation of strong encryption technology in Canada, the United States, and Europe progressed relatively unimpeded. As the Internet matured, law enforcement and intelligence agencies developed a complex array of new legal powers and investigative techniques—but encryption did not play a prominent role on the public agenda.

The fourth era encompasses from 2011 to the present day. Over the last decade, calls to compromise, weaken, and restrict access to encryption technology have steadily reemerged. This era has been characterized by the claim that encryption is once again responsible for a growing gap between the data that state agencies are lawfully authorized to obtain and their practical ability to access it. This narrative, engineered largely by the U.S. Federal Bureau of Investigations (FBI), has adopted the colloquial shorthand "going dark" as an organizing theme. In response, various agencies and high ranking officials in Canada, the United States, the United Kingdom, and Australia have demanded limits on encryption with an increasing sense of urgency. In 2016, the issue of encryption was raised as part of the Canadian government's far-reaching national security consultation process. In several other countries, including Australia, proposals explicitly addressing the encryption debate have returned to the legislative agenda. While these proposals have generally failed to engage with the important public interest objectives served by public access to secure encryption, they set the backdrop for the current debate.

Section Four reviews the broad spectrum of legal and policy responses to government agencies' perceived encryption "problem," including historical examples, international case studies, and present-day proposals. The section provides an overview of factors which may help to evaluate these measures in context. In particular, it emphasizes questions related to (1) whether the proposed measure is truly targeted, and avoids collateral or systemic impacts on uninvolved parties; (2) whether there is an element of conscription or compelled participation which raises an issue of self-incrimination or unfairly impacts the interests of a third party; (3) whether, in considering all the factors, the response remains both truly necessary and truly proportionate. The analysis of policy measures in this sections proceeds in three categories. The first category includes measures designed to limit the broad public availability of effective encryption tools. The second category reviews measures that are directed at intermediaries and service providers. The third category focuses on efforts that target specific encrypted devices, accounts, or individuals.

In the **first category,** we explore measures principally designed to limit the public availability of secure and uncompromised encryption. In the international context, there are examples where states have attempted to achieve this objective through the outright criminalization of encryption technology. Efforts to censor access to popular encryption tools and messaging applications also continue to be relatively common internationally, despite widespread public opposition and legal

resistance. These measures are rarely successful in meeting their stated objectives, seriously jeopardize human rights, and regularly entail far-reaching unintended consequences. Historically, limits on key length and regulations that prescribe "permissible" algorithms have played a similar role. The report also notes that there are significant parallels between those historical examples and modern-day calls to ban the use of end-to-end encryption in countries like the United Kingdom and Australia. In this section we also canvass less direct measures, such as export controls, which have both prevented the availability of strong encryption in other jurisdictions and deterred its development domestically. Finally, some government agencies have attempted to undermine the public availability and use of secure encryption by covertly subverting encryption standards and protocols. When vulnerabilities are secretly incorporated at the development stage, they can later be exploited to access data secured using these deficient systems.

The **second category** includes measures which target intermediaries, service providers, and manufacturers. The most frequently discussed proposals are those colloquially referred to as "exceptional access" models. These measures generally propose that intermediaries and service providers design their software in a manner that facilitates access by law enforcement and intelligence agencies but excludes all other third parties. Despite various proposals for models that purport to achieve this objective, the technical consensus remains that these systems introduce an unacceptable degree of risk and complexity, create single points of failure, and are fundamentally unworkable in practice. The same weaknesses introduced to facilitate state access inherently risk exploitation by other adversarial parties, including criminals and foreign governments alike. These measures therefore ultimately implicate the same public interest and human rights concerns as the first category. When applied to global platforms, "exceptional access" proposals create even more profound possibilities for abuse in authoritarian countries and those with problematic human rights records. The second category also examines the issue of voluntary private sector efforts to undermine user security by facilitating state access—compliance generally achieved through the use of political, economic, or co-regulatory pressure. The report then reviews the issue of how various legal instruments can be used to create mandatory decryption requirements for telecommunications service providers in Canada. These types of measures do not obligate affected intermediary to use one type of encryption mechanism over another. However, they can operate as a deterrence against the standardization of more secure encryption where this would disrupt the status quo by removing an intermediary's ability to decrypt communications. Finally, this section of the report briefly explores other forms of mandatory participation in law enforcement investigations by third party service providers, including provisions for production orders and assistance orders in the Canadian *Criminal Code*. In aggregate, these types of measures can dramatically weaken consumer trust, undermine the reputation of service providers, stifle technical innovation, and limit economic competitiveness.

In the **third category,** the report examines legal measures that enlist targeted individuals in the compelled decryption of their data, devices, or accounts. In most cases, these measures involve forcing the subject of an order to surrender an encryption key or password. Courts in both Canada and the United States have generally found that such measures—to the extent that they concern suspects or accused persons in criminal investigations—engage the individual's constitutionally protected rights to silence and against self-incrimination. This issue of compelled password disclosure is further explored in the context of "search incident to arrest," and where individuals are subject to the search of electronic devices at the Canadian border. In some jurisdictions, courts have drawn a distinction between alphanumeric passwords and biometric identifiers (e.g., fingerprints or facial scans) for the purpose of evaluating the accused person's rights against self incrimination. The report argues that these distinctions take an inappropriately formalistic view of the safeguards provided for in the Canadian *Charter* and fail to recognize the intimate connection between the rights to silence, against self-incrimination, and to privacy. A contextual and purposive approach instead requires that courts focus on the broader issue of compelled participation rather than on the particular technological form that participation takes. The report also highlights that the fact that an individual has made use of encryption software should not contribute to a finding of guilt. Such presumptions are neither contextually appropriate nor likely to withstand constitutional scrutiny, despite some courts having drawn prejudicial inferences from such use. Finally, we provide a brief overview of other forms of mandatory key disclosure that may also be problematic, but engage a different constitutional context, including civil orders for the preservation of evidence ("Anton Piller" orders) and bail conditions.

Section Five examines the necessity of proposed responses to the encryption "problem." First, it questions the extent to which encryption actually poses an insurmountable barrier for law enforcement and intelligence agencies. In practice, encryption rarely presents an absolute guarantee of security. State agencies already rely on an array of legal powers and investigative techniques to bypass encryption without requiring new powers or legal capabilities. Investigators will often be able to take advantage of weaknesses in the design or implementation of an encryption system in order to secure evidence or intelligence. They may also be able to exploit endpoint devices used by a target or their communication partners—in many cases, the weakest

link in a security system will be the humans who use it. These investigative techniques will undoubtedly involve additional resources, time, or complexity in some circumstances. However, these costs are better characterized as sources of investigative *friction*, rather than investigative impossibility. The practical barriers posed by encryption may also provide a healthy incentive for state agents to ensure that intrusive activities are tailored, targeted, and directed towards the most pressing and serious government objectives. It remains true that some encryption mechanisms will require more sophisticated strategies that are likely to remain within the exclusive purview of intelligence agencies, at least for the foreseeable future. However, these agencies are increasingly empowered to provide technical assistance to law enforcement and, moreover, local police departments are themselves beginning to develop the internal capacity to mitigate the challenges posed by encryption by developing specialized technical units and engaging in relationship-building with third party vendors. It should be noted that many of these investigative methods are highly intrusive and independently problematic, and thus raise their own distinct human rights and civil liberties concerns. Yet these techniques and measures are undeniably part of many law enforcement and intelligence agencies' current toolsets. Ignoring these capabilities while calling for more direct laws to regulate encryption therefore fails to take a contextual view of the problems that strong and uncompromised encryption technologies may pose for government agencies.

Though encryption will inevitably shield some data from state agencies, law enforcement and intelligence agencies generally do not lack the information necessary to do their work. Far from "going dark," more information about individuals' private lives is available today than at any previous moment in human history. Business incentives continue to favour the creation and aggregation of data in formats which remain accessible to service providers, state agents, and other third parties in unencrypted formats. Data is also collected from a wider range of sources than ever before—networked refrigerators, thermometers, fitness trackers, televisions, cars, and pacemakers all create records of activities that were previously ephemeral or nonexistent. Data is further available from cloud based storage services, metadata associated with file downloads or viewed videos, and open source intelligence sources such as social media. Finally, open source intelligence gathering is becoming a growing source of electronic evidence and intelligence. In all of these cases, information may be accessible in unencrypted formats once government agencies secure the appropriate judicial approval to obtain it. Canadian law enforcement and intelligence agencies have the legal tools and, increasingly, the technical capabilities to fully exploit these and other data sets to achieve their objectives.

A holistic and contextual analysis of the encryption debate makes clear that the investigative and intelligence costs imposed by unrestricted public access to strong encryption technology are often overstated. At the same time, the risks associated with government proposals to compromise encryption in order to ensure greater ease of access for state agencies are often grossly understated. When weighed against the profound costs to human rights, the economy, consumer trust, public safety, and national security, such measures will rarely—if ever—be proportionate and almost always constitute an irresponsible approach to encryption policy. In light of this, rather than finding ways to undermine encryption, the Government of Canada should make efforts to encourage the development and adoption of strong and uncompromised technology.

PART 1: CRYPTOGRAPHY 101: WHAT IS ENCRYPTION?

In this report, we have foregrounded a basic explanation of encryption technology because certain recurring policy responses to encryption—while often politically attractive or superficially persuasive—are untenable in the face of technological reality. Inaccurate beliefs or inadequate knowledge about how encryption works can be a major barrier to meaningful user security.[1] It can also be difficult for legislators and policymakers to understand the full implications of their decisions without accurate mental models or a working knowledge of basic technical principles. This section therefore explains some core terms and concepts before advancing to a broader discussion of the legal and policy landscape regarding encryption. Fundamentally, it is meant to provide a high-level technical overview in order to assist academics, legal professionals, judges, journalists, and policymakers better understand both the technology and its policy implications.[2]

A. BASIC TERMS & CONCEPTS

Cryptography is the study and application of techniques, methods, principles, and systems to protect information from adversaries.[3] *Encryption* refers to the application of cryptographic algorithms (generally called a *cipher*) to transform data (*plaintext*) using a random character string (a *key*) into an incomprehensible form (*ciphertext*). *Decryption*, by contrast, is the process of using a key to transform ciphertext back into plaintext, a readable form. Figure 1 presents an example of what ciphertext can look like:

```
hQIMA6RJHrIehQHrARAAmk6+p3x6LGGjIuabw//uWdWCll6x1bPmleeYzJ9Dpbfv
JupwylT0UtffM4Dud4xbyAk3XbudXqaayRlPhf0k+yrUlpehmdp+ArrgSo75SfBy
ShUseMWk+gMvdj0pDoQ7DD2uYIKYtRibUTAeNVb8415sOHClZdMc9gtw5X5UUvpP
xFvtkzd2PnPO8AgRnbkCizabNjbho/eaItuZ2dEQ80NFIakhKtDCobiBSxrXPPOo
75cn3Wyqxo2C1w/t03zwcP4rve3SbkFiqP8vrPOoT+p538wR1bgR+ClQqx2fqaY0
aKQk7rL7qzqLS0k9Loicflfm2czdNZAd+X6jgDVihobA8EJaF9XtQ4qRHnAXHMVX
PXgGqq2MGh0QBidUDCAEztj/P4Gngw9004+Yx/F61wGOcyAAe+QmlMtKVw3wmc6u
lcJ4Om7+NJMoEkkBjk2Bn0GNVZqNuR3vDjzpW8fZMX5gVZfiWzldhlKCn995TOuF
m1CMRCLne/LcSBK2hHwLfR3JmJ9OEbmNtCjV9a99Xa9BS9aXb1tBfGWGNvsgVsMn
3vDv5OUZ3q5e0nQ8dfbaDkazLaHh+CGk1hDwo//W9GwIaYSk6J0B5rsCRYqaCMUq
```

Figure 1: Sample Ciphertext

Encryption preserves the confidentiality of information: without the correct key, the ciphertext is illegible to third parties. Cryptography can also be used to authenticate the identity of the sender (i.e., to verify that the sender is who she says she is) or to confirm the integrity of a document, file, or message (i.e. to confirm the contents of a sealed or signed file have not been modified in transit). However, this report primarily focuses on the use of encryption as a confidentiality mechanism.[4] The process of encryption and decryption is often facilitated by a program that relies on a user-established *password* or *passphrase*.

A third party can attempt to decrypt the ciphertext without knowing the key in advance. For example, a *brute force* attack involves systematically guessing possible numeric or alphanumeric combinations exhaustively until the correct key is found (this

---

[1] Ruba Abu-Salma et. al. (2017), "Obstacles to the Adoption of Secure Communication Tools," IEEE Computer Security <https://www.ieee-security.org/TC/SP2017/papers/84.pdf> at 14:

> "The key takeaway from mental models research is that non-experts do not understand abstract security properties. They can only understand why a property matters in the context of a specific threat model that matters to them."

See also: Alma Whitten and J. D. Tygar (1999), "Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0," at USENIX Security Symposium <https://people.eecs.berkeley.edu/~tygar/papers/Why_Johnny_Cant_Encrypt/USENIX.pdf>.

2 For individuals seeking a resource to improve their personal digital security practices, see Security Planner (2017), The Citizen Lab <https://securityplanner.org>.

[3] See OECD Council Recommendation Concerning Guidelines for Cryptography Policy (1997), C(97)62/FINAL, adopted 27 March, 1997 <https://www.oecd.org/sti/ieconomy/guidelinesforcryptographypolicy.htm>, Annex: "Guidelines for Cryptography Policy."

> "Cryptography means the discipline which embodies principles, means, and methods for the transformation of data in order to hide its information content, establish its authenticity, prevent its undetected modification, prevent its repudiation, and/or prevent its unauthorised use."

4 For a fuller plain language explanation of the informational properties that encryption can support (including confidentiality, privacy, authenticity, availability, integrity, and anonymity), see e.g. Wolfgang Schulz & Joris van Hoboken (2016), "Human Rights and Encryption," UNESCO Series on Internet Freedom <http://unesdoc.unesco.org/images/0024/002465/246527E.pdf>, Section 2.

is sometimes called *exhaustive search*).[5] Similarly, *cryptanalysis* involves the use of mathematical techniques to identify errors, weaknesses, or patterns in an encryption system that would permit a key to be "guessed" or determined at a rate faster than by brute force alone.[6] Other attacks can target the implementation of a cryptographic system—for example by trying to obtain a target's key or password directly, or by accessing the plaintext after the target has decrypted it herself.

Properly implemented modern cryptographic systems can keep information secure even from governments and other powerful adversaries. This is because it is extremely computationally challenging to "guess" the correct key.[7] For example, the number of possible keys for a given string of ciphertext encrypted using the algorithm AES-128 is so large that it would take powerful supercomputers millions of billions of years and immense amounts of electricity to guess the correct key by exhaustive search.[8] For this reason, efforts to bypass encryption rarely involve brute force alone. Rather, adversaries target weaknesses in the design or implementation of an encryption system, the physical computers that are involved in implementing it, or the humans who use it. Such attacks frequently focus on obtaining direct access to the secret encryption key or associated password used by a target.[9]

To protect the key used in the encryption process, encryption tools will derive the secret key from a secret value known only to an individual user, or subject to the exclusive control of that user. That value is normally a string of characters chosen by the user in the form of a password, passphrase, or numeric code.[10] This process involves taking the user-provided value, combining it with another random character string (referred to as a "salt"), and then using an algorithm to generate the cryptographic key.[11] If the cryptographic system has been properly implemented, the secret key will be impossible to derive without the value provided by the individual user.[12] This means that for a device like a mobile phone, there is generally a single encryption key that does not change, as well as at least one user-determined PIN or password that "wraps" the encryption key (i.e., the PIN or password encrypts the key, which in turn encrypts the device). Some mobile devices also add an additional layer by using a biometric identifier (like a fingerprint or facial recognition scan) that releases a key once a successful biometric match occurs. That key is then used to unwrap the master key and decrypt the data.[13]

---

[5] National Institute of Standards and Technology (2013), "Glossary of Key Information Security Terms", NISTIR 7298 Rev 2, Richard Kissel, *Ed* (May 2013) <http://dx.doi.org/10.6028/NIST.IR.7298r2> at 27.

[6] *Ibid* at 52.

> "Cryptanalysis — 1) Operations performed in defeating cryptographic protection without an initial knowledge of the key employed in providing the protection. 2) The study of mathematical techniques for attempting to defeat cryptographic techniques and information system security. This includes the process of looking for errors or weaknesses in the implementation of an algorithm or of the algorithm itself."

[7] This of course is only the case in our current technological context. Potential future developments, including developments in the field of post-quantum computing and quantum cryptography, may change this. Note that these concerns generally only apply to public-key or asymmetric cryptosystems, whereas symmetric cryptosystems will theoretically remain secure.

See e.g., Lily Chen et. al. (2016), "Report on Post-Quantum Cryptography," NISTIR 8105, National Institute of Standards and Technology, U.S. Department of Commerce <http://dx.doi.org/10.6028/NIST.IR.8105>.

> From abstract: "If large-scale quantum computers are ever built, they will be able to break many of the public-key cryptosystems currently in use. This would seriously compromise the confidentiality and integrity of digital communications on the Internet and elsewhere."

[8] Jeffrey Goldberg (2013), "Guess Why We're Moving to 256-bit AES Keys", *Agilebits Blog*, (9 March 2013) <https://blog.agilebits.com/2013/03/09/guess-why-were-moving-to-256-bit-aes-keys/>.

[9] National Institute of Standards and Technology (2016), "Recommendation for Key Management, Part 1: General", *NIST Special Publication 800-57 Part 1, Rev 4* (January 2016) <https://dx.doi.org/10.6028/NIST.SP.800-57pt1r4> at 1.

> "... poor key management may easily compromise strong algorithms. Ultimately, the security of information protected by cryptography directly depends on the strength of the keys, the effectiveness of the mechanisms and protocols associated with the keys, and the protection afforded the keys. Cryptography can be rendered ineffective by the use of weak products, inappropriate algorithm pairing, poor physical security, and the use of weak protocols."

[10] National Institute of Standards and Technology (2010), "Recommendation for Password-Based Key Derivation, Part 1: Storage Application", NIST Special Publication 800-132 (December 2010) <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-132.pdf>.

[11] *Ibid.*; Internet Engineering Task Force (2011), "PKCS #5: Password-Based Key Derivation Function 2 (PBKDF2) Test Vectors," RFC 6070 (January 2011) <https://tools.ietf.org/html/rfc6070>.

[12] It should be noted, however, that even if data has been "password protected," that does not necessarily mean that it has been encrypted (and conversely, not all cryptographic systems use passwords).

[13] See e.g., discussion of TouchID and FaceID in Apple (2018), "iOS Security Guide—White Paper", (January 2018) <https://www.apple.com/business/docs/iOS_Security_Guide.pdf > at 5 et seq.

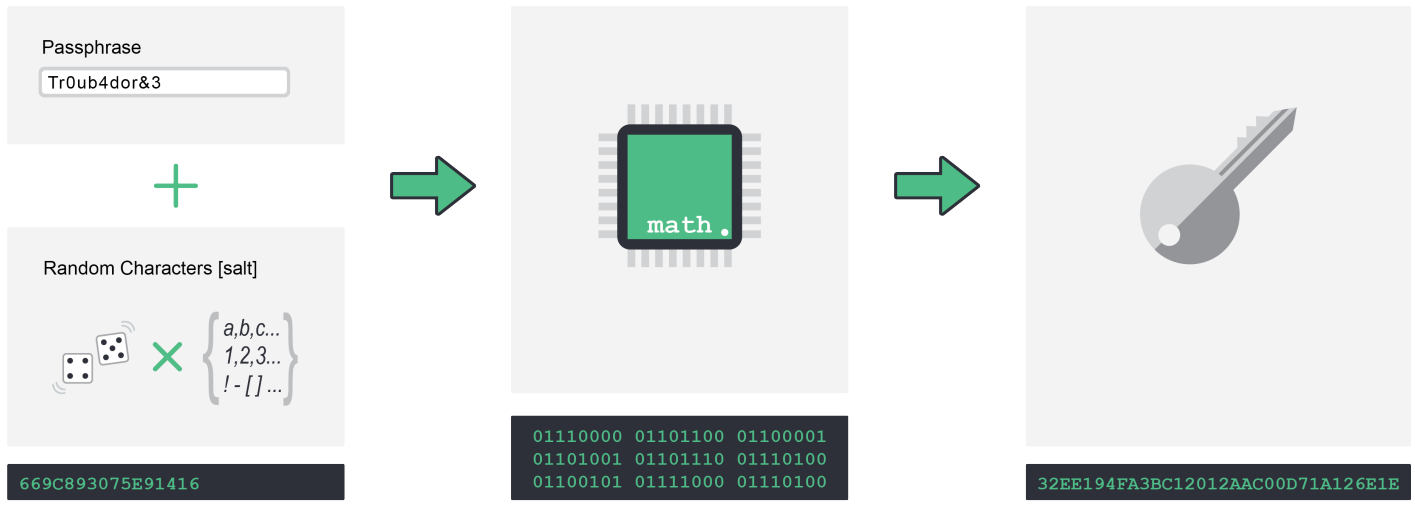


Figure 2: Encryption Key Derived from Password (Tina Salameh, 2018)

The particular mechanism used to derive a secret key can have practical, as well as legal, implications. For example, some courts have made a distinction between the constitutional protections afforded to an individual based on the type of technical mechanism in place (e.g., by distinguishing between a numeric pin and a fingerprint scan).

INFORMATION BOX 1: UNDERSTANDING THE STRENGTH OF A CRYPTOGRAPHIC SYSTEM

The cryptographic strength of an encryption algorithm is generally a function of the length of keys it uses.[i] The length of the key used determines how many different "guesses" an adversary will need to make in order to successfully decrypt a given string of ciphertext without initial access to the key. A 1-bit key size can generate two possible keys (1 or 0), whereas a 2-bit key size can generate 2^2 possible keys (i.e., 1-1, 1-0, 0-1 or 0-0). The strength of a given key increases exponentially with each added bit—using a 20-bit key length means that there are 2^{20} (or 1,048,576) different possible keys, over 260,000 times more than a 2 bit key size.

Most cryptographic systems require that the keys being used are generated at random. If a key generation algorithm is not actually random, an adversary may be able to predict patterns, reducing the number of keys it needs to "guess" before finding the right one. Even the security of a large key can be greatly undermined if the random number generator used to establish it is flawed or not truly random by design.

Cryptanalysis can also uncover other ways to reduce the number of "guesses" it would take to find the correct key through brute force. For example, known weaknesses in the way the popular 256-bit encryption algorithm AES-256 works mean that, under certain theoretical conditions, the AES-256 key will be discoverable in the time it would take to exhaustively search only 2^{70} different combinations instead of the full 2^{256} combinations, leading some experts to prefer AES-128 over AES-256, even though the latter relies on a significantly higher key length.[ii]

In this way, the key length employed by a given cryptographic system can be viewed as setting an upper ceiling for the overall strength of that system, but not as determinative of that strength.

i Note that while the concept of exponential complexity is generally true for symmetric algorithms, it is not true for many popular asymmetric algorithms like RSA. For an explanation of the difference between symmetric and asymmetric algorithms, see section "Symmetric and Asymmetric Encryption." RSA public keys consist of a very large number that is the product of two large primes. They are broken by factoring that number, and prime factorization is sub-exponential. Whereas a 128 bit AES symmetric key would be resistant to a brute force attack, a 128 bit RSA asymmetric key would be trivial to break. See: Jeffrey Knockel, Adam Senft & Ron Deibert, "WUP! There It Is: Privacy and Security Issues in QQ Browser", Citizen Lab (28 March 2016) <https://citizenlab.ca/2016/03/privacy-security-issues-qq-browser/>.

ii The attack requires certain theoretical conditions unlikely to be met in most instances of real-world symmetric use of AES-256. See Alex Biryukov, Orr Dunkelman, Nathan Keller, Dimitry Khovratovich & Adi Shamir, "Key Recovery Attacks of Practical Complexity on AES Variants with up to 10 Rounds", (August 2009) <https://eprint.iacr.org/2009/374.pdf>.

A number of other factors can impact the strength and nature of protection afforded by encryption, as well as impact who is empowered to make decisions regarding the application of encryption to data. These factors include a general distinction made between encryption at rest and encryption in transit.

B. ENCRYPTION AT REST

Encryption *at rest* refers to data which is secured while it is persistently stored at an endpoint, such as on a laptop, a mobile device, or on the server of a service provider. A user can choose to encrypt a single file, folder, or partition, or instead to encrypt an entire device all at once (this is called *full disk encryption*). Many modern devices use full disk encryption by default, or offer built-in tools that allow users to enable it. Users can also download specific software to encrypt their devices and files. When a device is fully encrypted at rest and powered down, its contents are scrambled and almost entirely incomprehensible to third parties without the decryption key. This protects the security of data, ensuring that it cannot be accessed by an unauthorized third party if the device is stolen or lost. Malicious actors can also use device encryption attacks to encrypt data without the permission of a device's owner, locking legitimate users out of their own computers (usually until they pay the malicious actor's fee, which is why this kind of code is often referred to as *ransomware*).[14]

Encryption at rest can be applied at different locations and by different entities, with varying implications for the user. When encryption is applied locally to data at rest on an end-user's device such as a mobile phone or home computer, it is typically referred to as *client-side* encryption. Data can also be stored and encrypted remotely, often referred to as *server-side* encryption. Server-side encryption is common where data is stored on behalf of a customer by a cloud service provider, an email or similar communications provider, or a range of other mobile application services (e.g., banking tools or health and fitness tracking software).[15] When encryption is applied server-side, the type and scope is typically determined by the service provider that controls the servers upon which the data is stored, without user input. When a third party service provider is responsible for encrypting user data, its decisions can affect the ultimate security of that information. In such instances it is up to the service provider to decide both whether to encrypt at all, and how much of the data to encrypt. Notably, many service providers will choose to encrypt the content of communications but not the metadata.[16]

Where a service provider does choose to apply encryption, it can do so using a variety of techniques. Note that data that is encrypted at rest is only as secure as access to the keys. A service provider can encrypt data in such a way that retains its access to the keys and, by extension, its ability to decrypt user information on demand—with or without that user's knowledge, consent, or participation. By contrast, service providers can also choose to design their software so that they do not have the ability to decrypt user data stored on their servers. Services like Spideroak One, Hushmail and Protonmail are all variations on this latter model. As a result, if one of these services is compromised by a malicious actor or legally compelled to produce a copy of a user's private data, only the encrypted, illegible form of the data will be accessible to the third party.[17]

---

[14] See e.g., Wikipedia, May 2017 WannaCry attack: <https://en.wikipedia.org/wiki/WannaCry_ransomware_attack> or Wikipedia, Petya family of encryption ransomware: <https://en.wikipedia.org/wiki/Petya_(malware)>.

[15] Health and fitness trackers provide a useful case study for understanding the potentially invasive scope of data that can be transmitted for remote storage on the service provider's servers.

See e.g., Andrew Hilts, Christopher Parsons & Jeffrey Knockel (2016), "Every Step You Fake: A Comparative Analysis of Fitness Tracker Privacy and Security," Open Effect <https://openeffect.ca/reports/Every_Step_You_Fake.pdf>; Kit Huckvale, José Tomás Prieto, Myra Tilney, Pierre-Jean Benghozi & Josip Car (2015), "Unaddressed Privacy Risks in Accredited Health and Wellness Apps: A Cross-Sectional Systematic Assessment," 13 *BMC Med* 214 <https://dx.doi.org/10.1186/s12916-015-0444-y>.

[16] See e.g., Micah Lee (2016), "Battle of the Secure Messaging Apps: How Signal Beat Whataspp", *The Intercept* (22 June 2016) <https://theintercept.com/2016/06/22/battle-of-the-secure-messaging-apps-how-signal-beats-whatsapp/>.

> "WhatsApp was able to announce it was using the Signal protocol to encrypt all messages, including multimedia messages and group chats, for all users, including those on iOS, by default. So if a government demands the content of WhatsApp messages, as in a recent case in Brazil, WhatsApp can't hand it over — the messages are encrypted and WhatsApp does not have the key. But it's important to keep in mind that, even with the Signal protocol in place, WhatsApp's servers can still see messages that users send through the service. They can't see what's inside the messages, but they can see who is sending a message to whom and when."

[17] Note the relationship between the encryption debate and data retention: you don't need to encrypt what you don't collect or process in the first place. See e.g. Open Whisper Systems (2016), *Grand jury subpoena for Signal user data*, Eastern District of Virginia (4 October 2016) <https://signal.org/bigbrother/eastern-virginia-grand-jury/>.

Data may be encrypted at rest in multiple locations at once. For example, Signal (an encrypted messaging application) encrypts all user content locally on their device. It also encrypts the data it stores or processes remotely on its own servers.[18] Signal retains the ability to decrypt certain data stored on its servers (including registered users' telephone numbers and profile information) so it can use the information when it processes user actions on its service. Similarly, when a user accesses the Signal app on her phone, the historical messages stored on that device will be decrypted so she can read them in plaintext.[19] Decisions about where data is stored, and which party has the power to decrypt it, will involve different risks, benefits, and trade-offs depending on the types of security threats that most concern the user. For example, a user who does not believe their device is physically secure may prefer to store all of their data on the servers of a cloud service provider, so that it can be retrieved even if their device is lost or stolen. By contrast, a user who does not trust their service provider to adequately protect their data from criminal actors or inappropriate state intrusion may prefer to store their data locally, on a device under their exclusive physical control.

Individual users can protect their data even when it is stored on a third party's servers by independently encrypting it before uploading it to the service provider. A user can, for example, encrypt a file on their computer using a tool like GPG,[20] and then upload the encrypted file to a service like Dropbox or send it as an attachment to an email using a service like Gmail. Though both Dropbox and Gmail can decrypt data they have encrypted themselves,[21] neither service would be able to decrypt the file in question because it was encrypted using keys solely in the hands of the end-user.

C. ENCRYPTION IN TRANSIT

Encryption *in transit* refers to the process of using encryption to secure information as it travels from one computer to another. This prevents data—such as web traffic, a text message, content entered into a webform, or an e-mail—from being intercepted or modified by an unauthorized third party as it travels to its destination over the network. Encryption in transit protects the confidentiality and integrity of the content while facilitating authentication.

When browsing the Internet using an unencrypted connection, private data (such as the specific web pages a user visits, the content of their communications on those websites, usernames, passwords, or other personal information they enter into webforms) can be seen by third parties—from government actors and law enforcement agencies to Internet service providers, criminal eavesdroppers, or casual listeners on an unsecured network.[22] By contrast, using HTTPS (that is, HTTP using the Transport Layer Security (TLS) standard) to encrypt a connection to a given website protects much of that information from eavesdropping or tampering (though the identity of the website, the user's IP address, and certain kinds of other information remain visible).[23] Of course, data that is encrypted in transit can still be vulnerable if it is not adequately secured and encrypted at rest once received.

D. INTERMEDIARY ACCESS & END-TO-END ENCRYPTION

As is the case when data is encrypted at rest, attempts to encrypt data in transit are only as secure as the keys used in the encryption process. *End-to-end encryption* refers to systems which encrypt a message in-transit so that *only* the devices at either end of the exchange have access to the keys required to decrypt the data. In other words, the service provider or intermediary

---

[18] See Open Whisper Systems, "Privacy Policy" (2016) <https://whispersystems.org/signal/privacy/> and Open Whisper Systems, "The Difficulty of Private Contact Discovery" (2014) <https://whispersystems.org/blog/contact-discovery/>.

[19] If the user has an Android device, their Signal application may also have a separate password.

See: Justin Meyers (2017), "How to Password-Protect Your Calls, Texts & Notification Previews", Gadget Hacks, (9 August 2017) <https://android.gadgethacks.com/how-to/signal-101-password-protect-your-calls-texts-notification-previews-0179365/>.

[20] Gnu Privacy Guard (1999), "The GNU Privacy Handbook", GNU General Public License, Free Software Foundation <https://www.gnupg.org/gph/en/manual/x110.html>.

[21] Dropbox, "Security" (accessed 5 February 2018) <https://www.dropbox.com/security>; Google, "Google Cloud Help – Security" (accessed 5 November 2017) <https://support.google.com/googlecloud/answer/6056693>.

[22] Electronic Frontier Foundation, "How HTTPS and Tor Work Together to Protect Your Anonymity and Privacy," (accessed 5 February 2018) <https://www.eff.org/pages/tor-and-https>; Electronic Frontier Foundation, "HTTPS Everywhere," (accessed 5 February 2018) <https://www.eff.org/https-everywhere>.

[23] *Ibid*. Note that in order to obfuscate the identity of the user, their location, and other kinds of metadata, an anonymity tool such as Tor must be used in addition to encrypting the traffic in transit.

does not have the ability to decrypt it, and cannot access the data as it travels from one user to another except in its encrypted form. This is the case for applications like Wire, WhatsApp, and Signal (which provide end-to-end encryption between the senders and recipients of voice calls and text messages). By contrast, some service providers will encrypt data in transmission but retain the decryption keys. For example, the default mode for Telegram uses *client-server/server-client* encryption while storing chats in an encrypted format on its own servers. In other words, Telegram by default has access to all the encryption keys, including the keys used to encrypt messages in transit between the message sender and its servers, the keys used to encrypt chats at rest for long term storage, and the keys used to encrypt the message between its servers and the message recipient.[24]

The ability of a service provider to access the unencrypted form of encrypted data, whether in transit or at rest, is a key determinant of an encryption system's overall security, and often has significant legal implications. For example, if Angelica wants to phone Benjamin, she can call him using the default voice application on her mobile device. The connection between her phone and the cell phone tower will be encrypted, and an unauthorized third party attempting to eavesdrop on that phone call will not be able to "listen in" to their conversation without taking more intrusive measures. Nevertheless, that conversation can still be intercepted, overheard, and recorded with the assistance of a telecommunications service provider—for example by a law enforcement officer who has sought prior judicial authorization for a wiretap under the *Criminal Code* or by a malicious adversary who has compromised the service provider's network. By contrast, if Angelica initiates her voice call with Benjamin using a mobile application that uses end-to-end encryption (e.g. Signal), third parties will not be able to listen in to the call regardless of whether they are a service provider, law enforcement officer, signals intelligence agency, or criminal eavesdropper. To Angelica and Benjamin, the process of making the phone call will feel more or less identical but, to a third party, their conversation becomes unintelligible. The relative privacy and security of their call is therefore fundamentally different depending on the technology they use and whether or not their conversation is encrypted end-to-end.

Absent end-to-end encryption, messages sent online are exposed to various service providers that might be able to decrypt the message between a sender and intended recipient. Each of these service providers constitutes an additional potential point of compromise. For example, imagine that Asma wants to e-mail her friend Behzad using their Gmail accounts. The connection between Asma's computer and Google's servers (and between Behzad's computer and Google's servers) can be encrypted so that a third party eavesdropper cannot read the message. However, Gmail will still be able to read the plaintext version of her e-mail on its own servers. This is the case for a large number of communication service providers, from Skype to Facebook Messenger, which either do not apply encryption, or retain encryption keys in applying it.[25] The security of these messages is predicated on the assumption that the service provider is not compromised by a malicious actor, not voluntarily disclosing user data to third parties (such as advertisers), and not being compelled to disclose information to law enforcement or intelligence agencies. By contrast, end-to-end encryption tools such as the OTR plugin—which lets users encrypt instant messages over services such as Google's chat application—generate secret keys only on end-user devices, leaving Google (or any other service provider involved in the transmission of the messages) unable to decrypt the contents of the communication.[26]

E. SYMMETRIC & ASYMMETRIC ENCRYPTION

Symmetric encryption is the term used when the same key is used to both encrypt and decrypt data. This kind of system works well for encryption of data at rest. However, unless two parties have a way to agree on a shared secret in advance—for example, if Ariel and Biella meet in a park and agree on a shared passphrase together, or swap a copy of a private key file on a USB drive—they will be unable to communicate privately over a public network. This is because distributing a secret key over a public network would compromise its secrecy.

---

[24] Telegram, "Privacy Policy—Storing Data" (accessed 5 February 2018) <https://telegram.org/privacy#2-storing-data>.

Telegram notes explicitly that it has never disclosed a single byte of data to a third party, inclusive of governments, as of February 2018. However, the messaging service faces growing pressure from some governments to provide access to its encryption keys.

See Leonid Bershidsky (2017), "Russia Wants to Make an Example of Telegram", *Bloomberg* (28 September 2017) <https://www.bloomberg.com/view/articles/2017-09-28/russia-wants-to-make-an-example-of-telegram>.

[25] Note that Facebook allows users to choose, on a chat-by-chat basis, to enable end-to-end encryption: see "Secret Conversations" (accessed 5 February 2018) <https://www.facebook.com/help/messenger-app/1084673321594605/?helpref=hc_fnav>.

[26] Note that in this example, Google can still access the metadata related to the conversation. See Off-the-Record Messaging, "Frequently Asked Questions" <https://otr.cypherpunks.ca/index.php#faqs>.

Asymmetric encryption, often referred to as *public key encryption,* addresses this problem by using a cryptographically generated pair of keys which have a special mathematical relationship to each other. In such systems, one of the keys is kept secret (the *private key*) and the other (the *public key*) is made freely available: it can be shared openly over an unsecured network. In this model, even if Ariel and Biella have never met, Ariel can post her public key online (e.g., on her website, to her Twitter account, or to servers dedicated to facilitating public key exchanges[27]). Biella can then use Ariel's public key to encrypt messages that only Ariel can decrypt using the unique, secret private key associated with the public one she shared. Public key cryptography is essential to securing web traffic and communications online, and is the foundation of encryption technologies like TLS/SSL and PGP.

INFORMATION BOX 2: WEB BROWSING WITHOUT ENCRYPTION

Encryption not only protects the confidentiality of transmitted data, but also the transmission of important online identifiers which govern access and control of online accounts.

Many online services use SSL/TLS encryption to secure the transmission of login credentials, but have historically failed to secure other user interactions with the website. When a user logs into a service such as Facebook, Google, Amazon or Twitter, a temporary unique identifier is set on that user's computer or mobile device. This temporary identifier is then used by the web service to recognize the user until she logs out of the service. Historically, transmission of these temporary identifiers was not encrypted. This left many transactions exposed to third party listeners.

As a now-defunct plugin for the Firefox browser called Firesheep[i] demonstrated, this weakness also let third parties take control of an account without intercepting the login and user password associated with it. Firesheep lets anyone "sidejack" other people's accounts at the click of a button by capturing temporary identifiers transmitted without encryption over unsecured WiFi networks such as those used at coffee shops and airports. Most services are no longer vulnerable to Firesheep because, following its release, major service providers transitioned to using SSL/TLS in all their user-server interactions.

i Eric Butler, "Firesheep", {codebutler} (24 October 2010) <http://codebutler.com/firesheep>.

F. FORWARD SECRECY

Another important security property is whether a given asymmetrical system offers *forward secrecy*. In order to understand forward secrecy, it is important to understand the concept of *session keys.* Asymmetric encryption algorithms are generally computationally expensive compared to symmetric algorithms. Rather than encrypting and decrypting each entire message with an asymmetric key pair, these systems use the asymmetric key pair to agree upon a new symmetric session key instead. That new session key is then used to encrypt and decrypt each message between the parties. Session keys are ephemeral, and discarded after the session is over.

When not using forward secrecy, a session key is locally generated, then sent and encrypted with the public key. If a third party recorded this exchange and then later obtained the private key, they would be able to decrypt both the session key and the content that it had been used to encrypt. By contrast, when using forward secrecy, the session key is agreed upon using an algorithm in a manner that ensures neither the session key nor enough information for a passive eavesdropper to reconstruct it is

[27] See e.g.: MIT PGP Public Key Server <https://pgp.mit.edu/>.

ever transmitted.[28] In this model, even if a private key is compromised, without the old session keys, historical messages remain secure and cannot be decrypted. An adversary, even with the private key, also could not passively decrypt future captured messages. Instead, they would need to actively attack the network between the parties during the time of their communication in order to obtain the data on a going-forward basis.

Without forward secrecy, historical messages are susceptible to decryption once the adversary obtains the private key. This means that if an adversary with network monitoring capabilities has been collecting copies of encrypted data over a long period of time, and then later acquires the private key, they could retroactively decrypt all of the encrypted data they possess. State actors can (and do) amass large volumes of encrypted network traffic in anticipation that the encryption used to secure those messages might one day be broken.[29]

G. ENCRYPTION & METADATA

A final factor impacting the overall scope of protection offered by encryption relates to the question of what data is actually encrypted. Depending on operational necessity, business model, and evolving technical best practices, not all types of data will be encrypted. Specifically, while many service providers render the *content* of a message incomprehensible, the *metadata* (typically defined as "information about information") with which that content is associated often remains legible to third parties. Metadata frequently remains exposed for reasons of operational necessity—for example, network equipment must be able to read the source and destination IP address associated with a IP transmission in order to route it to its destination.[30] While this information is potentially revealing, it cannot be readily encrypted because no encryption standard has been adopted for the routing equipment deployed by different networks, and purchased from different manufacturers, used to copy the packet across its path. In other contexts, service providers with access to a multi-provider encryption standard, or which do not require inter-provider interoperability, will nonetheless make a business decision to leave metadata exposed—often because they wish to save processing power to enhance speed and capacity, but sometimes also based on the historical misconception that metadata is intrinsically less sensitive than the content of a communication or file. In reality, metadata can be as revealing as digital "content" (if not more) and deserves at least the same level of protection.[31] Some examples where encryption may apply to content but leave metadata exposed include:

---

[28] See generally: Whitfield Diffie, Paul C. Van Oorschot & Michael J Wiener (1992), "Authentication and Authenticated Key Exchanges" (March 1992) <http://people.scs.carleton.ca/~paulv/papers/sts-final.pdf>; R. Shirey (2007), "Internet Security Glossary, Version 2", FYI 36, RFC 4949 (August 2007) <https://tools.ietf.org/html/rfc4949>; Y. Sheffer, R. Holz & P. Saint-Andre (2015), "Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)", BCP 195, RFC 7525 (May 2015) <https://tools.ietf.org/html/rfc7525>.

Note that both ends of the exchange first establish one shared number, and then each end generates secret numbers which they never exchange. They use a special mathematical operation to modify the shared number using both secrets with two important properties, (1) that it does not matter in which order the shared number is modified by each secret number, and (2) that a secret number cannot be efficiently derived from knowing both the shared number and a shared number modified with one of the secrets. To agree upon a session key, each end first modifies the shared number with their secret, and then sends the modified version to the other end, which modifies it with that end's secret. By property (1), both ends have agreed upon the same session key, despite modifying the shared number in the opposite order, and by property (2), a passive eavesdropper, who can observe both the shared number and its modification with each secret, cannot derive the session key because the eavesdropper cannot efficiently derive either secret and the session key itself is never transmitted.

[29] For example, the U.S. National Security Agency records all encrypted (and other) communications and keeps them for about three to five days, with encrypted data streams deemed potentially useful retained for longer periods of time.

See Glenn Greenwald (2013), "XKeyscore: NSA tool collects 'nearly everything a user does on the internet'", *The Guardian* (31 July 2013) <https://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data>; Glenn Greenwald (2013), "Revealed: how US and UK spy agencies defeat internet privacy and security", *The Guardian* (6 September 2013) < https://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security>; National Security Agency (2009), "TURBULENCE: APEX Active/Passive Exfiltration, STDP: S32354 & T112, NCSC/C91 (August 2009) available at Electronic Frontier Foundation:<https://www.eff.org/files/2015/02/03/20150117-spiegel-apex_method_of_combining_passive_with_active_methods_to_exfiltrate_data_from_networks_attacked.pdf>.

[30] See Canadian Internet Policy and Public Interest Clinic (2009), Submission to the Office of the Privacy Commissioner of Canada: Rogers' Use of Deep Packet Inspection Equipment (2 December 2009) <https://cippic.ca/sites/default/files/OPC-Submission-Rogers_and_DPI-FINAL.pdf> at 10.

[31] United Nations (2014), Office of the United Nations High Commissioner for Human Rights, "The right to privacy in the digital age" A/HRC/27/37, at para 19.

> "In a similar vein, it has been suggested that the interception or collection of data about a communication, as opposed to the content of the communication, does not on its own constitute an interference with privacy. From the perspective of the right to privacy, this distinction is not persuasive. The aggregation of information commonly referred to as 'metadata' may give an insight into an individual's behaviour, social relationships, private preferences and identity that go beyond even that conveyed by accessing the content of a private communication. As the European Union Court of Justice recently observed, communications metadata 'taken as a whole may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained.'"

- If Angelisa sends an encrypted e-mail to Bilal using software like PGP, the message ("Dear Bilal…") she sends him will appear as a meaningless string of characters to an eavesdropping third party. However, the information contained in the e-mail header will not be encrypted. Metadata, including information such as the e-mail "Subject" line, the time and date it was sent, the service provider used, and the e-mail addresses of both sender and recipient will remain visible to third parties. These fields are necessary for the message delivery process and therefore cannot be encrypted by the sender using PGP.

- If Etienne encrypts a report on his computer using Microsoft Word, a third party will not be able to read the document itself. However, information such as when that file was created, when it was last modified, its approximate size, and the file name will remain visible. Tools such as VeraCrypt or the backup service SpiderOak One reduce this visibility by placing the files in encrypted "containers" or by assigning files random sequential numbers as file names when stored remotely.[32]

- If Imani wants to make a mobile phone call, the content of that call will be encrypted by the service provider in transmission between her phone and the nearest network cell phone tower. However, a digital identifier associated uniquely with her SIM card (an IMSI number) may be transmitted in plaintext or using weak encryption, allowing third parties to identify otherwise anonymous individuals and track them pervasively with the proper tools.[33]

- If Alejandro visits a company's website—like a social media service or his financial institution—using an encrypted connection secured with HTTPS, he can protect information (such as the personal data he enters into a webform, his login credentials, and the specific site URLs that he visits) from third parties. However, metadata (including the IP address of the computer or mobile device he used to access the site and of the website itself, as well as the website's domain name) will remain visible to hackers, Internet service providers, and government agencies alike.[34] Anonymity tools such as Tor can be used to hide these types of identifiers, including a user's identity and location online.[35]

Despite historic misconceptions to the contrary, metadata can be highly revealing. One study of phone call metadata logs on mobile devices found that a high volume of caller profiles allowed for sensitive inferences regarding the political views, religious beliefs, health conditions and intimate partners of individual callers.[36] The invasive potential of metadata can also be substantially magnified when collected and analyzed en masse. This is due to its semi-structured and machine-readable nature, which makes it highly susceptible to nuanced analysis at large scale. This, in turn, allows for deep inferences to be drawn in an automated and systematic manner, which is more challenging to do when analyzing the "content" of data. On this basis, the sensitivity and privacy interest in metadata is increasingly recognized by courts, academics, and legal experts, as is the need to secure such data against unauthorized access.[37]

---

[32] SpiderOak (2017), "Encryption White Paper" <https://spideroak.com/resources/encryption-white-paper>.

[33] While the IMSI must be exposed to the network service provider in order to process mobile calls, it need not be transmitted unencrypted over the radio network, where it is highly vulnerable to interception by a large number of entities.

See Tamir Israel and Christopher Parsons (2016), "Gone Opaque? An Analysis of Hypothetical IMSI Catcher Overuse in Canada," v 2.0, Telecom Transparency Project and Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic (August 2016) <https://citizenlab.ca/wp-content/uploads/2016/09/20160818-Report-Gone_Opaque.pdf>.

[34] Compare unencrypted internet use to use with HTTPS to use with Tor. See: Electronic Frontier Foundation, "How HTTPS and Tor Work Together to Protect Your Anonymity and Privacy," <https://www.eff.org/pages/tor-and-https>.

[35] *Ibid.*

[36] Jonathan Mayer, Patrick Mutchler & John C. Mitchell (2015), "Evaluating the Privacy Properties of Telephone Metadata," 113(20) *Proceedings of the National Academy of Sciences (PNAS)* 5536, <http://www.pnas.org/content/113/20/5536.full>.

[37] Necessary & Proportionate Coalition (2014), "International Principles on the Application of Human Rights Law to Communications Surveillance," (May 2014) <https://necessaryandproportionate.org/principles>.

> "Traditionally, the invasiveness of Communications Surveillance has been evaluated on the basis of artificial and formalistic categories. …. While it has long been agreed that communications content deserves significant protection in law because of its capability to reveal sensitive information, it is now clear that other information arising from communications – metadata and other forms of non-content data – may reveal even more about an individual than the content itself, and thus deserves equivalent protection. Today, each of these types of information might, taken alone or analysed collectively, reveal a person's identity, behaviour, associations, physical or medical conditions, race, color, sexual orientation, national origins, or viewpoints; or enable the mapping of the person's location, movements or interactions over time, or of all people in a given location, including around a public demonstration or other political event. As a result, all Protected Information should be given the highest protection in law."

Investigative agencies also recognize the value and importance of metadata. For example, an communications data analyst for the Royal Canadian Mounted Police (RCMP) explained:

> "So when it comes to communications metadata, it's information about the phone calls themselves. … We normalize it and organize it in a way to turn it from data to information. A date on its own means nothing. When I turn a date into the day of the week, I can find patterns of usage that repeat themselves, say on Sunday. When I turn a date into a month, I can see which month a suspect's visited a general area the most. Now I've turned data into information.
>
> In this digital age, we're leaving crumbs of digital data behind everywhere we go and in everything that we do. Modern mobile devices are ubiquitous. They go to sleep with us, speak to our friends, and access the websites we're interested in. They do everything that we like to do and go with us everywhere we go. And they're our camera, our alarm clock, our calendar, our web-browsing device — cellphones are the Swiss Army knife of technology. … The frequent usage of these devices really turns them into a tracker in the hand of the user. And if you know how to leverage that information and make sense of it, there's so much you can do with it."[38]

Understanding the nature of metadata is important to understanding the importance of encryption for user security, as well as the technology's limits. Even the most comprehensive encryption will continue to leave some metadata exposed which, in turn, minimizes the degree to which encryption can impede legitimate investigations.

[38] Royal Canadian Mounted Police (2017), "Crumbs of digital data: Data analyst makes sense of phone calls", *Gazette Magazine* 79:3 (4 July 2017) <http://www.rcmp-grc.gc.ca/en/gazette/crumbs-digital-data?re>.

PART 2: WHY ENCRYPTION MATTERS

> **"It is neither fanciful nor an exaggeration to say that, without encryption tools, lives may be endangered. In the worst cases, a Government's ability to break into its citizens' phones may lead to the persecution of individuals who are simply exercising their fundamental human rights."**
>
> **— United Nations High Commissioner for Human Rights Zeid Ra'ad Al Hussein**

Encryption enables the exercise of fundamental rights and freedoms, including freedom of thought, belief, opinion, expression, and association. It allows for greater democratic participation in the digital sphere and it is integral to protecting and affirming the privacy rights, dignity, and the security of persons, in particular those persons most marginalized or otherwise vulnerable. Encryption technology also has countless commercial, scientific, and defensive applications, underpinning everything from modern banking and the secure storage of medical records to the operation of critical infrastructure. Finally, it has critical benefits for public safety, national defence, and global security. In this section, we outline the social, political, and economic significance of access to encryption technology.

A. ENCRYPTION ENABLES FUNDAMENTAL RIGHTS & FREEDOMS

There is a strong basis for the protection and development of secure communications tools under both international and domestic human rights law and norms. The right to privacy, protected by Article 12 of the Universal Declaration of Human Rights (UDHR)[39] and Article 17 of the International Covenant on Civil and Political Rights (ICCPR),[40] is the right most directly supported by the availability and use of robust encryption. But encryption is also closely linked to freedom of expression, protected by Articles 19 of the UDHR and the ICCPR, for at least two reasons. First, encryption code is itself a form of expression that is protected as speech by some constitutional frameworks, including in the United States.[41] Second, robust encryption is critical in realizing free expression in digital networks. Encryption is also critical to a range of other human rights, including freedom of association, and is an increasingly

---

[39] United Nations General Assembly (1948), "Universal Declaration of Human Rights", United Nations (10 December 1948) <http://www.un.org/en/universal-declaration-human-rights/>:

> "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."

[40] United Nations General Assembly (1976), "International Covenant on Civil and Political Rights", United Nations (16 December 1966) < http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx>:

> 1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
>
> 2. Everyone has the right to the protection of the law against such interference or attacks.

[41] Electronic Frontier Foundation (2015), "Anonymity and Encryption", Comments submitted to the United Nations Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression (10 February 2015) <https://www.eff.org/files/2015/02/10/unanonymity-encryption-eff.pdf> at 36:

> "Developers of encryption software are engaged in their own expressive activity when they publish code. Any attempt to prohibit encryption would also run up against the freedom of expression. Many strong end-to-end encryption programs are open source code, publicly posted and available to anyone to download from a wide variety of sources. If a state were to attempt to prohibit these programs, it would need to control access to this information, prohibit publication, or institute the infrastructure necessary to detect and penalize use. All of these methods would have severe and negative consequences for freedom of expression."

See also, Amul Kalia (2016), "Encryption is a Human Rights Issue: Your Privacy and Free Speech Depend on it", *Learn Liberty* (21 December 2016) <http://www.learnliberty.org/blog/encryption-is-a-human-rights-issue-your-privacy-and-free-speech-depend-on-it/>; Andrew Crocker and Nate Cardozo (2015), "Deep Dive into Crypto "Exceptional Access" Mandates: Effective or Constitutional—Pick One", *Electronic Frontier Foundation* (13 August 2015) <https://www.eff.org/deeplinks/2015/08/deep-dive-crypto-exceptional-access-mandates-effective-or-constitutional-pick-one>; D. Victoria Baranetsky (2017), "Encryption and the Press Clause," *Journal of Intellectual Property and Entertainment Law* (2017) 6:2 <jipel.law.nyu.edu/wp-content/uploads/2017/04/NYU_JIPEL_Vol-6-No_2_1_Baranetsky_PressClause.pdf>.

important precondition for many core democratic functions, from protecting the integrity of democratic elections and judicial proceedings to effective political advocacy.

These rights are also guaranteed and protected by the Canadian *Charter of Rights and Freedoms*. Attempts to interfere with the use or development of encryption technology therefore often invite *Charter* scrutiny as a result of the potential impact on the fundamental freedoms guaranteed in section 2 of the *Charter* and the right to be secure against unreasonable search and seizure in section 8. In some circumstances, attempts by state actors to limit, undermine, or circumvent the use of encryption tools may also have important implications for other rights, such as the right to security of the person (section 7); the right to silence, the protection against self-incrimination, and the right not to be compelled as a witness against oneself (sections 7, 11, and 13); or even equality rights (section 15). In the final sections of this report, we will explore specific impacts on these *Charter*-protected rights that can arise when efforts are made to undermine or bypass encryption.

Encryption is essential to preserving the privacy and integrity of countless digital interactions in an era where communication occurs on globalized traffic flows that are routinely subjected to mass and untargeted surveillance[42] by a range of government agencies worldwide. Increasingly, encryption provides one of the only reliable, pragmatic safeguards against such untargeted state surveillance, carving out private spaces that would otherwise be impossible online. Encryption is also critical to the work of certain kinds of professionals (e.g., lawyers, doctors, researchers, journalists, and therapists) who are routinely entrusted with sensitive and privileged information by and about others. In some cases, this special role makes them targets for heightened scrutiny (or even abuses of power) by state actors at home or abroad, and by those seeking access to information about those they protect. Access to encryption allows such professionals to better meet their legal and ethical obligations to clients, patients, and sources—and to otherwise protect the individuals they serve from harm.

Encryption not only secures the confidentiality of data against unauthorized access, but also the underlying integrity of information. For example, encryption secures transmission of passwords and verification codes, which in turn protects the content in those accounts from being obtained by a third party. But it also prevents that content from being altered, destroyed,[43] or otherwise hijacked to publish false, misleading, or wrongfully attributed information.[44] Encryption can also inhibit certain kinds

---

[42] While inconsistent with international human rights law, many states disregard the privacy of foreigners under the mistaken presumption that a state's obligation to protect privacy stops at its borders. This mistaken presumption leads to a "capture any foreign interaction" attitude (with notable collateral impacts on domestic privacy rights) that is become increasingly feasible at the technical level.

See e.g.: United Nations (2014), Office of the United Nations High Commissioner for Human Rights, "The right to privacy in the digital age" (2014) A/HRC/27/37 at para 35; United Nations (2014), "Concluding observations on the fourth periodic report of the United States of America," International Covenant on Civil and Political Rights Human Rights Committee (2014) CCPR/C/USA/CO/4 at para 22.

[43] For example, by encrypting the information as part of a ransomware attack.

[44] Amar Toor & Russell Brandom (2015), "A Spy in the Machine," *The Verge* (21 January 2015) <https://www.theverge.com/2015/1/21/7861645/finfisher-spyware-let-bahrain-government-hack-political-activist>:

> "Now 33, Moosa [Abd-Ali Ali]mhas spent most of his life campaigning for democracy and equal rights in Bahrain ... One day in 2011, Moosa opened the Facebook Messenger app on his iPhone. What he saw was chilling: someone else typing under his name to an activist friend of his in Bahrain. Whoever it was kept posing personal questions prodding for information, and Moosa watched unfold right before eyes. He panicked. … In another instance, Moosa noticed that someone posing as him solicited his female Facebook friends for sex — part of an effort, it seemed, to blackmail or perhaps defame him in Bahrain's conservative media."

See also: Heidi Moore and Dan Roberts, "AP Twitter Hack Causes Panic on Wall Street and Sends Dow Plunging", *The Guardian* (23 April 2013) <https://www.theguardian.com/business/2013/apr/23/ap-tweet-hack-wall-street-freefall>:

> "The 143-point fall in the Dow Jones industrial average came after hackers sent a message from the Twitter feed of the Associated Press, saying the White House had been hit by two explosions and that Barack Obama was injured. ... News organizations set their own passwords for their Twitter accounts, which makes hacking a risk."

of censorship—network or device filters cannot censor content or prohibited websites when they cannot distinguish one word, destination website, or hyperlink from another.[45]

Encryption is also a particularly critical technology in maintaining anonymity online. In digital contexts, "[a]nonymity in communications is one of the most important advances enabled by the Internet, and allows individuals to express themselves freely without fear of retribution or condemnation."[46] However, the fact that digital identifiers accompany much of our online activities can threaten the effective exercise of that right.[47] As the United Nations (UN) Special Rapporteur on freedom of expression noted in his seminal report on digital security tools, encryption can:

> "…provide the privacy and security necessary for the exercise of the right to freedom of opinion and expression in the digital age. Such security may be essential for the exercise of other rights, including economic rights, privacy, due process, freedom of peaceful assembly and association, and the right to life and bodily integrity."[48]

The report also highlights the fact that while freedom of opinion has historically received less attention from commentators, "the mechanics of holding opinions have evolved in the digital age and exposed individuals to significant vulnerabilities … [as] holding opinions in the digital age is not an abstract concept limited to what may be in one's mind."[49] Today, a complex record of an individual's beliefs, thoughts, reflections, and questions can be revealed as part of their digital footprint (e.g., through their personal search and browsing history or through review of archived text messages). Access to encryption technology (in concert with other security and anonymity tools) mitigates the potential for these newly recorded manifestations of our innermost thoughts to become the inappropriate subject of state scrutiny.

Scholars and courts have consistently recognized that even just the *belief* that one is under surveillance or that one's communications are insecure is enough to have a chilling effect, causing individuals to change their speech, behavioural patterns,

---

[45] Jonathan Zittrain, Robert Faris, Helmi Noman, Justin Clark, Casey Tilton, and Ryan Morrison-Westphal (2017), "The Shifting Landscape of Global Internet Censorship", Berkman Klein Center for Internet & Society Research Publication <http://nrs.harvard.edu/urn-3:HUL.InstRepos:33084425> at 1.

> "The default implementation of encrypted connections by major social media and content hosting platforms along with messaging applications has effectively downgraded the filtering apparatuses used by states that filter the Internet by counting on "deep packet inspection" or URL analysis to intercept unwanted connections as users attempt to forge them. In those cases, state authorities can no longer selectively block individual accounts, web pages, and stories. For example, governments can generally no longer selectively block a specific article on the New York Times or Wikipedia, or a particular account on Twitter or Facebook, without blocking those sites and services in their entirety."

See also Citizen Lab (Munk School of Global Affairs, University of Toronto) and Collin Anderson (2015), Joint Submission to the United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Mr. David Kaye (10 February 2015) <https://citizenlab.ca/wp-content/uploads/2015/02/SR-FOE-submission.pdf>; David Kaye (2015), Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/29/32, 29th session of the Human Rights Council <http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/Pages/ListReports.aspx> at para 25.

[46] Frank La Rue (2013), "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression," A/HRC/23/40 (17 April 2013) <http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf> at para 23; *R v Spencer*, 2014 SCC 43 at para 43.

[47] *R v Spencer*, 2014 SCC 43 at para 43.

[48] David Kaye (2015), Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/29/32, 29th session of the Human Rights Council <http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/Pages/ListReports.aspx> at paras 20-21.

[49] *Ibid* at para 20.

and habits online.[50] A 2016 study demonstrated a link between the 2013 National Security Agency (NSA) surveillance revelations and reduced web traffic to Wikipedia articles that are (or that are perceived to be) likely to be monitored by the state.[51] Another recent study found that participants exhibited a reluctance to speak out in hostile opinion climates after being made aware of the possibility of state surveillance.[52] All individuals are affected by these chilling effects, especially when expressing dissenting views or seeking information that is less aligned with accepted majority discourses.[53] However, the chill of unmitigated surveillance can have particular repercussions for journalists, vulnerable communities and human rights advocates, and those in the medical and legal professions. Robust encryption and effective anonymity tools, by extension, have specific and noteworthy implications for each of these segments of society.

Encryption technology is critical to ensuring freedom of the press, and to protecting journalists, researchers, sources, and whistleblowers alike. It facilitates journalism by providing the press with the confidence necessary to explore stories that are controversial or that may threaten those who wield the very surveillance powers in question. For example, a PEN America survey of journalists found that almost a quarter of respondents had "deliberately avoided certain topics in phone or email conversations" and 28% "curtailed or avoided social media activities" due to surveillance concerns following the Snowden disclosures.[54] These fears have also been mirrored in research on attitudes held by the Canadian press, notably in a study conducted by the Centre for Free Expression at Ryerson University in collaboration with PEN Canada and the Canadian Association of Journalists.[55] Sources–particularly government sources–have also become less willing to interact with reporters in light of ubiquitous surveillance capabilities. A study conducted by Human Rights Watch and the American Civil Liberties Union (ACLU) in the wake of the Snowden revelations found that public officials were "substantially less willing to be in contact with the press, even with regard to unclassified matters or personal opinions."[56] This chilling trend, which undermines the ability of a free press to obtain the information that it requires to continue to serve its fundamental democratic function, can only be expected to grow as surveillance techniques are increasingly levelled directly at uncovering reporters' sources or records.[57] For example, a recent Commission of Inquiry in Quebec documented a number of instances where law enforcement agencies directed surveillance powers at suspected sources in journalistic reporting on police-related matters.[58] As a byproduct of these inquiries

---

[50] See United Nations (2013), Office of the United Nations High Commissioner for Human Rights, "The right to privacy in the digital age" (2014) A/HRC/27/37 at para 20:

> "Even the mere possibility of communications information being captured creates an interference with privacy, with a potential chilling effect on rights, including those to free expression and association."

See also *R v Taylor*, [1990] 3 SCR 892, at paras 76-77:

> "... s. 13(1) works to suppress private communications, demonstrating an extensive and serious intrusion upon the privacy of the individual. ... I do not disagree with the view that telephone conversations are usually intended to be private; it is surely reasonable for people to expect that these communications will not be intercepted by third persons. ... The connection between s. 2(b) and privacy is thus not to be rashly dismissed, and I am open to the view that justifications for abrogating the freedom of expression are less easily envisioned where expressive activity is not intended to be public, in large part because the harms which might arise from the dissemination of meaning are usually minimized when communication takes place in private, but perhaps also because the freedoms of conscience, thought and belief are particularly engaged in a private setting."

See also *Bennett v Lenovo*, 2017 ONSC 1082 at para 27:

> "The risk of unauthorized access to private information is itself a concern even without any actual removal or actual theft. For example, if a landlord installs a peephole allowing him to look into a tenant's bathroom, the tenant would undoubtedly feel that her privacy had been invaded even if the peephole was not being used at any particular time".

See also Cindy Cohn (2016), "Protecting the Fourth Amendment in the Information Age: A Response to Robert Litt," (2016) 126 Yale LJ 107 <https://www.yalelawjournal.org/pdf/11.CohnFinalPDF_d5acfu8u.pdf>.

[51] Jon Penney (2016), "Chilling Effects: Online Surveillance and Wikipedia Use" (2016) 31(1) *Berkeley Technology Law Journal* 117 <https://ssrn.com/abstract=2769645>.

[52] Elizabeth Stoycheff (2016), "Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring", (2016) 93(2) *Journalism & Mass Communication* Q 296 <http://journals.sagepub.com/doi/pdf/10.1177/1077699016630255>.

[53] *Ibid.*

[54] PEN America (2017), "Chilling Effects: NSA Surveillance Drives U.S. Writers to Self-Censor," (12 November 2017) <https://pen.org/sites/default/files/Chilling%20Effects_PEN%20American.pdf>.

[55] Centre for Free Expression, Ryerson University in collaboration with PEN Canada and the Canadian Association of Journalists (2016), "Chilling Free Expression in Canada: Canadian Writers' and Journalists' Views on Mass Surveillance" (November 2016) <https://cfe.ryerson.ca/sites/default/files/Chilling_Free_Expression_in_Canada_FINAL_NOV_9_2016.pdf>.

[56] Human Rights Watch and the American Civil Liberties Union (2014), "With Liberty to Monitor All: How Large-ScaleU.S.Surveillance is Harming Journalism, Law, and American Democracy" (July 2014) <https://www.hrw.org/report/2014/07/28/liberty-monitor-all/how-large-scale-us-surveillance-harming-journalism-law-and>.

[57] See e.g., *R. v. Vice Media Canada Inc.*, 2017 ONCA 231 [leave to appeal to the Supreme Court of Canada granted, SCC File No. 37574].

[58] Québec (2017), Commission d'enquête sur la protection de la confidentialité des sources journalistiques, "Report Overview", (Québec: Gouvernement du Québec, 2017) <https://www.cepcsj.gouv.qc.ca/fileadmin/documents_client/documents/CEPCSJ_Synthese-ANG_Accessible_2017-12-14.pdf >.

into police "leaks," journalists were systematically tracked through access to cell tower location data and call logs in a manner that exhibited a "lack of sensitivity [that] is especially relevant to journalists' work in collecting information and protecting their sources."[59] The use of encrypted communication tools allow journalists to interact with their sources in ways that are less likely to expose the content of their communications, and the use of anonymity tools can help to protect source identities.

Encryption is also integral to the work of human rights activists and other individuals working to hold governments accountable, who frequently face heightened surveillance risks. The targeting of encryption and anonymity tools by authoritarian governments during periods of social and political unrest has become an increasingly commonplace tactic to undermine freedom of expression, assembly, and peaceful protest.[60] Device encryption allows human rights advocates to bring potentially sensitive data with them as they travel, including sensitive data that is vital to their advocacy missions.[61] The ability to properly secure devices and accounts can prevent regimes with problematic human rights records from compromising the devices of human rights activists, or from impersonating their owners in order to discredit them.[62] In this manner, encryption operates as an important counterweight to persecution in repressive regimes. As UN Human Rights Commissioner Zeid Ra'ad Al Hussein has eloquently articulated, compelling companies to undermine encryption can threaten lives:

> "In order to address a security-related issue related to encryption in one case [*referring to the Apple v FBI dispute*], the authorities risk unlocking a Pandora's Box that could have extremely damaging implications for the human rights of many millions of people, including their physical and financial security … this case is not about a company – and its supporters -- seeking to protect criminals and terrorists, it is about where a key red line necessary to safeguard all of us from criminals and repression should be set. …
>
> A successful case against Apple in the US will set a precedent that may make it impossible for Apple or any other major international IT company to safeguard their clients' privacy anywhere in the world. … It is potentially a gift to authoritarian regimes, as well as to criminal hackers. There have already been a number of concerted efforts by authorities in other States to force IT and communications companies such as Google and Blackberry to expose their customers to mass surveillance. …
>
> Encryption tools are widely used around the world, including by human rights defenders, civil society, journalists, whistle-blowers and political dissidents facing persecution and harassment… It is neither fanciful nor an exaggeration to say that, without encryption tools, lives may be endangered. In the worst cases, a Government's ability to break into its citizens' phones may lead to the persecution of individuals who are simply exercising their fundamental human rights."[63]

Encryption and anonymity tools also help to protect the speech and participation of vulnerable and marginalized groups who, by virtue of their identity or social status, are more likely to be subject to certain kinds of scrutiny (whether by governments or their more immediate communities).[64] Research demonstrates that women and young people are disproportionately impacted by the chilling effect of online surveillance, feeling greater pressure to self-censor and self-regulate online.[65] State-level

---

[59] *Ibid.*

[60] David Kaye (2015), Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/29/32, 29th session of the Human Rights Council <http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/Pages/ListReports.aspx> at 18.

[61] Ewen MacAskill (2017), "Campaign group to challenge UK over surrender of passwords at border control", *The Guardian* (14 May 2017) <https://www.theguardian.com/politics/2017/may/14/campaign-group-to-challenge-uk-over-surrender-of-passwords-at-border-control>; Interview with Muhammed Rabbani (International Director), "The Law is not correct about passwords", *CAGE*, available on Youtube: <https://www.youtube.com/watch?time_continue=16&v=CV32H8lxQjk>.

[62] Amar Toor & Russell Brandom (2015), "A Spy in the Machine", *The Verge* (21 January 2015) <https://www.theverge.com/2015/1/21/7861645/finfisher-spyware-let-bahrain-government-hack-political-activist>.

[63] United Nations (2016), Office of the High Commissioner for Human Rights, "Apple-FBI Case Could Have Serious Global Ramifications for Human Rights: Zeid", *Media Release* (4 March 2016) <http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=17138#sthash.o25R7Bqg.dpuf>.

[64] Elizabeth Stoycheff (2016), "Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring", (2016) 93(2) *Journalism & Mass Communication* Q 296 <http://journals.sagepub.com/doi/pdf/10.1177/1077699016630255>.

[65] See Jon Penney (2017), "Internet Surveillance, Regulation, and Chilling Effects Online: A Comparative Case Study", *Internet Policy Review*, 2017 <https://ssrn.com/abstract=2959611>.

adversaries are not the only threats to participation and free expression online. Online abuse of women and girls has been consistently recognized as a growing concern by international human rights bodies[66] and has been made only more urgent as technology enables new forms of gender-based harassment and domestic partner violence.[67] As a recent report by the UN Educational, Scientific and Cultural Organisation (UNESCO) has noted, "much of the debate about encryption has, until now, been gender-blind, or perhaps worse, male-dominated," despite the fact that women and girls experience both disproportionate and qualitatively distinct threats to their privacy, security, dignity, and ability to participate fully in the online sphere.[68] Similarly, members of sexual minorities may be reluctant to participate fully online if the security of their communications and activity records are perceived to put them at greater risk.[69] Encryption technology fosters the security necessary for meaningful inclusion, democratic engagement, and equal access to participation in the digital sphere without fear of arbitrary and unjust surveillance.[70] These secure communications tools enable individuals with similar interests or experiences (such as medical conditions, religious beliefs, or sexual orientations) to communicate while otherwise maintaining the confidentiality of information. Encryption ensures the security of the technical infrastructure, which in turn acts as a guarantor of the social trust and/or the legal obligations that exist within the community. This principle, that encryption acts as a technological guardian of trusted relationships, is of paramount importance to all vulnerable populations and all those who work with them.

B. ENCRYPTION IS A CORNERSTONE OF ELECTRONIC COMMERCE

Encryption provides critical protection for sensitive industrial information, trade secrets, and other kinds of intellectual property, while enabling digital commerce by facilitating secure online transactions and trust in online services. From processing online payments to managing vast databases of sensitive and private user data, most of the activities conducted by the private sector online require encryption to function safely. Efforts to weaken or limit the use of encryption increases the potential attack surface in each of these cases, and could expose highly sensitive and potentially valuable information to access by unauthorized parties.

Industry actors have been strong opponents of government attempts to limit or control the use or development of cryptographic tools on the basis that weakening encryption also jeopardizes these companies' abilities to maintain consumer trust and to compete internationally.[71] Indeed, even the perception that communications tools are compromised by government actors can have a significant impact on commercial interests. Following the Snowden revelations, American companies experienced considerable economic blowback as consumers sought alternatives to what were perceived to be insecure tools.[72] By weakening the security of technical systems or undermining the use of strong encryption, governments risk eroding trust in domestic software and reducing the competitiveness of these less secure products in a globalized marketplace.

Robust encryption is not only important to the competitiveness of customer-facing technological products—it is also critical to securing e-commerce platforms themselves. Cybersecurity breaches are increasingly frequent, with 29% of respondent businesses reporting the loss or damage of internal records as a result of a security incident in one 2018 survey of executives from 122 countries.[73] Consumer trust is also fading: only 25% of consumer respondents to a 2017 survey indicated that they believe most companies handle their personal data responsibly, while 85% of respondents indicated they would not do business with a

---

[66] See Dubravka Šimonović (2016), Special Rapporteur on violence against women, its causes and consequences, Report of the Special Rapporteur (A/HRC/32/42) Human Rights Council, Thirty-second session, United Nations General Assembly (19 April 2016) <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G16/080/53/PDF/G1608053.pdf?OpenElement> at 18 et seq.

[67] Citizen Lab (Munk School of Global Affairs, University of Toronto) (2017), Submission to the United Nations Special Rapporteur on violence against women, its causes and consequences, Ms. Dubravka Šimonović (November 2017) <https://citizenlab.ca/wp-content/uploads/2017/11/Final-UNSRVAG-CitizenLab.pdf>, in particular at 7-10.

[68] Wolfgang Schulz & Joris van Hoboken (2016), "Human Rights and Encryption," UNESCO Series on Internet Freedom <http://unesdoc.unesco.org/images/0024/002465/246527E.pdf> at 13.

[69] For a qualitative study of this issue see Sarah Jamie Lewis, *Queer Privacy: Essays from the Margins of Society* (Leanpub: 2017) <https://leanpub.com/queerprivacy>.

[70] Christopher Parsons (2015), "Beyond Privacy: Articulating the Broader Harms of Pervasive Mass Surveillance," (2015) *Media and Communication* 3(3).

[71] See Open Letter to President Obama on Encryption Policy (19 May 2015) <https://cdn.arstechnica.net/wp-content/uploads/2015/05/cryptoletter.pdf>.

[72] Claire Cain Miller (2014), "Revelations of N.S.A. Spying Cost U.S. Tech Companies," *New York Times* (21 March 2014) <https://www.nytimes.com/2014/03/22/business/fallout-from-snowden-hurting-bottom-line-of-tech-companies.html>.

[73] PwC (2017), "The Global State of Information Security Survey 2018," *PwC Reports* <https://www.pwc.com/us/en/cybersecurity/information-security-survey.html>.

company if they have concerns over the company's security practices.[74] In an era that has become characterized by high profile data breaches, undermining the overall strength of encryption technologies will only serve to further undermine attempts to secure e-commerce platforms.

Finally, it should be noted that private companies operate under a global responsibility "to avoid causing or contributing to adverse human rights impacts through their own activities" per the United Nations *Guiding Principles on Business and Human Rights.*[75] These principles make clear that companies have a responsibility to respect human rights—one that is independent of a given states' willingness to fulfill its own human rights obligations.[76] Private actors therefore face difficult legal and ethical dilemmas when they are asked to jeopardize user rights in the service of government demands for greater surveillance and law enforcement capabilities. At minimum, they must consider the domestic and international impact on human rights that might result from a decision to forgo effective encryption techniques or to otherwise undermine the security of consumer technology.

C. ENCRYPTION SAFEGUARDS PUBLIC SAFETY & NATIONAL SECURITY

While most policy debates related to digital surveillance have been divisive amongst stakeholders, determining the appropriate role of encryption has led to deep internal divisions amongst law enforcement and intelligence agencies as well. Encryption shields sensitive government data, preserves the confidentiality of law enforcement and intelligence investigations, and is an essential technology for military intelligence and communications. It protects the integrity of critical national infrastructure from malicious intrusion, including everything from telecommunications and transportation systems to financial services and the energy sector. As electoral processes are increasingly digitalized, weak information security becomes an existential threat to the democratic process. Encryption also protects confidential government information that could detrimentally affect the Canadian government's ability to conduct its domestic and international affairs if revealed. This includes protected and confidential information used by members of Parliament, civil servants, and diplomats, which could be used to weaken their ability to represent constituents, direct the functions of government, or advance Canada's interests abroad.

The importance of strong encryption to national security and public safety has been recognized by all manner of deliberative councils, advisory agencies, and legislative bodies in several countries. In late 2013, the United States President's Review Group on Intelligence and Communications Technologies recommended that the U.S. Government should "(1) fully support and not undermine efforts to create encryption standards; (2) not in any way subvert, undermine, weaken or make vulnerable generally available commercial software; and (3) increase the use of encryption and urge US companies to do so, in order to better protect data in transit, at rest, in the cloud, and in other storage."[77] In 2016 a Congressional Working Group on encryption affirmed the need to protect encryption, recognizing that while there is no "'one-size-fits-all' answer" to the investigative challenges it raises, the technology remains essential for national security, defence, and the protection of vital assets.[78] Leaders from the intelligence community which have opposed measures to weaken encryption have included, for example, the former Director of the Central Intelligence Agency (CIA) and former Director of the NSA Michael Hayden, the former United States Secretary of Homeland Security Michael Chertoff, the former Director of the Government Communications Headquarters (GCHQ) Robert Hannigan, and the former Director-General of the British Security Service (MI5) Jonathan Evans.[79]

---

[74] PwC (2017), "Consumer Intelligence Series: protect.me," *PwC Reports* <https://www.pwc.com/us/en/advisory-services/publications/consumer-intelligence-series/protect-me/cis-protect-me-findings.pdf>.

[75] United Nations Human Rights Office of the High Commissioner (2011), "Guiding Principles on Businesses and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework", (New York and Geneva, 2011) <http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf> [also available as A/ HRC/17/31] at 14.

[76] *Ibid*.

[77] United States (2013), President's Review Group on Intelligence and Communications Technologies, "Liberty and Security in a Changing World: Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies", (12 December 2013) <https://www.propublica.org/documents/item/930409-2013-12-12-rg-final-report-on-nsa> recommendation 29 at 38.

[78] House Judiciary Committee and House Energy and Commerce Committee Encryption Working Group (2016), "Encryption Working Group Year-End Report", (20 December 2016) <https://judiciary.house.gov/wp-content/uploads/2016/12/20161220EWGFINALReport.pdf> at 4.

[79] Paul Szoldra (2016), "Ex-NSA chief thinks the government is dead wrong in asking Apple for a backdoor", *Business Insider* (25 February 2016) <http://www.businessinsider.com/michael-hayden-encryption-apple-2016-2>; Conor Friedersdorf (2015), "Former National-Security Officials Now See the Peril of Weakening Encryption", *The Atlantic* (30 July 2015) <https://www.theatlantic.com/politics/archive/2015/07/former-national-security-officials-see-the-peril-of-weakening-encryption/399848/>; John Leyden (2017), "Former GCHQ boss backs end-to-end encryption", *The Register* (10 July 2017) <https://www.theregister.co.uk/2017/07/10/former_gchq_wades_into_encryption_debate/>; Jamie Grierson (2017), "Ex-MI5 chief warns against crackdown on encrypted messaging apps", *The Guardian* (11 August 2017) <https://www.theguardian.com/technology/2017/aug/11/ex-mi5-chief-warns-against-crackdown-encrypted-messaging-apps>.

Other states have come to similar conclusions. In 2016 the Dutch government officially endorsed the importance of strong encryption for Internet security.[80] The German government's National Cybersecurity Strategy (2016) reaffirms the country's longstanding commitment to the development and protection of strong encryption tools.[81] In 2016, Europol and the European Union Agency for Network and Information Security (ENISA) issued a joint statement on encryption, which rejected any approach that would weaken encryption standards or the integrity of communications.[82] In June 2017, the European Union Parliament's Committee on Civil Liberties, Justice and Home Affairs made recommendations that would actively promote the use of end-to-end encryption, and which would specifically forbid the implementation of "backdoor" systems in tools developed by electronic communications services providers.[83]

Because encryption is at the core of security for consumer electronic devices, digital storage, and communications software, it is also a major tool for crime prevention. Weak end-point security (e.g., the lack of effective full disk encryption on mobile devices or laptops) heightens incentives for theft of electronic devices and the data stored therein. An internal U.S. National Intelligence Council report released as part of the Snowden documents recognizes the critical importance of encryption in this context, noting that "[a]lmost all current and potential adversaries—nations, criminal groups, terrorists, and individual hackers—now have the capability to exploit, and in some cases attack, unclassified access-controlled U.S. and allied information systems."[84] The 2009 report attributed the ever-increasing cost of espionage, sabotage and crime "to the slower than expected adoption … of encryption and other technologies."[85]

The introduction of encryption backdoors or other weaknesses into commercially available encryption technology necessarily increases system complexity and the opportunity for exploitation by criminals, leaving the technology more vulnerable to exploitation by malicious actors. Such vulnerabilities may in turn increase various forms of online crime, including identity theft, ransom, and fraud. In taking over vulnerable systems, malicious actors can also potentially access sensitive personal information, financial records, account credentials, and intimate files and photographs. It is important to recall that encryption protects information that is entirely legal but which may be nonetheless embarrassing or damaging were it to be made public, such as romantic liaisons, healthcare challenges, religious activities, or sexual proclivities. Not only can this data be exploited for illicit financial gain, but also to manipulate, monitor, blackmail, harass, and humiliate vulnerable individuals—for example, by enabling domestic partner violence through the proliferation of "stalkerware" or by facilitating financial exploitation

---

[80] Ministry of Security and Justice (Netherlands) (2016), "Cabinet's view on encryption", (4 January 2016) <https://www.enisa.europa.eu/about-enisa/structure-organization/national-liaison-office/news-from-the-member-states/nl-cabinet-position-on-encryption>; Robert Hackett (2016), "Dutch Government Backs Uncrackable Encryption", *Fortune* (6 January 2016) <http://fortune.com/2016/01/05/dutch-government-encryption-no-backdoors/>, translating Government of the Netherlands, "Kabinetsstandpunt encryptie", Cabinet Position on Encryption (4 January 2016) <https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2016Z00009&did=2016D00015>:

> "The government believes that it is not desirable at this time to take restrictive regulatory measures with respect to the development, availability, and use of encryption within the Netherlands."

[81] Sven Herpig and Stefan Heumann (2017), "Germany's Crypto Past and Hacking Future", *Lawfare* (13 April 2017) <https://www.lawfareblog.com/germanys-crypto-past-and-hacking-future>; Cybersecurity Strategy for Germany (CyberSicherheits strategie für Deutschland) (2016) <https://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/ModerneVerwaltung-OeffentlicherDienst/Informationsgesellschaft/cybersicherheitsstrategie-2016.html>.

[82] Europol and the European Union Agency for Network and Information Security (2016), "Joint Statement on lawful criminal investigation that respects 21st century data protection", (20 May, 2016) <https://www.europol.europa.eu/publications-documents/lawful-criminal-investigation-respects-21st-century-data-protection-europol-and-enisa-joint-statement-0> at 1—2.

[83] See European Parliament, Committee on Civil Liberties, Justice and Home Affairs, 2017/0003(COD), "Draft report on the proposal for a regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)", <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2F%2FEP%2F%2FNONSGML%2BCOMPARL%2BPE-606.011%2B01%2BDOC%2BPDF%2BV0%2F%2FEN> at Amendment 116, Proposal for a regulation, Article 17 – paragraph 1 a (new):

> "The providers of electronic communications services shall ensure that there is sufficient protection in place against unauthorised access or alterations to the electronic communications data, and that the confidentiality and safety of the transmission are also guaranteed by the nature of the means of transmission used or by state-of-the-art end-to-end encryption of the electronic communications data. Furthermore, when encryption of electronic communications data is used, decryption, reverse engineering or monitoring of such communications shall be prohibited. Member States shall not impose any obligations on electronic communications service providers that would result in the weakening of the security and encryption of their networks and services."

[84] James Ball (2015), "Secret US cybersecurity report: encryption vital to protect private data", *The Guardian* (16 January 2015) <https://www.theguardian.com/us-news/2015/jan/15/-sp-secret-us-cybersecurity-report-encryption-protect- data-cameron-paris-attacks>.

[85] *Ibid*.

using "sextortion" techniques.[86] In short, calls to undermine encryption tools by law enforcement and the intelligence community may result in an increase to online crime rather than serve to prevent it.

In addition to undermining national security and public safety, efforts to undermine encryption technology may also run counter to Canada's foreign policy interests—including its ability to take a leadership role in the promotion of global security and human rights internationally. Even former FBI Director James Comey (a strong proponent of policy measures which would undermine encryption) recognized this problem in a 2015 speech:

> "It is also true that other countries—particularly those without our commitment to the rule of law—are using this [encryption] debate as a cynical means to create trade barriers, impose undue burdens on our companies, and undermine human rights. We should be clear that any steps that we take here in the United States may impact the decisions that other nations take—both our closest democratic allies and more repressive regimes."[87]

This type of concern arose in Canada[88] and the United States[89] when export restrictions to Iran limited Iranian citizens' ability to rely on encryption and security tools while participating in democratic uprisings. The decision to adopt exceptions to sanction regimes in order to promote the use of encryption technologies and other security tools highlights their role in Canada's foreign policy agenda.

Weakening encryption can also have negative implications for law enforcement and intelligence-gathering efforts. To begin with, law enforcement agencies use encryption and anonymity tools in their investigative efforts, such as when they attempt to access target websites or chat platforms undercover, or when hosting truly anonymous tip lines.[90] Restrictions on encryption would undermine law enforcement's ability to conduct such activities securely. Restricting encryption could also push secure communication providers to foreign states, thus impeding the ability of domestic agencies to access unencrypted data held by that company:

> "Law enforcement stakeholders acknowledged … that a Congressional mandate with respect to encryption—requiring companies to maintain exceptional access to data for law enforcement agencies, for example—would apply only to companies within the United States. … These forces

---

[86] For an exploration of the relationship between encryption and the prevention of gender-based violence, see Citizen Lab (Munk School of Global Affairs, University of Toronto) (2017), Submission to the United Nations Special Rapporteur on violence against women, its causes and consequences, Ms. Dubravka Šimonović (November 2017) <https://citizenlab.ca/wp-content/uploads/2017/11/Final-UNSRVAG-CitizenLab.pdf> in particular at 7-10.

[87] United States Department of Justice (2015), "Deputy Attorney General Sally Quillian Yates and FBI Director James B. Comey Deliver Statement Before the Senate Judiciary Committee", (8 July 2015) <https://www.justice.gov/opa/ speech/deputy-attorney-general-sally-quillian-yates-and-fbi-director-james-b-comey-deliver>.

[88] Government of Canada (2013), Department of Foreign Affairs and International Trade Canada, "Canada Further Tightens Sanctions on Iran—Backgrounder", *Foreign Affairs Media Relations Office* (29 May 2013), <https://www.canada.ca/en/news/archive/2013/05/canada-further-tightens-sanctions-iran.html>:

> "Canada's new sanctions include exemptions for technologies that protect Iranians online and help them break through the regime's curtain of propaganda."

See also Government of Canada (2013), "Regulations Amending the Special Economic Measures (Iran) Regulations", PC 2013-599, SOR/2013-108 (29 May 2013) <http://gazette.gc.ca/rp-pr/p2/2013/2013-06-19/html/sor-dors108-eng.html>:

> "an exemption aimed at increasing the availability of consumer communication technologies that contribute to Internet freedom" and clause 5 amending section 8.1(a) of the Regulations, exempting: "equipment, services and software that facilitate secure and widespread communications via information technologies, or the provision or acquisition of financial services in relation to such equipment, services and software, provided that an export permit has been issued in respect of any goods listed in the Guide".

[89] United States, Department of the Treasury (2013), "United States Takes Action to Facilitate Communications by the Iranian People and Targets Iranian Government Censorship", *Press Center* (30 May 2013), <https://www.treasury.gov/press-center/press-releases/Pages/jl1961.aspx>:

> "As the Iranian government attempts to silence its people by cutting off their communication with each other and the rest of the world, the United States will continue to take action to help the Iranian people exercise their universal human rights, including the right to freedom of expression. The people of Iran should be able to communicate and access information without being subject to reprisals by their government. To help facilitate the free flow of information in Iran and with Iranians, The U.S. Department of the Treasury, in consultation with the U.S. Department of State, is issuing a General License today authorizing the exportation to Iran of certain services, software, and hardware incident to personal communications."

See also: Center for Democracy and Technology (2013), "Administration Promotes Internet Freedom in Iran with Smarter Sanctions", *cdt.org* (5 June 2013) <https://cdt.org/blog/administration-promotes-internet-freedom-in-iran-with-smarter-sanctions/>.

[90] See e.g., The Tor Project (2018), "Users of Tor", <https://www.torproject.org/about/torusers.html.en>; See also Roger Dingledine, "Anti-Censorship & Transparency," *IIS* (26 October 2010) Från Internetdagarna. Folkets Hus, Stockholm <https://youtu.be/35l56KjTCb8?t=1h25m20s>.

> might incentivize larger companies to leave the United States, and render small business and other innovators in the field obsolete. If a U.S.-based company moved operations to a country with a more favorable legal regime, the law enforcement and intelligence communities might lose access to everything in that company's holdings—encrypted or not."[91]

In this regard, regulation of encryption might not only fail to facilitate state access to digital evidence and intelligence by encouraging developers to migrate abroad, but may also directly impair important investigative techniques.

[91] House Judiciary Committee and House Energy and Commerce Committee Encryption Working Group (2016), "Encryption Working Group Year-End Report", (20 December 2016) <https://judiciary.house.gov/wp-content/uploads/2016/12/20161220EWGFINALReport.pdf> at 5.

PART 3: GOING DARK? FOUR DECADES OF DEBATE

"Encryption works. Properly implemented strong crypto systems are one of the few things that you can rely on."

— Edward Snowden[92]

Even highly sophisticated and well-resourced adversaries—including signals intelligence agencies such as the United States' National Security Agency (NSA) and Canada's Communications Security Establishment (CSE)—do not have the power to decrypt messages encrypted with most modern algorithms without the right keys. While future developments may change this dynamic, in our current technological context this means that at least some information can be kept secure from state actors indefinitely. The availability of encryption for securing electronic communications, data, and devices has proliferated rapidly in recent years—and particularly following the 2013 Snowden revelations. As a result, certain types of data which were previously available to law enforcement and intelligence agencies in plaintext form are increasingly encrypted at the moment of interception or seizure. This has led some state officials and investigative agencies to treat encryption technology as an obstacle to be regulated and constrained. Calls for exceptional access to encrypted data are often framed around the colloquial shorthand "going dark" to reflect the notion that previously available communications are becoming unavailable to state investigators as a result of encryption. Some of these exceptional access proposals run contrary to past (or even current) government policy, on the basis that many state officials and agencies recognize the central importance of robust cryptographic tools for their own activities.

In this section, we briefly outline the early historical debates around encryption and their relationship to present-day controversies. The focus in this section is on the historical progression of this policy arena over time and the different types of controls employed or proposed. We generally do not evaluate the feasibility, proportionality, or lawfulness of these proposals in this section—those issues are instead addressed in Part 4.

A. AN ERA OF STRICT ENCRYPTION CONTROL (PRE-1990S)

Prior to the 1990s, state agencies maintained strict control over the development, availability, and use of cryptographic tools, using a range of measures designed to prevent the broad non-military/intelligence adoption of strong encryption. For example, in the United States the NSA created internal and semi-external think tanks to attract leading U.S. cryptographers, and then classified their work so that it would not become publicly available.[93] In effect, intelligence agencies controlled cryptography by having "the only reservoir of expertise in the field."[94] Control over substantial research funding was another tool used by intelligence agencies in this era to guide research, shape development, and limit access to the technology.

i. Strict Control and Closed Door Controversies

In this era, various agencies also began relying on their ability to apply political pressure to limit the wider commercial availability of encryption—debates over the strength and scope of encryption tools remained largely contained to government agencies and the technical community. For example, in the early 1980s, a controversy arose as to whether robust encryption should be adopted into a new standard for mobile communications (i.e., the debate surrounding A5/1 encryption, which was to be included in the mobile GSM standard). Political pressure from intelligence agencies within some NATO governments (primarily France and the United Kingdom, it appears, with German agencies opposing) led to a rejection of the stronger 128-bit key length

---

[92] Glenn Greenwald (2013), "Edward Snowden: NSA whistleblower answers reader questions", (17 June 2013) *The Guardian* <https://www.theguardian.com/world/2013/jun/17/edward-snowden-nsa-files-whistleblower>.

[93] Michael Schwartzbeck (circa 1997), "The Evolution of US Government Restrictions on Using and Exporting Encryption Technologies", *Central Intelligence Agency*, (Unclassified for Release: 2014/09/10) <https://www.cia.gov/library/readingroom/docs/DOC_0006231614.pdf>.

[94] James Bamford (1982), *The Puzzle Palace: Inside the National Security Agency, America's Most Secret Intelligence Organization* (Penguin: 1982) <https://cryptome.org/nsa-v-all.htm>.

proposed by the technical and corporate community, which led to the ultimate adoption of a much shorter key length.[95] The debate was secret and only mentioned in public over a decade later—it has since been confirmed that the NSA had the capability break the resulting encryption.[96] Similarly, when IBM created a strong 128-bit encryption system (called "Lucifer") for commercial use, the company was convinced by the NSA in closed-door discussions to reduce the key size (this time to 56 bits) for what ultimately became the predominant non-military cryptographic system of the era, the Data Encryption Standard (DES).[97]

ii. Export Controls and the Intelligence-Military Mindset

Near the end of this period, cryptographic standards began to emerge from divergent non-military sources, and governments began to rely on legal recourse intended to protect weapons (generally in the form of export controls) as a way to discourage and prevent the publication of strong encryption systems by the academic community and private sector.[98] For example, a full decade after the adoption of A5/1 encryption in mobile communications, standards bodies were called upon to develop an even *weaker* encryption algorithm (A5/2) for mobile devices being exported outside of Europe on the basis that the key size used in A5/1 was too large to comply with export restrictions.[99] The A5/2 algorithm was not only shown to be breakable in real-time[100] but it could be used to compromise other, more effective encryption (i.e., A5/1 and, later, A5/3) used by the same device.[101] Finally, a series of directives were issued in the mid-1980s that explicitly gave the NSA control over technology for safeguarding sensitive government information, which effectively granted the agency responsibility for certifying encryption standards.[102] This elicited a strong adverse public reaction from civil society and the technical community, and was viewed as an assertion of control by the NSA—a military agency with a history of hostility towards strong commercial cryptography—over an increasingly important class of technologies. This tension led to the adoption of the *Computer Security Act of 1987* in the United States, a law which sought to enshrine the National Institute for Standards and Technology (NIST), a division of the Department of Commerce, as the primary authority responsible for standardizing information security technologies.[103]

---

[95] Arild Faeraas (2014), "Sources: We Were Pressured to Weaken the Mobile Security in the 80's" *Aftenposten* (9 January 2014) <https://www.aftenposten.no/verden/i/Olkl/Sources-We-were-pressured-to-weaken-the-mobile-security-in-the-80s>: The A5/1 algorithm allowed for 64 bit key lengths, but the last 10 bits were secretly and arbitrarily set to '0' in all keys, reducing the effective key length to 54 bits. See also Marc Briceno, Ian Goldberg & David Wagner (1998), "A Pedagogical Implementation of A5/1", *Smartcard Developer Association* <http://www.scard.org/gsm/a51.html>.

[96] Ross Anderson (1994), "A5 (Was: HACKING DIGITAL PHONES)", *Newsgroups: sci.crypt*, *alt.security*, *uk.telecom* (17 June 1994) <https://groups.google.com/forum/#!msg/uk.telecom/TkdCaytoeU4/Mroy719hdroJ> and Snowden Archive, "C3: (TS//SI)" <https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASH013d/c4c6e608.dir/doc.pdf>,

[97] James Bamford (1982), *The Puzzle Palace: Inside the National Security Agency, America's Most Secret Intelligence Organization*, (Penguin: 1982) <https://cryptome.org/nsa-v-all.htm>; Arthur Sorkin (1984), "Lucifer, A Cryptographic Algorithm", 8(1) *Cryptologia* 22 <https://dx.doi.org/10.1080/0161-118491858746>: Danielle Kehl, Andi Wilson, and Kevin Bankston (2015), "Doomed to Repeat History? Lessons from the Crypto Wars of the 1990s", New America Open Technology Institute <https://www.newamerica.org/cybersecurity-initiative/policy-papers/doomed-to-repeat-history-lessons-from-the-crypto-wars-of-the-1990s/> at footnote 45.

[98] James Bamford (1982), *The Puzzle Palace: Inside the National Security Agency, America's Most Secret Intelligence Organization*, (Penguin: 1982) <https://cryptome.org/nsa-v-all.htm>; *Bernstein v Department of Justice*, 945 F.Supp. 1279 (1996, US Dist Ct, ND, Calif); aff'd 176 F.3d 1132 (1999, US 9th Circuit); See also Michael Schwartzbeck (circa 1997), "The Evolution of US Government Restrictions on Using and Exporting Encryption Technologies", *Central Intelligence Agency* (Unclassified for Release: 2014/09/10) <https://www.cia.gov/library/readingroom/docs/DOC_0006231614.pdf>.

[99] Elad Barkan, Eli Biham, and Nathan Keller (2006), "Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication", Technion - Computer Science Department Technical Report CS-2006-07-2006 <http://www.cs.technion.ac.il/users/wwwb/cgi-bin/tr-get.cgi/2006/CS/CS-2006-07.pdf>.

[100] Ian Goldberg, David Wagner & Lucky Green (1999), "The (Real-Time) Cryptanalysis of A5/2", *Rump Session of Crypto'99*.

[101] 3GPP (2003), "Implications of the A5/2 Attack for 3GPP WLAN Access", 3GPP TSG SA WG3 Security (November 2003) <ftp://www.3gpp.org/tsg_sa/WG3_Security/TSGS3_31_Munich/Docs/PDF/S3-030733.pdf>. As a result, standards organizations eventually withdrew the A5/2 encryption algorithm and prohibited its use in mobile devices. However, this transition was slow, leaving mobile devices vulnerable for over two decades from its adoption in the late 1980s to its eventual withdrawal in 2007.

See also Technical Specification Group Services and System Aspects; Security Related Network Functions, Rel 4, 3GPP TS 43.020 v4.4.0 (Sept 2007) <http://www.3gpp.org/ftp/Specs/archive/43_series/43.020/43020-440.zip> [ZIP]:

> "It is mandatory for A5/1 and non encrypted mode to be implemented in mobile stations. It is prohibited to implement A5/2 in mobile stations."

[102] Electronic Privacy Information Center, "Computer Security Act of 1987" <https://www.epic.org/crypto/csa/>.

[103] The newly emergent predominance of NIST was rapidly undermined by a Memorandum of Understanding between NIST and the NSA, which entrusted cryptography to a joint working group co-hosted by the two entities but seemingly led by the NSA.

See Electronic Privacy Information Center, "Computer Security Act of 1987" <https://www.epic.org/crypto/csa/>; Clinton Brooks, Special Assistant to the Director, National Security Agency, "Memorandum on NSDD-145 and the Computer Security Act", <https://www.epic.org/crypto/csa/brooks.gif>.

B. CRYPTO WARS 1: THE ROAD TO LIBERALIZATION (1990-2000)

Beginning in the early 1990s, cryptography emerged as a central and hotly contested policy issue as public demand for strong encryption grew alongside the widespread adoption of the Internet. The ascendant control exerted by intelligence agencies (and particularly by the NSA) over public access to cryptography could not be sustained in the face of demonstrable need to secure information more broadly.[104] While governments acknowledged this need, they remained unwilling to allow greater user security to impact on their own surveillance capabilities, which, in turn, led to an era where various proposals sought to create some form of hybrid solution that reconciled investigative and cybersecurity objectives. This period of time is often referred to as the "Crypto Wars." Over this period, law enforcement agencies in Canada mirrored American calls for some form of exceptional access that would let them bypass strong cryptographic protections,[105] and the Canadian government appears to have been initially supportive of efforts by the United States to adopt cryptography restrictions on the international stage.[106]

i. The Clipper Chip and the Push for Key Escrow

This era saw the development of the now infamous "Clipper Chip" through a hybrid working group run by the NSA and NIST in 1993.[107] The Clipper Chip, a cryptographic chipset, would have allowed devices on which it was installed to use SKIPJACK, the most robust encryption algorithm sanctioned by the U.S. government at that time. The algorithm used what appeared to be sound cryptographic principles[108] and 80-bit key lengths when, to date, the United States had otherwise largely succeeded in limiting key lengths to 56-bits.[109] However, the U.S. government also planned to retain a copy of a secret, device-specific encryption key associated with each and every Clipper chip in escrow, giving law enforcement and intelligence agencies the ability to decrypt traffic.[110] Whenever a Clipper Chip established a connection, it transmitted a "Law Enforcement Access Field" (LEAF) which included the particular chip's Unique Identifier as well as a copy of the session key used to encrypt the specific communication.[111] While measures were put in place to protect interference with the LEAF, security researchers discovered significant systemic flaws.[112]

---

[104] Michael Schwartzbeck (circa 1997), "The Evolution of US Government Restrictions on Using and Exporting Encryption Technologies", *Central Intelligence Agency* (Unclassified for Release: 2014/09/10) <https://www.cia.gov/library/readingroom/docs/DOC_0006231614.pdf> at 22—23.

[105] Brad Evenson (1996), "Going Cryptic on the Net", *The Ottawa Citizen* (23 August 1996) archived at: <http://www.efc.ca/pages/media/ottawa.citizen.23aug96.html>:

> "The RCMP and Canadian Association of Chiefs of Police want some kind of 'back door' that would allow them to decrypt telephone and e-mail communication they intercept by wiretapping."

[106] For example, Canadian representatives at the OECD were initially supportive of US efforts to advance a key escrow mandate in an instrument—the OECD Guidelines on Cryptography—that was being negotiated at the time. See Michael Schwartzbeck (circa 1997), "The Evolution of US Government Restrictions on Using and Exporting Encryption Technologies", *Central Intelligence Agency* (Unclassified for Release: 2014/09/10) <https://www.cia.gov/library/readingroom/docs/DOC_0006231614.pdf> at 27—28.

[107] This working group was established soon after the passing of the *Computer Security Act of 1987*, undermining Congress' attempt to establish NIST, a civilian agency, as the primary state authority on commercial encryption. See Electronic Privacy Information Center, "Computer Security Act of 1987" <https://www.epic.org/crypto/csa/>.

[108] However, concerns were raised that the SKIPJACK algorithm itself was kept secret and only subjected to cryptanalysis by a small and select group of independent cryptographers. As such, it was suspected that the algorithm's soundness was perhaps less than was concluded on the basis of this limited independent review. See Matt Blaze (1994), "Protocol Failure in the Escrowed Encryption Standard", (20 August 1994) <http://www.crypto.com/papers/eesproto.pdf>.

[109] DES, limited to 56 bit key lengths and described above, remained the prevalent encryption mechanism at the time.

Ernest F Brickel et al. (1993), "The SKIPJACK Algorithm", Interim Report (28 July 1993) <https://epic.org/crypto/clipper/skipjack_interim_review.html>; Danielle Kehl, Andi Wilson, and Kevin Bankston (2015), "Doomed to Repeat History? Lessons from the Crypto Wars of the 1990s", New America Open Technology Institute <https://static.newamerica.org/attachments/3407-doomed-to-repeat-history-lessons-from-the-crypto-wars-of-the-1990s/Crypto%20Wars_ReDo.7cb491837ac541709797bdf868d37f52.pdf> at footnote 45.

[110] FIPS 185 (1994), "Escrowed Encryption Standard" (9 February 1994, withdrawn 19 October 2015) <https://csrc.nist.gov/csrc/media/publications/fips/185/archive/1994-02-09/documents/fips185.pdf>.

[111] *Ibid.*; Matt Blaze (1994), "Protocol Failure in the Escrowed Encryption Standard", (20 August, 1994) <http://www.crypto.com/papers/eesproto.pdf>.

[112] *Ibid.*

The proposal was ultimately defeated as a result of sustained pressure from civil liberties organizations and in light of academic consensus that demonstrated that the escrow system left communications disproportionately vulnerable.[113] In the years that followed, the Clipper Chip was followed by a number of other failed efforts to mandate software key escrow or to impose obligations on service providers. These efforts were premised on the ideological position that strong cryptography should be made widely available, but only if government actors could have and maintain unrestricted access to data in its unencrypted form.[114]

At the same time, the use of export restrictions as a means of limiting the public adoption of strong cryptography became increasingly infeasible. A U.S. government lawsuit against cryptographer Phil Zimmerman (who created the PGP email encryption system) ultimately failed, on the finding that there was no connection between Zimmerman and the websites accused of "exporting" the encryption system by making it available online. Next, a security company formed by MIT academics (called RSA) began establishing subsidiary companies in other countries as a means to sell encryption technology abroad without running afoul of U.S. export restrictions. Both these efforts demonstrated that while export controls continued to operate as obstacles, the Internet and globalization were making them less capable of preventing commercially available public cryptography. Finally, an historic lawsuit was launched by the newly emergent Electronic Frontiers Foundation (EFF) on behalf of a PhD candidate who sought to publish his encryption software and research papers online. The EFF successfully argued that the U.S. export restrictions, as formulated, constituted an impermissible restraint on his freedom of speech by preventing him from publishing the research.[115]

ii. An International Move Toward Commercial Liberalization and Public Control

On the international stage, the United States attempted to advance its key escrow agenda through an Organisation for Economic Co-operation and Development (OECD) policy that was being developed on cryptography.[116] However, the ultimate recommendations adopted by the OECD emphasized the need to ensure that national restrictions on the use or dissemination of cryptography did not create obstacles to information and communication networks.[117] While the OECD recommendations accepted the possibility of lawful access mechanisms, including key escrow or other key recovery mechanisms, as legitimate options in national cryptography policies, the United States failed to convince other states to adopt *any* mandatory global lawful access requirement, let alone its preferred mechanism.[118] Instead, the OECD recommendations firmly established a model of

---

[113] AT&T was the only company that agreed to implement the Clipper chip and the company was subjected to heavy public criticism and planned boycotts for its decision to do so. See Michael Schwartzbeck, "The Evolution of US Government Restrictions on Using and Exporting Encryption Technologies", *Central Intelligence Agency* (circa 1997, Unclassified for Release: 2014/09/10) <https://www.cia.gov/library/readingroom/docs/DOC_0006231614.pdf> at 23.

See also Danielle Kehl, Andi Wilson, and Kevin Bankston (2015), "Doomed to Repeat History? Lessons from the Crypto Wars of the 1990s," *New America Open Technology Institute* <https://static.newamerica.org/attachments/3407-doomed-to-repeat-history-lessons-from-the-crypto-wars-of-the-1990s/Crypto%20Wars_ReDo.7cb491837ac541709797bdf868d37f52.pdf> at 7.

[114] *Ibid* at 9—11.

[115] *Bernstein v Department of Justice*, 922 F.Supp. 1426 (1996, ND Calif); *Bernstein v Department of Justice*, 945 F.Supp. 1279 (1996, ND Calif); aff'd 176 F.3d 1132 (1999, US 9th Circuit); See also Michael Schwartzbeck, "The Evolution of US Government Restrictions on Using and Exporting Encryption Technologies" (circa 1997), *Central Intelligence Agency* (Unclassified for Release: 2014/09/10) <https://www.cia.gov/library/readingroom/docs/DOC_0006231614.pdf>.

[116] *Ibid* at 27—28:

> "... David Aaron, US Special Envoy to the OECD, stated that important US allies support President Clinton's position that governments should be able to recover encryption keys when necessary", noting specifically that he had discussed cryptography issues with OECD representatives from France, the UK, Germany, Belgium and Canada."

See also Sarah Andrews (2000), "Who Holds the Key? A Comparative Study of US and European Encryption Policies", 2 *J of Information, L and Tech* <https://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2000_2/andrews/> at section 3.1.

[117] OECD Council Recommendation Concerning Guidelines for Cryptography Policy, C(97)62/FINAL (adopted 27 March 1997) <https://www.oecd.org/sti/ieconomy/guidelinesforcryptographypolicy.htm> at Annex: "Guidelines for Cryptography Policy".

[118] *Ibid* at Annex: "Guidelines for Cryptography Policy," Principle 6; Michael Schwartzbeck, "The Evolution of US Government Restrictions on Using and Exporting Encryption Technologies" (circa 1997), *Central Intelligence Agency* (Unclassified for Release: 2014/09/10) <https://www.cia.gov/library/readingroom/docs/DOC_0006231614.pdf> at 27—28.

The U.S. also failed in its efforts to encode key escrow systems as the primary permissible means of exporting strong cryptography when the Wasenaar Agreement on Export Controls for Dual-Use Goodes and Technologies and Conventional Arms was adopted in 1998. See Sarah Andrews (2000), "Who Holds the Key? A Comparative Study of US and European Encryption Policies", 2 *J of Information, L and Tech* <https://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2000_2/andrews/> at section 3.1 and 3.2.

civilian control of the development of cryptography[119] and required that any lawful access measures must respect privacy rights, user choice, and confidence in the integrity and confidentiality of information and communications systems.[120]

The OECD Cryptography Guidelines, in their final form, represented the culmination of a shift towards the liberalization of cryptography policy that took place in the United States and among allied states, including Canada. By late 1999, most OECD governments had recognized the need for strong commercial cryptography and many adopted national cryptography policies based on the OECD model.[121] The United States also appeared to finally abandon its plans for a key escrow system in late 1999, when it removed the remaining export restrictions that imposed a licensing requirement for cryptographic keys over 56 bits in length without a key recovery mechanism.[122] Some European countries, and the European Commission itself, adopted even stronger pro-cryptography positions, categorizing key escrow and related proposals as a threat to encryption in public communiqués and other statements.[123] While none of these positions were legally binding, they did signal a new direction in the approach taken to commercial cryptography by a number of states—evolving from one of open hostility, to grudging acceptance, to open recognition of the critical role encryption played in maintaining the integrity and security of public networks.

The United States also sought to advance its initially restrictive encryption policies through another international mechanism—the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Technologies and Goods. Prior to 1998, Participating States agreed to generally restrict the export of encryption technologies if an export permit was obtained, although Wassenaar did not generally impose specific conditions under which a state might refuse or grant a license.[124] Wassenaar also included an exemption for mass market and public domain software (contained in the General Software Note or GSN). Per the exemption, export permits were only required for hardware and customized software.[125] The Wassenaar agreement is not a treaty, however, and while Participating States are expected to adopt its provisions, the Arrangement is not directly binding.[126] In late 1998, licensing restrictions were wholly lifted for encryption products employing keys not exceeding 56 bits of

---

[119] OECD Council Recommendation Concerning Guidelines for Cryptography Policy, C(97)62/FINAL (adopted 27 March 1997) <https://www.oecd.org/sti/ieconomy/guidelinesforcryptographypolicy.htm> Principle 3:

> "The development and provision of cryptographic methods should be determined by the market in an open and competitive environment. Such an approach would best ensure that solutions keep pace with changing technology, the demands of users and evolving threats to information and communications systems security. The development of international technical standards, criteria and protocols related to cryptographic methods should also be market driven. Governments should encourage and co-operate with business and the research community in the development of cryptographic methods."

[120] *Ibid* at Principles 1, 2 and 5.

[121] W3C, Activities Related to the United States, "Framework for Global Electronic Commerce", <https://www.w3.org/TR/NOTE-framework-970706>.

[122] Peter Swire & Kenesa Ahmad (2012), "Encryption and Globalization", 23 *Columbia Sci & Tech L Rev* <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1960602> at 439—441; Danielle Kehl, Andi Wilson, and Kevin Bankston, "Doomed to Repeat History? Lessons from the Crypto Wars of the 1990s" (2015), *New America Open Technology Institute* <https://static.newamerica.org/attachments/3407-doomed-to-repeat-history-lessons-from-the-crypto-wars-of-the-1990s/Crypto%20Wars_ReDo.7cb491837ac541709797bdf868d37f52.pdf> at 15—17; Michael Schwartzbeck (circa 1997), "The Evolution of US Government Restrictions on Using and Exporting Encryption Technologies", *Central Intelligence Agency (*circa 1997, Unclassified for Release: 2014/09/10) <https://www.cia.gov/library/readingroom/docs/DOC_0006231614.pdf> at 2; Sarah Andrews (2000), "Who Holds the Key? A Comparative Study of US and European Encryption Policies", (2000) 2 *J of Information, L and Tech* <https://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2000_2/andrews/> at section 4.2.

[123] *Ibid* at section 5.2.

See also Sven Herpig and Stefan Heumann, "Germany's Crypto Past and Hacking Future" (2017), *Lawfare* (13 April 2017) <https://www.lawfareblog.com/germanys-crypto-past-and-hacking-future>. Germany adopted a national cryptography policy in 1999 that included the following core components:

> "1) There will be no ban or limitation on crypto products; 2) Crypto products shall be tested for their security in order to increase the user's trust in those products; 3) The development of crypto products by German manufacturers is essential for the country's security and their ability to compete internationally shall therefore be strengthened; 4) Law enforcement and security agencies shall not be weakened by the widespread use of encryption. The development of additional technical competencies for those agencies shall be fostered; 5) International cooperation on crypto issues such as open standards and interoperability is vital and shall be fostered bi- and multilaterally."

[124] Government of Canada (1998), "Discussion Paper: A Cryptography Policy Framework for Electronic Commerce—Building Canada's Information Economy and Society", *Industry Canada* <https://cippic.ca/uploads/GoC-Canadas_Cryptographic_Policy-1998.pdf> at 30.

[125] Government of Canada (1998), "Discussion Paper: A Cryptography Policy Framework for Electronic Commerce--Building Canada's Information Economy and Society", *Industry Canada* <https://cippic.ca/uploads/GoC-Canadas_Cryptographic_Policy-1998.pdf> at 9.

[126] Notably, the United States had never implemented the pre-1998 licensing exception for mass-market customer software encoded in the GSN.

See: Sarah Andrews (2000), "Who Holds the Key? A Comparative Study of US and European Encryption Policies", 2 *J of Information, L and Tech* <https://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2000_2/andrews/> at section 3.2.

symmetric length.[127] The GSN was also expanded to encompass mass market hardware, whereas before it was limited to software.[128] However, at the same time, the GSN was controversially limited in application so that export permits would be required for *any* encryption products employing keys in excess of 64 bits of symmetric key length, including mass market products.[129]

The 1998 Wassenaar changes are perhaps best understood through the lens of American encryption policy, as the U.S. was a driving force behind the shift.[130] The United States approach to encryption export control at the time, which was mirrored in its domestic policy and also updated in late 1998, was far more restrictive than that adopted in Wassenaar—notably, it set the license ceiling for non-recoverable symmetric key lengths at 54 bits.[131] From this perspective, the changes represent the United States' failure to convince Wassenaar partners of the merits of its approach to export restrictions.[132] The ultimate irony of the US-led Wassenaar changes, however, is that by late 1999 the United States itself had greatly liberalized its domestic export policy well beyond the more restrictive conditions it had pushed for within Wassenaar by allowing the export of encryption products of any key length to non-government end users.[133]

---

[127] Sarah Andrews, "Who Holds the Key? A Comparative Study of US and European Encryption Policies", (2000) 2 *J of Information, L and Tech* <https://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2000_2/andrews/> at section 3.2; United States House of Congress (1999), House Committee on Commerce, Subcommittee on Telecommunications, Trade and Consumer Protection, Testimony of Bill Reinsch, Undersecretary of Export Administration, Department of Commerce, "Security and Freedom Through Encryption Act – HR 850", (25 May 1999) <https://fas.org/irp/news/1999/05/990525-crypto.htm>.

[128] *Ibid*.

[129] *Ibid*:

> "Most importantly, the Wassenaar members agreed to remove encryption software from Wassenaar's General Software Note and replace it with a new cryptography note. Drafted in 1991, when banks, government and militaries were the primary users of encryption, the General Software Note allowed countries to permit the export of mass market encryption software without restriction. The GSN was created to release general purpose software used on personal computers, but it inadvertently encouraged some signatory countries to permit the unrestricted export of encryption software. It was essential to modernize the GSN and close the loophole that permitted the uncontrolled export of encryption with unlimited key length. Under the new cryptography note, mass market hardware has been added and a 64-bit key length or below has been set as an appropriate threshold. This … does not mean encryption products of more than 64 bits cannot be exported. Our own policy permits that, as does the policy of most other Wassenaar members. It does mean, however, that such exports must be reviewed by governments consistent with their national export control procedures."

[130] *Ibid*:

> "In December [1998], through the hard work of [United States] Ambassador David Aaron, the President's special envoy on encryption, the Wassenaar Arrangement members agreed on several changes relating to encryption controls."

See also Sarah Andrews (2000), "Who Holds the Key? A Comparative Study of US and European Encryption Policies", 2 *J of Information, L and Tech* <https://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2000_2/andrews/> at section 3.2.

[131] This policy was largely put in place late 1996, and, notably, updated on September 22, 1998 (that is, effectively in conjunction with finalization of the 1998 Wassenaar changes) when exceptions were added for exports of encryption using any key length to in 46 designated countries if destined for the insurance and medical/health sectors or to online merchants for the purpose of securing online transactions with customers.

See Danielle Kehl, Andi Wilson, and Kevin Bankston (2015), "Doomed to Repeat History? Lessons from the Crypto Wars of the 1990s," *New America Open Technology Institute* <https://static.newamerica.org/attachments/3407-doomed-to-repeat-history-lessons-from-the-crypto-wars-of-the-1990s/Crypto%20Wars_ReDo.7cb491837ac541709797bdf868d37f52.pdf> at 15-17; United States House of Congress (1999), House Committee on Commerce, Subcommittee on Telecommunications, Trade and Consumer Protection, Testimony of Bill Reinsch, Undersecretary of Export Administration, Department of Commerce, "Security and Freedom Through Encryption Act – HR 850", (25 May 1999) <https://fas.org/irp/news/1999/05/990525-crypto.htm>.

[132] Sarah Andrews, "Who Holds the Key? A Comparative Study of US and European Encryption Policies" (2000), 2 *J of Information, L and Tech* <https://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2000_2/andrews/> at section 3.2:

> "It is significant to note, however, that once again US efforts to gain international approval for their key recovery proposals failed and the new Control List makes no concessions for the export of such products."

[133] Some restrictions remained in place. While retail and open source products could be exported without limit, customized encryption products destined for non-government required a "technical review" by the U.S. government prior to export. Exports destined for foreign government end users continued to require a license assessed on a case by case basis.

See Peter Swire & Kenesa Ahmad, "Encryption and Globalization" (2012), 23 *Columbia Sci & Tech L Rev* <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1960602> at 439-441; Danielle Kehl, Andi Wilson, and Kevin Bankston (2015), "Doomed to Repeat History? Lessons from the Crypto Wars of the 1990s," *New America Open Technology Institute* <https://static.newamerica.org/attachments/3407-doomed-to-repeat-history-lessons-from-the-crypto-wars-of-the-1990s/Crypto%20Wars_ReDo.7cb491837ac541709797bdf868d37f52.pdf> at 15-17; Sarah Andrews (2000), "Who Holds the Key? A Comparative Study of US and European Encryption Policies", 2 *J of Information, L and Tech* <https://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2000_2/andrews/> at section 4.2.

iii. The Canadian Context and the Cryptography Policy

Canada's national "Cryptography Policy" was adopted in 1998, and is very much a product of the era. Prior to 1998, Canadian cryptography policy was largely restricted to export control rules, and largely in line with its commitments under the Wassenaar Arrangement.[134] This included a complete ban on exports to a sub-set of specific countries as well as a licensing requirement for 56-bit customized symmetric encryption software or hardware with encryption.[135] Commercial actors in Canada were also impacted by restrictions imposed by the United States and others.[136] For example, the weak mobile communications encryption set in the European GSM standard 1980s described above became global standards and were adopted by Canadian mobile providers as well.[137] As the Canadian government joined its counterparts in formalizing a national and international cryptography policy, Canadian law enforcement and national security agencies mobilized in support of more overt and robust Canadian restrictions on cryptography. The consultation that formulated Canada's cryptography policy featured calls from law enforcement and national security agencies to ensure that any broadly adopted encryption policy would include the ability for government to decrypt data they acquired or intercepted.[138] The consultation document itself advanced the option of government prohibitions on the creation, import, export, or use of any strong encryption that lacked a key escrow or recovery mechanism—a proposition strongly opposed by a large international coalition of civil society groups.[139] The final government policy was ultimately premised on the OECD Guidelines, and includes six core but non-binding points. The four most relevant of those points are as follows:

- It "affirms the freedom of Canadians to develop, import and use whatever cryptography products they wish" and expresses that the government wants "Canadian businesses and citizens to have access to a wide range of products and services, including the very strongest forms of encryption."

- It states that the government "will not implement mandatory key recovery requirements or licensing regimes for certification authorities or trusted third parties."

---

[134] Government of Canada (1998), "Discussion Paper: A Cryptography Policy Framework for Electronic Commerce--Building Canada's Information Economy and Society", *Industry Canada* <https://cippic.ca/uploads/GoC-Canadas_Cryptographic_Policy-1998.pdf> at 9.

[135] *Ibid*; Brad Evenson, "Going Cryptic on the Net" (1996), *The Ottawa Citizen* (23 August 1996) archived at: <http://www.efc.ca/pages/media/ottawa.citizen.23aug96.html>:

> "The export of encryption software, which converts a document into an undecipherable code, is considered so sensitive to Canada's interest, it is treated the same as guns or tobacco. It cannot be exported to such countries as Iraq and Libya; the law considers this as serious as smuggling weapons. American laws are stricter still: Only encryption that U.S. authorities know how to decipher can be exported. "Generally, (export) restrictions are there to make sure subversive or terrorist organizations don't get these products", says White. It takes Entrust four to six weeks to get an export permit from the Foreign Affairs Department, which reviews each international sale."

[136] Jeffrey Shallit & David Jones (1997), "Statement on Canadian Cryptography Policy", *Electronic Frontiers Canada* (14 August 1997) <http://www.efc.ca/pages/crypto/policy.html>:

> "It is widely recognized that interests and priorities established by American law enforcement and national security agencies have had a significant impact, both on U.S. policy, as well as cryptography policies around the world. As an illustration, several Canadian banks discriminate against a subset of their Canadian customers who do electronic commerce by not providing them with software that uses strong encryption. They do this in order to comply with contractual obligations with American companies that provide strong encryption software. Those companies, in turn, are obligated to include those terms in their contracts in order to comply with American cryptography policy. In this way, American policy has a specific and extra-territorial impact on Canadians and Canadian-owned companies."

[137] For example, in 2006, 37% of Canada's 18 million or so mobile subscribers used Rogers Communications. Rogers mobile services used the GSM protocol, which deployed the same weakened A5/1 or A5/2 encryption adopted in the 1980s in Europe.

See e.g., CRTC, Communications Monitoring Report 2008 (July 2008) <http://publications.gc.ca/collections/collection_2008/crtc/BC9-9-2008E.pdf> Figure 5.5.7, Figure 5.5.1, and at 254.

[138] Electronic Frontiers Canada (1998), "International Human Rights Organizations Express Privacy Concerns About Canadian Cryptography Policy" (27 April 1998) <http://www.efc.ca/pages/pr/efc-pr.27apr98.html>:

> "Advocates for government restrictions on the use of encryption technology include the Canadian Association of Chiefs of Police (CACP), the Royal Canadian Mounted Police (RCMP), the Canadian Security and Intelligence Service (CSIS), and the Communications Security Establishment (CSE), all of which were represented at the Ottawa meeting, where they expressed concern about losing the ability to eavesdrop on email or voice communications when conducting investigations. "Law enforcement agencies *must* be provided a means by which they can decrypt information they gather", said RCMP Commissioner Philip Murray at the meeting, and in the RCMP's written submission to Industry Canada."

[139] Global Internet Liberty Campaign (1998), "Statement on Canadian Crypto Policy" (20 April 1998) <http://www.efc.ca/pages/crypto/gilc-letter.20apr98.html>.

- It states that the government will "encourage industry to establish responsible practices, such as key recovery techniques for stored data and industry-led accreditation of private sector certification authorities," in order to "build consumer and business confidence in these products and services, and assure business continuity in case of loss or corruption of keys." It states that the government's procurement processes will be used to encourage commercial key back-up.

- It states that "Government proposes to make legislative amendments which will protect consumers' privacy and will also give law enforcement agencies and national security agencies the legal framework they need to ensure public safety. This includes making it an offence to wrongfully disclose private encryption key information and to use cryptography to commit or hide evidence of a crime." The Minister also stated that "we also need to make it clear that warrants and assistance orders also apply to situations where encryption is encountered - to obtain the decrypted material or decryption keys."[140]

This policy represented a clear rejection of the more aggressive proposals for mandatory key escrow that were hallmarks of the encryption debate earlier in the decade. It also called for legislative changes that would clarify the degree to which service providers in receipt of a search warrant could be compelled to assist in decrypting any data subsequently acquired. However, efforts to clarify such powers failed to materialize in public law, and for over a decade following the policy's release, public engagement on the question was largely abandoned.

C. GLOBAL SHIFTS IN THE ENCRYPTION DEBATE (2000-2010)

In the United States, Canada, and most European countries, the encryption issue reached an equilibrium of sorts following the heated debates of the 1990s. While governments continued to push for expanded search and seizure powers—pitched as necessary to address technological change—encryption was not a prominent feature on the list of scourges plaguing investigators and intelligence agents in the first decade of the new millennium. During this era, law enforcement and intelligence agencies instead focused on maximizing their ability to exploit the vast and detailed information that was a hallmark of the participative web—social media interactions, ubiquitous location data, cloud-based document storage, and a broad assortment of digital content which presented an intimate picture of any individual's life, habits, or relationships.[141] To the extent that encryption posed an investigative barrier in this era, agencies employed existing powers to work around encryption and found other ways to obtain the same data. At the same time, some states began to attempt to impose decryption requirements on increasingly global communications platforms based in the United States, Canada, and Europe, which added a globalization dimension to the encryption debate.

i. Ubiquitous Access to New Kinds of Data

Encryption was not a dominant component of law enforcement or intelligence agencies' lobbying agenda in the 2000s.[142] For example, in 2002 a Canadian Department of Justice consultation document was issued for the purpose of assessing whether new laws or powers were needed, stating that "rapidly evolving technologies [were posing] a significant challenge to law enforcement and national security agencies … [by making] it more difficult to gather the information required to carry out effective investigations."[143] This document outlined a number of investigative challenges and proposed a range of new powers, yet it did not mention encryption even once as posing such an investigative barrier[144] and it conspicuously excluded even the minor amendments called for in the 1998 National Cryptography policy. Legislative proposals that emerged from this consultation included only limited attempts to overtly regulate encryption or facilitate state access to encrypted data. At the same

---

[140] Speaking Notes on "Canada's Cryptography Policy" (1998) for the Honourable John Manley, Minister of Industry, to the National Press Club (1 October 1998) <http://fas.org/irp/news/1998/10/981001-crypto.htm>.

[141] Of course, a full catalogue of the new data sources that emerged as a byproduct of the participative web is well beyond the scope of this report.

For an overview, see OECD (2007), "Participative Web: User-Created Content", DSTI/ICCP/IE(2006)7/FINAL (12 April 2007) <https://www.oecd.org/sti/38393115.pdf>.

[142] Peter Swire & Kenesa Ahmad (2012), "Encryption and Globalization", 23 *Columbia Sci & Tech L Rev* <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1960602>.

[143] Canada, Department of Justice (2002), "Lawful Access—Consultation Document", (25 August 2002) <http://www.justice.gc.ca/eng/cons/la-al/la-al.pdf>.

[144] *Ibid*.

time, the Council of Europe's Cybercrime Convention—which was finalized in 2001 and adopted by numerous states, including Canada and the United States—addressed perceived challenges posed by emerging technologies to various investigative and intelligence gathering objectives without making encryption a primary focus.[145]

There is also some evidence to suggest that the information blackout underpinning government concerns about encryption in the 1980s and 90s simply failed to materialize. For example, communications surveillance was historically conducted primarily under Part VI of the Criminal Code, which governs wiretaps and some other forms of real-time electronic surveillance. Yet the number of Part VI authorizations issued annually to the RCMP in Canada decreased only modestly in the 2000-2011 period. Perhaps more importantly, the annual number of proceedings relying on Part VI or Part VI-derived evidence and successful resulting prosecutions remained roughly equivalent over this period of time as well. Together, this data suggests that the RCMP's ability to obtain and leverage evidence from historical electronic surveillance mechanisms remained largely unimpeded during this period.

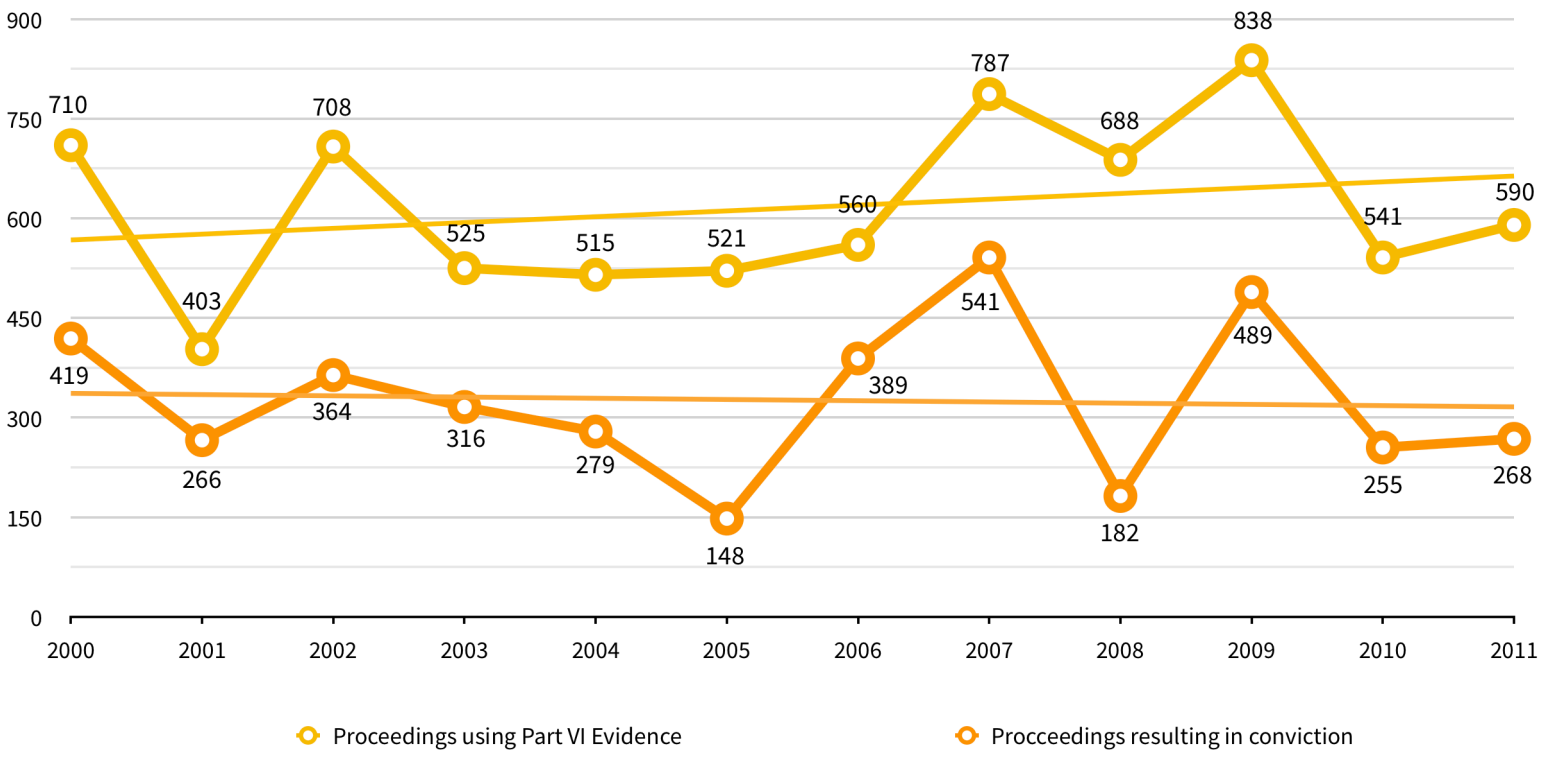


Figure 3: Proceedings & Convictions Using Part VI-Derived Evidence[146]

[145] Encryption was initially listed as an obstacle to technological investigations of crime in the initial 1996 terms of reference that eventually led to the ultimate adoption of the Cybercrime Convention. However, the Convention itself provides no provisions at all designed to facilitate state access to encrypted data, and even recommends the use of encryption when one state transmits electronic evidence to a foreign state to facilitate the foreign state's investigative needs.

See Convention on Cybercrime, ETS No 185 (23 November 2001) <http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf>; see also Explanatory Report to the Convention on Cybercrime, Budapest (23 November 2001) <https://rm.coe.int/16800cce5b> at para 11.iv.

[146] Compiled from: Public Safety Canada, (2004-2015), "Annual Report on the Use of Electronic Surveillance", issued annually in the years between 2004 to 2015 <https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/index-en.aspx>. To ensure data is the most up-to-date available, each data point data is derived from the most recent year available: data presented for the year 2000 is derived from the 2004 Annual Report; data presented for the year 2001 is derived from the 2005 Annual Report; etc. Data points for "Proceedings using Part VI Evidence" compile figures for the number of criminal proceedings commenced by the Attorney General of Canada that adduced private communications intercepted under Part VI as evidence and in which information obtained as a result of a Part VI interception was adduced in evidence, although the private communication itself was not. Data for "Proceedings Resulting in Conviction" compiles reported convictions resulting from these respective proceedings. Data for both "Proceedings using Part VI Evidence" and "Proceedings Resulting in Conviction" is reported further to paragraphs 195(2)(m) and (n) of the Criminal Code, and presented in Tables 11 & 12 in Annual Reports issued for the years 2013-2015 and in Figures 3 & 4 in Annual Reports issued for years prior to 2012.

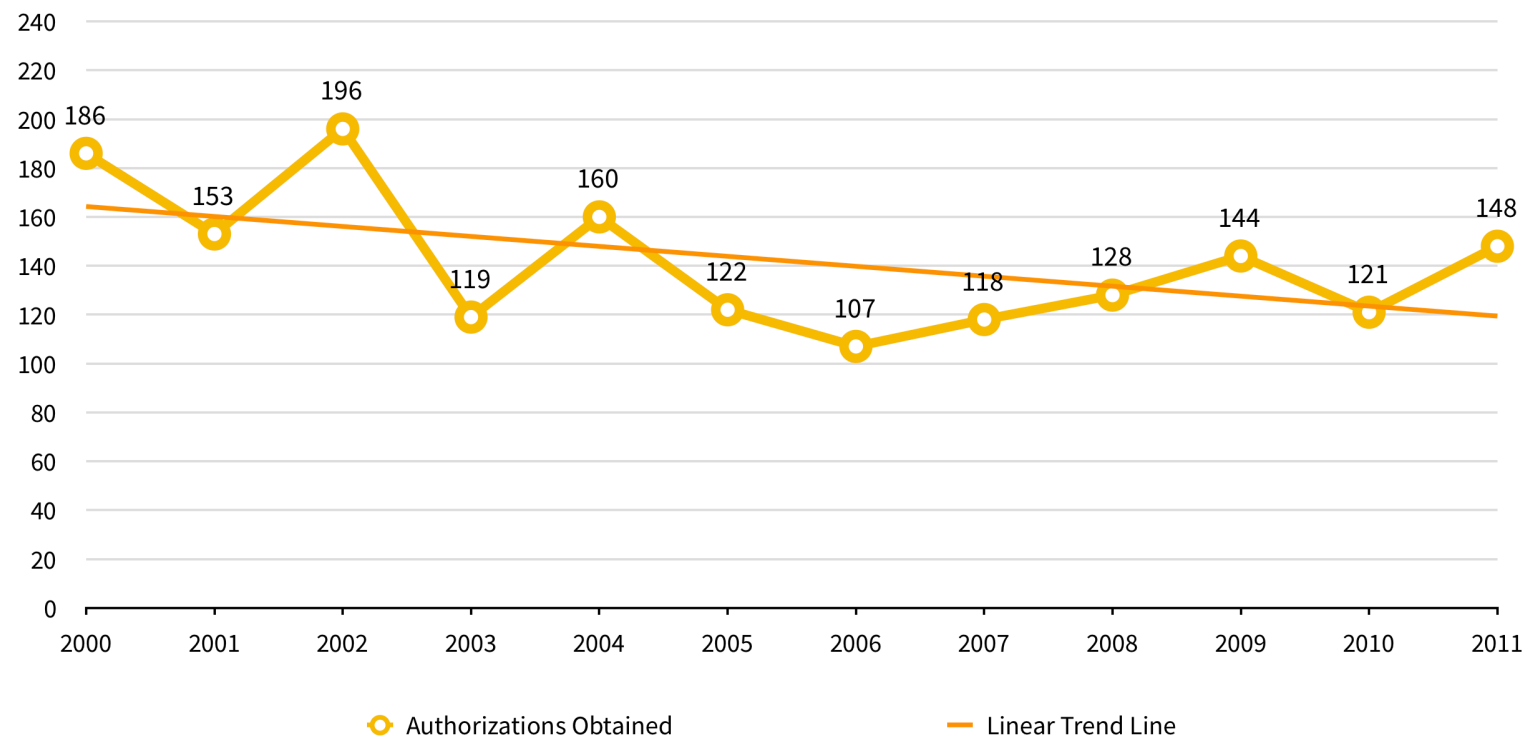


Figure 4: Part VI Authorizations Obtained[147]

Wiretap authorizations in the United States indicate similarly consistent surveillance capabilities in the face of encryption.[148] Indeed, what data is available regarding other techniques suggests that while the volume of U.S. law enforcement wiretaps remained largely stable during this period, this stability was accompanied by a dramatic increase in the use of other invasive digital surveillance tools such as those directed at intercepting metadata.[149] It is also now clear that signals intelligence agencies such as the CSE and its partners, the NSA and the United Kingdom's GCHQ (members of the Five Eyes intelligence partnership) were not significantly constrained during this era. Beginning in 2001, these agencies dramatically expanded their capabilities to capture unprecedented amounts of electronic data—which is now regularly analyzed, stored, and operationalized.[150]

While they have never been systemically documented, a range of existing powers of general application were also employed by state agencies to bypass encryption in this era. For example, the Five Eyes signals intelligence agencies relied on their general mandates to develop sophisticated techniques over this period to obtain data in plaintext even where encryption

---

147 Compiled from: Public Safety Canada, (2004-2015), "Annual Report on the Use of Electronic Surveillance", issued annually in the years between 2004 to 2015 <https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/index-en.aspx>. To ensure data is the most up-to-date available, each data point is derived from the most recent year available: data presented for the year 2000 is derived from the 2004 Annual Report; data presented for the year 2001 is derived from the 2005 Annual Report; etc. Data excludes authorization renewals. Data points compile authorizations obtained annually as further to paragraph 195(2)(a) of the Criminal Code and presented in Table 1 in referenced Annual Reports.

148 Peter Swire & Kenesa Ahmad (2012), "Encryption and Globalization", 23 *Columbia Sci & Tech L Rev* <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1960602> at 471:

> "Three thousand, one hundred and ninety-four wiretap court orders were issued for the interception of electronic, wire, or oral communications in 2010. In the six instances where encryption was encountered in 2010, the encryption did not prevent law enforcement from retrieving the plaintext forms of communication."

149 Naomi Gilens (2012), "New Justice Department Documents Show Huge Increase in Warrantless Electronic Surveillance", ACLU, (27 September 2012) <https://www.aclu.org/blog/national-security/new-justice-department-documents-show-huge-increase-warrantless-electronic>.

150 Glenn Greenwald and Ewen MacAskill (2013), "Boundless Informant: The NSA's Secret Tool to Track Global Surveillance Data", *The Guardian* (11 June 2013) https://www.theguardian.com/world/2013/jun/08/nsa-boundless-informant-global-datamining.

was involved.[151] Law enforcement similarly began to explore ways in which generalized assistance powers might be used to compel service providers to bypass their own encryption.[152] However, such efforts occurred largely in secret, and thus did not become a significant part of the public discussion. Ultimately, while some historically available datasets might have become more difficult to access, encryption does not appear to have greatly impeded government's ability to investigate and prevent crime or to gather intelligence in this period.

ii. Global Markets and Global Problems

While the encryption debate was somewhat dormant in Canada, the United States, and Europe following the liberalization of the late 1990s, global Internet and communications companies faced aggressive demands from other governments during the same period. Research in Motion (RIM), whose Blackberry phones became top-selling mobile devices (in large part based on the strength of their perceived security), experienced challenges that were indicative of a more general climate. Around 2007, a number of countries began to pressure RIM to make the encrypted mobile services (e.g., email and instant messaging) including in BlackBerry devices more accessible to government agencies.[153] This culminated in prominent international standoffs, with countries such as the United Arab Emirates and India threatening to block Blackberry services nation-wide. RIM ultimately capitulated, establishing dedicated servers in a number of countries—reportedly also including China, India, Indonesia, Russia, Saudi Arabia, and the United Arab Emirates—to facilitate direct state access to otherwise encrypted Blackberry communications.[154] While RIM's compromise only impacted its consumer-facing services[155] the case study demonstrates how domestic encryption policies such as those of the United Arab Emirates, India, and China may force service providers to weaken core product features in order to participate in local markets, jeopardizing user security in the process.

RIM built its global market share on the strength of its data security practices and became the provider of choice for governments and corporations around the world. But within networks where foreign governments pose a threat—as adversaries in business, ideology, security, or diplomatic affairs—business solutions that allow foreign governments access to encrypted communication can be subverted to compromise security at home. States that seek to impose restrictions on encryption need to

---

[151] Government Communications Headquarters (GCHQ), "BULLRUN Col – Briefing Sheet", *Snowden Archive* <https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASH01f0/54648c90.dir/doc.pdf>:

> "In recent years there has been an aggressive effort, lead by NSA, to make major improvements in defeating network security and privacy involving multiple sources and methods, all of which are extremely sensitive and fragile. These include: Computer Network Exploitation (CNE); collaboration with other Intelligence Agencies; investment in high-performance computers; and development of advanced mathematical techniques. … To achieve this, NSA has introduced the BULLRUN Col to protect our abilities to defeat the encryption used in network communication technologies. This covers both the 'fact of" a capability against a specific technology and resulting decrypts (which may be either plaintext or metadata (events). GCHQ Is also introducing BULLRUN. (CSEC, DSD and GCSB are expected to do likewise.)"

See also National Security Agency, "Classification Guide Title/Number: Project BULLRUN/2-16", *Snowden Archive* (16 June 2010) <https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASHea20.dir/doc.pdf>:

> "Project BULLRUN Deals with NSA's Abilities to defeat the encryption used in specific network communication technologies. BULLRUN Involves multiple sources, all of which are extremely sensitive. They Include CNE, interdiction, industry relationships, collaboration with other IC entities, and advanced mathematical techniques."

See also Greg Weston (2013), "Spy Agency CSEC Needs MPs Oversight, Ex-Director Says", *CBC News* (7 October 2013) <http://www.cbc.ca/news/politics/spy-agency-csec-needs-mps-oversight-ex-director-says-1.1928983>:

> "[Former CSEC Director John] Adams won't reveal details about how CSEC spies operate in this country, but they are apparently breaking through encryptions. "The reality is encryption is ubiquitous, it's everywhere, so clearly if intelligence agencies are going to seek information, they're going to be able to breach encryption." All of which helps to explain Adams's warning for average Canadians: if you think anything you read, write or send via the internet is private, think again."

Peter Swire & Kenesa Ahmad (2012), "Encryption and Globalization", 23 *Columbia Sci & Tech L Rev* <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1960602> at 465:

> "Despite 'losing' the crypto wars, agency concerns were still addressed. The FBI received additional funding for its technical interception capabilities, which has continued to grow over time."

[152] Ryan Singel (2007), "Encrypted E-mail Company Spills to Feds", *Wired* (11 July 2007) <https://www.wired.com/2007/11/encrypted-e-mai/>.

[153] Barry Meier and Robert F. Worth (2010), "Emirates to Cut Data Services of BlackBerry", *New York Times* (1 August 2010) <http://www.nytimes.com/2010/08/02/business/global/02berry.html>.

[154] Andrew Hammond (2010), "UAE says BlackBerry dispute resolved before deadline", Reuters (8 October 2010) <https://www.reuters.com/article/us-blackberry-emirates/uae-says-blackberry-dispute-resolved-before-deadline-idUSTRE6970S320101008>; Marguerite Reardon (2010), "BlackBerry security: Blessing and a curse", *CNet* (9 August 2010) <https://www.cnet.com/news/blackberry-security-blessing-and-a-curse/>.

[155] RIM offers a more secure enterprise service called BlackBerry Enterprise Server.

consider what Swire and Ahmad have called the “least trusted country problem." This problem presumes that since companies will treat all states equally, each state must be comfortable with other states adopting encryption policies as restrictive or permissive as their own.[156] Domestic policies that apply to companies operating in a globalized marketplace can dictate (directly and indirectly) the level of protection provided to foreigners abroad, and foreign policies have the converse power to undermine protections available domestically. Simultaneously, the transnational nature of the Internet operates as a countervailing force, making circumvention of domestic anti-encryption policy easy for motivated actors—as long as alternative encryption tools remain available online, and at least for states unwilling to engage in extraordinary forms of Internet censorship. A state willing to compel a global service provider to adopt weakened encryption must accept that the digital interactions of its own citizens, its own companies, and its own officials and diplomats might ultimately be subject to the same level of access should a foreign (and potentially adversarial) state follow suit.

D. GOING DARK: THE CURRENT DEBATE (2011-2018)

> **The laws of mathematics are very commendable, but the only law that applies in Australia is the law of Australia. I’m not a cryptographer, but we are seeking…their assistance.”**
>
> **— Malcolm Turnbull, Prime Minister of Australia[157]**

In early 2010 the Federal Bureau of Investigations (FBI) led investigative agencies in the United State in publicly reopening the encryption debate using the colloquial shorthand of "going dark.”[158] The “going dark" narrative pointed to a perceived (and perceived to be growing) gap between what kinds of data law enforcement agencies were lawfully able to access and their practical technical ability to obtain it.[159] This perceived gap was attributed in part to the growing use of encryption, as well as to new transmission mechanisms employed by modern web applications. Such mechanisms had become more ephemeral and difficult to intercept and retain than before.[160] The use of encryption by individuals and companies can pose investigative barriers for state actors by reducing the amount and type of plaintext information that is easily available about a given target or network. Government agencies’ fear that unfettered public access to strong encryption tools deprives governments of both the evidence and intelligence necessary to protect public safety was perhaps best summarized by former FBI Director James Comey, who wrote, “there is simply no doubt that bad people can communicate with impunity in a world of universal strong encryption.”[161] Director Comey’s statement captures the general impetus behind many of the recent public calls for a shift in encryption policy, which have only increased in the urgency of their rhetoric.

In 2014, technology companies began adopting more sophisticated encryption and security measures following Edward Snowden’s public disclosures regarding the scope of state surveillance. This led to a shift in the “going dark” discourse. The

---

[156] Peter Swire & Kenesa Ahmad (2012), “Encryption and Globalization”, 23 *Columbia Sci & Tech L Rev* <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1960602> at 419, 443.

So for example, if India wishes to bypass Blackberry encryption used by individuals in nearby Pakistan, it must be comfortable with Pakistan obtaining the same level of access. Indeed, after being one of the most persistent states demanding RIM accommodations, India ultimately decided to drop its demands for access to RIM’s BlackBerry Enterprise Server (BES) services, settling for co-located RIM servers that facilitate direct access to customer-facing services.

See Digit News Desk (2012), "RIM sets up server for Indian govt. to intercept BBM data in real-time”, *Digit* (21 February 2012) <https://www.digit.in/mobile-phones/rim-sets-up-server-for-indian-govt-to-intercept-bbm-data-in-real-time-8807.html>:

> “[India gave] up trying to intercept the highly-encrypted BES data, now claiming that this communication is not of ‘high concern,’ as it is between employees of registered enterprises.”

[157] Rachel Roberts (2017), "Prime Minister claims laws of mathematics 'do not apply' in Australia”, *The Independent* (15 July 2017) <https://www.independent.co.uk/news/malcolm-turnbull-prime-minister-laws-of-mathematics-do-not-apply-australia-encryption-l-a7842946.html>.

[158] Charlie Savage (2010), “US Is Working to Ease Wiretaps on the Internet”, *New York Times* (27 September 2010) <https://query.nytimes.com/gst/fullpage.html?res=9E03E4D61030F934A1575AC0A9669D8B63>; Valerie Caproni (2011), General Counsel, Federal Bureau of Investigation, “Going Dark: Lawful Electronic Surveillance in the Face of New Technologies”, *prepared testimony for Hearing Before the Subcommittee On Crime, Terrorism, and Homeland Security of the House of Commons Committee on the Judiciary*, 112th Cong. 10 <http://judiciary.house.gov/hearings/printers/112th/112-59_64581.PDF>; Peter Swire & Kenesa Ahmad (2012), “Encryption and Globalization”, 23 *Columbia Sci & Tech L Rev* <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1960602>.

[159] *Ibid*.

[160] *Ibid*.

[161] James Comey (2015), “Encryption, Public Safety, and “Going Dark”, (6 July 2015) <http://www.lawfareblog.com/encryption-public-safety-and-going-dark>.

premise became that lawful investigations and intelligence gathering efforts were being irreparably undermined as terrorists, child predators, and other criminals adopted effective digital security tools.[162] This narrative bolstered the concerted and increasingly aggressive demands for solutions to the encryption "problem" from high-level public officials in Five Eyes countries, including new legislation proposed in Australia in 2018. In Canada, the 2016 National Security Consultation flagged encryption among other intelligence challenges that motivated the government's agenda for reform.

i. Renewed Demands for Undefined Solutions

Contrary to the first round of the "Crypto Wars," the "going dark" narrative is often far clearer on the need for a solution than on what such a solution might look like. Many of its proponents appear to possess great optimism in the future ingenuity of software engineers to come to a solution when faced with legal threats, but have declined to provide concrete examples of workable technical options themselves.

In early 2018 in the United States, FBI Director Christopher Wray pointed to smartphone encryption as a "major public safety issue,"[163] which built on calls from U.S. Deputy Attorney General Rod Rosenstein for "responsible encryption" (which appears to reduce to a rebranding initiative for encryption backdoors).[164] In the United Kingdom, the *Investigatory Powers Act (2016)* granted the Secretary of State the new power to issue "technical capability orders" 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."[165] The provisions were controversial and in their final form they excluded the ability to compel measures that were not "technically feasible."[166] It remains unclear how "technical infeasibility" will be interpreted, and whether the provision will allow the government to compel engineers to redesign software products in fundamental ways. The most extreme interpretation could see service providers forced to undo end-to-end encryption systems or other mechanisms which would prevent a service provider from decrypting its users' communications. Following these amendments, high-level U.K. officials have also renewed explicit calls for legislation that would prevent the use of end-to-end encryption. Home Secretary Amber Rudd has advanced the view that end-to-end encryption is not for "real people" and should be banned, with tacit support from Prime Minister Theresa May.[167] If these reforms come to pass, many global service providers—such as Apple, Facebook, and Open Whisper Systems—may be forced to choose between making dramatic changes to their technology or simply making their products unavailable in the U.K..[168] The Australian government has also been active on the issue, with Prime Minister Malcolm Turnbull declaring that the laws of mathematics will need to find a way to bend to the laws of Australia. In 2017, then-Attorney General George Brandis also announced a plan to introduce legislation that would compel technology companies to decrypt customer data.[169]

---

[162] Kristin Finklea (2016), "Encryption and the 'Going Dark' Debate", *Congressional Research Service* (20 July 2016), <https://fas.org/sgp/crs/misc/R44481.pdf> at 5.

[163] Ellen Nakashima (2017), "FBI Chief Calls Encryption a "Major Public Safety Issue", *Washington Post* (9 January 2017) <https://www.washingtonpost.com/world/national-security/fbi-chief-calls-encryption-a-major-public-safety-issue/2018/01/09/29a04166-f555-11e7-b34a-b85626af34ef_story.html>.

[164] United States (2017), Department of Justice, Deputy Attorney General Rod J Rosenstein, "Remarks on Encryption at the United States Naval Academy" (remarks as prepared for delivery) (10 October 2017) <https://www.justice.gov/opa/speech/deputy-attorney-general-rod-j-rosenstein-delivers-remarks-encryption-united-states-naval>; Riana Pfefferkorn (2017), "A Response to 'Responsible Encryption", *Centre for Internet and Society* (11 October 2017) <http://cyberlaw.stanford.edu/blog/2017/10/response-%E2%80%9Cresponsible-encryption%E2%80%9D>.

[165] United Kingdom, *Investigatory Powers Act 2016,* c. 25 at s 253(5)(c).

[166] Alex Hern (2016), "Technology Firms' Hopes Dashed by 'Cosmetic Tweaks' to Snooper's Charter", *The Guardian* (1 March 2016) <https://www.theguardian.com/technology/2016/mar/01/technology-firms-hopes-dashed-by-cosmetic-tweaks-to-snoopers-charter>

[167] See e.g., Timothy Revell (2017), "Theresa May's repeated calls to ban encryption still won't work", *New Scientist* (5 June 2017) <https://www.newscientist.com/article/2133644-theresa-mays-repeated-calls-to-ban-encryption-still-wont-work/>; Alex Hern (2017), "UK government can force encryption removal, but fears losing, experts say", *The Guardian* (29 March 2017) <https://www.theguardian.com/technology/2017/mar/29/uk-government-encryption-whatsapp-investigatory-powers-act>; Rob Price (2017), "UK home secretary Amber Rudd says 'real people' don't need end-to-end encryption", *Tech Insider* (1 August 2017) <http://www.businessinsider.com/home-secretary-amber-rudd-real-people-dont-need-end-to-end-encryption-terrorists-2017-8>; Dave Lee (2017), "Message encryption a problem - Rudd", *BBC* (1 August 2017) <http://www.bbc.com/news/technology-40788180>.

[168] *Ibid*.; United Kingdom, *Investigatory Powers Act 2016,* c. 25 at s 253.

[169] Press conference with the Prime Minister, Attorney-General, Senator, the Hon. George Brandis QC and the Acting Commissioner of the Australian Federal Police, Mr. Michael Phelan APM, AFP Headquarters, Sydney (14 July 2017) <http://www.pm.gov.au/media/2017-07-14/press-conference-attorney-general-senator-hon-george-brandis-qc-and-acting>; Henry Belot (2017), "Ex-NSA boss questions encrypted message access laws proposed by Malcolm Turnbull", *ABC News* (1 August 2017) <http://www.abc.net.au/news/2017-08-01/former-nsa-boss-questions-malcolm-turnbull-encryption-laws/8761542>; Natasha Lamas (2017), "Australia wants Five Eyes to squeeze tech firms on encryption", *TechCrunch* (25 June 2017) <https://techcrunch.com/2017/06/25/australia-wants-five-eyes-to-squeeze-tech-firms-on-encryption/>; Peter Hartcher & James Massola (2017), "G20 summit: Malcolm Turnbull to urge Donald Trump to act against tech terrorists", *The Sydney Morning Herald* (5 July 2017) <https://tenplay.com.au/news/national/july-2017/Accused%20criminals%20to%20handover%20computer%20passwords%20or%20face%20jail>; Nick Evershed (2017), "Australia's Plan to Force Tech Giants to Give Up Encrypted Messages May Not Add Up", *The Guardian (*14 July 2017) <https://www.theguardian.com/technology/2017/jul/14/forcing-facebook-google-to-give-police-access-to-encrypted-messages-doesnt-add-up>.

The "going dark" concern has also been raised by lobbyists for the Canadian law enforcement community. It was explicitly flagged as an issue in Canada's 2016 National Security Consultation, explored in greater detail below. In addition, Public Safety Canada's annual 2017 terrorist threat analysis report flagged encryption as a primary investigative and intelligence challenge:

> "Terrorist entities also rely on cyberspace to enhance the security of their conventional activities. Most notably, the increasing prevalence of encryption technologies allows terrorists to conceal their communications and evade detection by police and intelligence agencies. The ability to intercept terrorist communications is no longer always possible due to strong encryption. This is a significant challenge to the Government's ability to investigate and charge threat actors. This phenomenon is popularly described as "going dark".[170]

Canadian law enforcement lobbyists have also highlighted encryption as an investigative challenge. For example, in 2016 the Canadian Association of Chiefs of Police (CACP) adopted a resolution calling for new powers to compel decryption[171] and echoed global calls to secure new electronic investigative powers by organizations like the International Association of Chiefs of Police (IACP).[172]

In late 2016, an internal document presented by the RCMP to Public Safety Canada recognized that robust encryption technologies "increase privacy and security" but that the same technologies can also "create a black hole for law enforcement when a method for decrypting or otherwise removing the encryption is unavailable." It noted that the "'going dark' digital evidence challenges... [are] likely to become even more pronounced as technology continues to develop at an exponential rate."[173] The document acknowledged that no solutions to this problem had been developed, and called for an evidence-based public narrative espousing the detrimental impacts of encryption.[174] In support of this "evidence-based" effort, the RCMP provided privileged access to secret details of 10 select case studies of ongoing investigations to a small number of journalists in 2016. The RCMP asserted to the journalists that encryption had become a major barrier to the investigation of serious crimes in Canada.[175] However, these details were contested by academics and civil society advocates as a potentially selective and one-sided account which failed to present a comprehensive picture of the issue.[176]

Canada has also been actively working with its Five Eye partners (Australia, New Zealand, the United Kingdom and the United States) on the "going dark" problem. In late 2015, a Going Dark Five Eyes Law Enforcement Group (FELEG) Forum was established to work through the technical and policy issues raised by encryption, with membership that includes the RCMP, the Australian Federal Police, the New Zealand Police, the U.K. National Crime Agency, and the United States FBI, Homeland Security Investigations, and the Secret Service.[177] Encryption has also become a focal issue at Five Eyes periodic meetings,[178] culminating

---

[170] Public Safety Canada, "2017 Public Report on the Terrorist Threat to Canada: Building A Safe and Resilient Canada" (21 December 2017) <https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/pblc-rprt-trrrst-thrt-cnd-2017/pblc-rprt-trrrst-thrt-cnd-2017-en.pdf> at 9.

[171] Canadian Association of Chiefs of Police (2016), Resolution 2016-03, "Reasonable Law to Address the Impact of Encrypted and Password-protected Electronic Devices" <https://cacp.ca/resolution.html?asst_id=1197> at 19—20.

[172] International Association of Chiefs of Police (2015), "Data, Privacy, and Public Safety: A Law Enforcement Perspective on the Challenges of Gathering Electronic Evidence," IACP Summit Report (February 2015) <http://www.theiacp.org/portals/0/documents/pdfs/IACPSummitReportGoingDark.pdf> at 4—12.

[173] Royal Canadian Mounted Police (2016), "Encryption and Law Enforcement", Brief obtained under the *Access to Information Act* by Christopher Parsons in 2017 <https://cippic.ca/uploads/ATI-RCMP-Encryption_and_Law_Enforcement-2016.pdf> at 3.

[174] *Ibid.*

[175] Dave Seglins, Robert Cribb, and Chelsea Gomez (2016), "RCMP want new powers to bypass digital roadblocks in terrorism, major crime cases", CBC News (15 November 2016) <http://www.cbc.ca/news/investigates/rcmp-digital-roadblocks-1.3850018>; Dave Seglins, Robert Cribb, and Chelsea Gomez (2016), "Top-secret RCMP files show digital roadblocks thwarting criminal investigations in Canada", *Toronto Star* (15 November 2016) <https://www.thestar.com/news/canada/2016/11/15/top-secret-rcmp-files-show-digital-roadblocks-thwarting-criminal-investigations-in-canada.html>.

[176] Tamir Israel & Christopher Parsons (2016), "RCMP is Overstating Canada's 'Surveillance Lag'", *Toronto Star* (21 November 2016) <https://www.thestar.com/opinion/commentary/2016/11/21/rcmp-is-overstating-canadas-surveillance-lag.html>; Christopher Parsons (2016), "Pleading the Case: How the RCMP Fails to Justify Calls for New Investigatory Powers", *Technology, Thoughts, and Trinkets* (15 November 2016) < https://christopher-parsons.com/pleading-the-case-how-the-rcmp-fails-to-justify-calls-for-new-investigatory-powers/>; Jordan Pearson (2016), "The RCMP Is Using the Media to 'Create Moral Panic' About Encryption", *Motherboard* (15 November 2016) <https://motherboard.vice.com/en_us/article/xygmkz/the-rcmp-is-using-the-media-to-create-moral-panic-about-encryption-cbc-toronto-star>.

[177] Royal Canadian Mounted Police (2016), "Encryption and Law Enforcement", Brief obtained under the *Access to Information Act* by Christopher Parsons in 2017 <https://cippic.ca/uploads/ATI-RCMP-Encryption_and_Law_Enforcement-2016.pdf> at 3.

[178] See e.g. the reference to the "Joint meeting of the Five Country Ministerial and Quintet of Attorneys General on February 16, 2016, in Washington D.C., 'Session 3: Cyber: Encryption and How to Engage with ISPs" in Royal Canadian Mounted Police (2016), "Encryption and Law Enforcement", Brief obtained under the *Access to Information Act* by Christopher Parsons in 2017 <https://cippic.ca/uploads/ATI-RCMP-Encryption_and_Law_Enforcement-2016.pdf> at 1.

in a Five Eyes Ministerial conference hosted by Canada in June 2017 that coincided with public statements on the issue by officials in all five member states.[179] Following the June 2017 meeting a Joint Communiqué was released. The Communiqué shed little additional light on the issue except to note that Five Eyes members were "committed to develop [their] engagement with communications and technology companies to explore shared solutions while upholding cybersecurity and individual rights and freedoms."[180] A coalition of 83 major civil society organizations from Canada, the United States, the United Kingdom, Australia, and New Zealand issued an open letter shortly after the meeting, calling on Five Eyes members to respect the right to use and develop strong encryption and to pursue future dialogue on the subject in a transparent public forum.[181]

Contrary to historic calls for specific key escrow mechanisms that characterized the first Crypto Wars, the "going dark" narrative has often been much clearer on the position that greater access to encrypted data is necessary than it has been about how that goal should be achieved. Perhaps the most damaging premise advanced by political leadership in the encryption debate is the belief that there is some practical way to facilitate greater state access *en masse* without seriously compromising the security properties of an encryption system or the privacy of its users.[182] The technical reality of such an inherent tradeoff is perhaps best documented by a 2015 report authored by a collection of the world's leading cryptographers from academia and industry entitled "Keys Under Doormats."[183] The report outlines why adopting proposed technical "solutions" would be likely to undermine essential modern security practices such as forward secrecy and authenticated encryption; needlessly increase system complexity (and by extension increase the risk of unauthorized third party access to private data); and create strong incentives for malicious actors to target government credentials and "lawful access" tools with potentially disastrous consequences.[184] In other words, the introduction of technical weaknesses which favour government access to communications and devices would likely also be exploited by foreign state adversaries and criminal actors.

This principle—that there is simply no practical way to weaken or undermine encryption technology without compromising that technology for *all* users—will be revisited repeatedly throughout this report. Nonetheless, some proponents of the "going dark" narrative continue to suggest that it is possible to design encryption systems in a manner that only grants access to legitimate actors while denying it to all others. Proponents of this view appear to have faith that by imposing a legal obligation

---

[179] Reuters (2017), "Australia to Seek Greater Powers on Encrypted Messaging at 'Five Eyes' Meeting", in *The New York Times* (25 June 2017) <*https://www.nytimes.com/reuters/2017/06/13/technology/13reuters-australia-security.html*>; David Wore (2017), "How the Turnbull government plans to access encrypted messages", *The Age* (11 June 2017) <http://www.theage.com.au/federal-politics/political-news/how-the-turnbull-government-plans-to-access-encrypted-messages-20170609-gwoge0.html>; Danny O'Brien (2017), "Five Eyes Unlimited: What A Global Anti-Encryption Regime Could Look Like", *Electronic Frontier Foundation* (29 June 2017) <https://www.eff.org/deeplinks/2017/06/five-eyes-unlimited>.

[180] Public Safety Canada (2017), Five Country Ministerial, Joint Communiqué <https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/fv-cntry-mnstrl-2017/fv-cntry-mnstrl-2017-en.pdf>.

[181] Canadian Internet Policy and Public Interest Clinic (2017), "Coalition Objects to Renewed Calls for Weaker Encryption Following 'Five Eyes' Ottawa Meeting," (June 30, 2017) <https://cippic.ca/en/news/coalition_objects_to_renewed_calls_for_weakened_encryption_following_5eyes_ottawa_meeting>, statement reaffirming the Secure the Internet Coalition statement (2016) <https://www.securetheinternet.org> that:

> "Governments should not ban or otherwise limit user access to encryption in any form or otherwise prohibit the implementation or use of encryption by grade or type;
>
> Governments should not mandate the design or implementation of "backdoors" or vulnerabilities into tools, technologies, or services;
>
> Governments should not require that tools, technologies, or services are designed or developed to allow for third-party access to unencrypted data or encryption keys;
>
> Governments should not seek to weaken or undermine encryption standards or intentionally influence the establishment of encryption standards except to promote a higher level of information security. No government should mandate insecure encryption algorithms, standards, tools, or technologies; and
>
> Governments should not, either by private or public agreement, compel or pressure an entity to engage in activity that is inconsistent with the above tenets."

[182] James Titcomb (2017), "Malcolm Turnbull says laws of Australia trump laws of mathematics as tech giants told to hand over encrypted messages", *The Telegraph* (14 July 2017) <http://www.telegraph.co.uk/technology/2017/07/14/malcolm-turnbull-says-laws-australia-trump-laws-mathematics/>:

> "Well the laws of Australia prevail in Australia, I can assure you of that. The laws of mathematics are very commendable, but the only law that applies in Australia is the law of Australia," he said. "I'm not a cryptographer, but what we are seeking to do is to secure their assistance. They have to face up to their responsibility. They can't just wash their hands of it and say it's got nothing to do with them."

[183] Harold Abelson et. al. (2015), "Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications" (2015) <https://www.schneier.com/academic/paperfiles/paper-keys-under-doormats-CSAIL.pdf>.

[184] *Ibid* at 2.

to develop a technical solution upon cryptographers or the private sector, such a solution will materialize.[185] However, this wishful thinking has been rejected by the full spectrum of policy actors including, at times, by governments and investigative agencies themselves.[186]

In response to the problem of "going dark," a number of policy proposals have emerged from law enforcement and intelligence communities. Some of these proposals would leverage existing legal powers while others would require legislative change. Before turning to a more detailed examination of these proposals in Part 4 of this report, it is helpful to explore Canada's 2016 National Security Consultation in greater detail, as it forms the backdrop upon which any proposal from the Canadian government is likely to be advanced.

ii. The Canadian National Security Consultation

In the fall of 2016, the Canadian federal government undertook a large-scale public consultation on matters of national security.[187] In addition to soliciting input on matters of oversight, accountability, government surveillance, and general national security reform, the consultation materials appeared to set the stage for a renewed debate surrounding investigative and intelligence-gathering challenges posed by modern communications systems. Civil society advocates and academics raised alarm regarding the possibility that this consultation exercise would later serve to justify the introduction of greater and more

---

[185] Ellen Nakashima (2017), "FBI Chief Calls Encryption a "Major Public Safety Issue", *Washington Post* (9 January 2017) <https://www.washingtonpost.com/world/national-security/fbi-chief-calls-encryption-a-major-public-safety-issue/2018/01/09/29a04166-f555-11e7-b34a-b85626af34ef_story.html>:

> "[FBI Director Christopher] Wray acknowledged the solution is not 'clear cut' … I just do not buy the claim that it is impossible."

Nick Evershed (2017), "Australia's Plan to Force Tech Giants to Give Up Encrypted Messages May Not Add Up", *The Guardian* (14 July 2017) <https://www.theguardian.com/technology/2017/jul/14/forcing-facebook-google-to-give-police-access-to-encrypted-messages-doesnt-add-up>:

> "Seemingly contradictory statements aside, and without yet seeing the legislation, it looks as if the government is going to lay out the requirements for tech companies and then let the companies themselves work out the methods."

United States (2017), Department of Justice, Deputy Attorney General Rod J Rosenstein, "Remarks on Encryption at the United States Naval Academy" (remarks as prepared for delivery) (10 October 2017) <https://www.justice.gov/opa/speech/deputy-attorney-general-rod-j-rosenstein-delivers-remarks-encryption-united-states-naval>:

> "The proposal that providers retain the capability to make sure evidence of crime can be accessed when appropriate is not an unprecedented idea. Such a proposal would not require every company to implement the same type of solution. The government need not require the use of a particular chip or algorithm, or require any particular key management technique or escrow. The law need not mandate any particular means in order to achieve the crucial end: when a court issues a search warrant or wiretap order to collect evidence of crime, the provider should be able to help."

[186] Peter Swire & Kenesa Ahmad (2012), "Encryption and Globalization", 23 *Columbia Sci & Tech L Rev* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1960602, at 440-41 and footnote 53:

> "Any government is inclined to listen closely to law enforcement and national security advisors when they warn against problems caused by new technology. Over time, however, two basic conclusions became clear: (1) strong cryptography is essential to the growth and success of an open network such as the Internet; and (2) no technical fix, such as key escrow, was available to provide access only to the 'good guys' but not the 'bad guys.'"

See also Europol and the European Union Agency for Network and Information Security (2016), "Joint Statement on lawful criminal investigation that respects 21st century data protection," (May 20, 2016) <https://www.europol.europa.eu/publications-documents/lawful-criminal-investigation-respects-21st-century-data-protection-europol-and-enisa-joint-statement-0>:

> "Solutions that intentionally weaken technical protection mechanisms to support law enforcement will intrinsically weaken the protection against criminals as well, which makes an easy solution impossible. So far, we observe a continued arms race between cryptographers and crypto-analysts. In terms of practical breaks, cryptographers are currently miles ahead, which is good news for all the legitimate users who can benefit from the improving protection of their data."

See also RCMP Commissioner Bob Paulson (2015), "Keynote Address at the Securetech 2016 Conference", *Royal Canadian Mounted Police* (25 November 2015) <http://www.rcmp-grc.gc.ca/en/news/2015/27/commissioner-bob-paulson-presents-keynote-address-securetech-2015-conference>:

> "Now... about going dark; the encryption that is developing and providing all sorts of advantages and ... I don't want to insult you by suggesting that there aren't commercial competitive advantages to having your communications encrypted, there are. That ought not to be the Holy Grail of policing as we enter the technological world. ... [T]he idea of going dark is not a new one. I was thinking of this as I came to speak to you here at noon. I used to chase bikers out on the West Coast, ... they were very difficult to catch, because they had gone dark. And they hadn't gone dark technologically, they had gone dark in their behaviours. ... The solution couldn't have been to make them use their phones. That's not going to work. We're not going to create a law that says, ok, if you are organized crime, you must use your communication devices so that the police can intercept them. ... We had to change our thinking, and we had to engage key partners in communities with regulatory powers, with other powers to be able to bring the full weight of an organized society to bear on criminal conduct that was going unchecked. ... So the similar approach needs to be brought, I think, to technology. We're chasing the wrong Holy Grail."

[187] Canada (2016), Consultation on National Security <https://www.canada.ca/en/services/defence/nationalsecurity/consultation-national-security.html>.

intrusive surveillance powers and, as outlined below, the document identifies encryption as a specific challenge requiring potential legislative solutions.[188]

As part of the process, the federal government established an online questionnaire consisting of over 60 open-ended (and frequently leading) questions on ten themes, including the following:

> "If the Government were to consider options to address the challenges encryption poses in law enforcement and national security investigations, in what circumstances, if any, should investigators have the ability to compel individuals or companies to assist with decryption?"
>
> [and]
>
> "How can law enforcement and national security agencies reduce the effectiveness of encryption for individuals and organizations involved in crime or threats to the security of Canada, yet not limit the beneficial uses of encryption by those not involved in illegal activities?"

The consultation process was accompanied by a Green Paper as well as a 75-page background document. Together, they served to illuminate the federal government's thinking—at least as of mid-2016—on the issue of encryption. These materials identified "the use of advanced encryption techniques that can render messages unreadable" as one of four primary threats to investigative capabilities in the digital sphere.[189] While acknowledging the technical and economic benefits of encryption, the report also points to how encryption tools impose limits on government agencies' abilities to detect, investigate, and prosecute wrongdoers.[190] It also suggests that the Canadian government intends (or intended) to conduct an internal review of the 1998 Cryptography Policy.

As examples of potential policy responses, the background materials make reference to compelled decryption powers in the United Kingdom under the *Regulation of Investigatory Powers Act, 2000,* the history of attempts in the United States to introduce hardware backdoors to circumvent encryption (including the "Clipper Chip" proposals of the 1990s), and the dispute between Apple and the FBI over a secured iPhone that arose in the context of the 2015 San Bernardino shooting case.[191] The authors of the consultation documents note that such efforts have been considered controversial and acknowledge that in Canada, "no provisions specifically designed to compel decryption are found in the *Criminal Code*, the *CSIS Act* or in other Canadian laws. In other words, there is no law in Canada designed to require a person or organization to decrypt their communications."[192]

The background materials also recognized the general importance of considering human rights, the investigative needs of law enforcement and national security agencies, commercial interests, the integrity of existing digital infrastructure, cybersecurity concerns and the value of e-commerce in designing encryption policy. However, the report did not explain how consideration of these various interests should be weighed, balanced, or understood in relation to each other. It also failed to explore the availability or sufficiency of various alternative tools that were already available to state agencies seeking access to encrypted data, and did not recognize the broader investigative and intelligence windfalls that have resulted from ubiquitously networked modern life. While the materials identified specific instances where encryption was likely to increase the difficulty or cost of certain investigative or intelligence-gathering initiatives, they failed to demonstrate any pressing need capable of justifying the vast security and human rights costs at stake.

---

[188] Micheal Vonn (2016), "A different shade of Green Paper: What the government forgot to mention", (28 November 2016) *British Columbia Civil Liberties Association* <https://bccla.org/2016/11/a-different-shade-of-green-paper-what-the-government-forgot-to-mention/>; Tamir Israel & Christopher Parsons (2016), "Canada's National Security Consultation I: Digital Anonymity & Subscriber Identification Revisited… Yet Again", *Canadian Internet Policy & Public Interest Clinic & Citizen Lab* (5 October 2016) <https://cippic.ca/en/news/national_security_consultation_revisiting_online_anonymity_yet_again>.

[189] Public Safety Canada (2016), Our Security, Our Rights", Green Paper <https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-scrt-grn-ppr-2016/index-en.aspx> at 18.

[190] Public Safety Canada (2016), "Our Security, Our Rights", Background Paper <https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-scrt-grn-ppr-2016-bckgrndr/index-en.aspx> at 60.

[191] *Ibid* at 60.

[192] *Ibid* at 61.

The consultation generated substantial input from expert and individual Canadians, including in a series of town halls and over 59,000 responses to an online questionnaire.[193] The government commissioned an independent study to evaluate the responses from the public—the report concluded that "a clear majority of participants oppose giving government the capacity to intercept personal communications, even if a court authorizes the interception, and oppose any moves to weaken encryption technology."[194] The report preceded to state that almost half of the online respondents felt that the investigative tools that were available to government agencies were already sufficient, and that "giving investigators updated tools would only increase the power of investigative authorities to collect private data, install a backdoor on encryption or otherwise infringe on Canadians' rights."[195] The report also included the following passage on the possibility of new powers to compel decryption or to enlist intermediaries with the process of undermining the security of encrypted systems:

> "Views were equally strong against giving investigators the ability to compel individuals or companies to assist with decryption. A clear majority of civil liberties, legal, academic and industry organizations whose submissions addressed this issue believe strong encryption is vital to protecting privacy and maintaining freedom of expression. Many organizations opposed "backdoors" for law enforcement because they would weaken network security and leave them vulnerable to attack, with industry organizations stressing that encryption technologies are essential to promote trust in the system. Law enforcement said that, while the Framework should seek to maintain security for law-abiding citizens, it should also give authorities the tools they need to access the communications of those who use secure communications technologies for criminal purposes."[196]

While legislative proposals emerging from this consultation have not yet directly addressed the "going dark" challenge, the issue remains a live policy issue in Canada and among its Five Eye partners. To this end, it is helpful to keep both the substantive contents and the political context of the 2016 consultation in mind when discussing the future of the encryption debate in Canada.

---

[193] Public Safety Canada (2017), "National Security Consultations: What We Learned Report" <https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2017-nsc-wwlr/index-en.aspx>.

[194] *Ibid* at 13.

[195] *Ibid*.

[196] *Ibid* at 14.

PART 4: EVALUATING RESPONSES TO THE ENCRYPTION PROBLEM

Governments worldwide have sought to control access to strong encryption technology using a complex array of legal, technical, and economic measures over the course of the last four decades. In this section, we canvas the full spectrum of policy responses to the encryption "problem," including historical examples, present-day proposals, and emerging legal responses in Canadian law.[197] The section proceeds in three parts. First, we explore policy responses that aim to systemically limit the use of effective encryption technology by the public at large. This includes the criminalization and censorship of encryption tools, as well as the largely historical use of export controls. We also discuss historical limits imposed by governments regarding key length and choice of algorithm, as well as modern-day calls to restrict the availability of end-to-end encryption, and covert efforts by governments to undermine encryption standards. All of these measures share an intention to limit the public availability of secure encryption capabilities.

In the second part, we review a range of measures generally directed toward intermediaries whose technologies involve the use of encryption (e.g., Internet and telecommunications service providers, file storage companies, and social media and communications platforms). This includes an analysis of the debate surrounding "exceptional access" and various forms of key escrow. We also explore the issue of voluntary private sector action intended to facilitate government access, as well as the imposition of mandatory decryption capabilities, key disclosure, and other forms of assistance mandates on third parties. All of these measures are intended to leverage the roles of various Internet intermediaries, service providers and manufacturers in developing or operating their respective technologies in order to create decryption opportunities. While not presented as imposing limits on the general public availability of secure encryption, they will nonetheless sometimes have that effect.

In the third part, we evaluate policy responses that target the encrypted devices or accounts of specific individuals. We review the issue of compelled decryption and compelled key disclosure in the context of criminal law search and seizure as well as related powers, including both the common law power of "search incident to arrest," and the search and questioning that occurs in the cross-border context. We also discuss other forms of mandatory key disclosure that may have a less direct impact on the rights of individuals. The common feature in these measures is an attempt to enlist an individual in the decryption of their own devices and accounts, or those of their communication partners.

Among Canada's allies, the possibility of sweeping anti-encryption legislation regularly looms large in public debate. Yet there is no perfect taxonomy or hierarchy that can perfectly describe policy responses to the encryption "problem" on the basis that proposed measures are highly varied and practice there is often considerable overlap between categories. For example, government actors in some countries have been known to target certain individuals because their professional role grants them privileged access to their employer's security infrastructure, making the service provider they work for the ultimate target.[198] In other cases, law enforcement will attempt to deputize a large-scale service provider and their full range of engineering capabilities in order to secure evidence against a single individual or small group.[199] An investigative technique will often appear targeted at first glance but may involve significant and widespread collateral impacts on uninvolved individuals and interests on closer inspection. In other cases, a measure might appear to apply to all actors equally but, in practice, have a disproportionate impact on only a small number of individuals or a particular subgroup.

Nonetheless, the framework set out in this section is likely to be a helpful starting point for most readers. It may also be useful to make reference to the factors enumerated in Box 3 when evaluating a given investigative technique, policy response, or legal power. Among those factors, it may be particularly valuable to consider (1) whether the measure in question is truly targeted, as opposed to whether there is the possibility of larger-scale or systemic impacts on the rights and interests of uninvolved parties; (2) whether there is an element of conscription or coercion which may raise an issue of self-incrimination or unfairly impact the interests of a third party; (3) whether the response remains both truly necessary and truly proportionate.

---

[197] In practice, law enforcement and intelligence agencies already employ a wide variety of technical and legal capabilities that allow them to circumvent the presence of encryption technology without systematically interfering with the technology itself. We discuss some of the investigative powers already available to Canadian authorities and question the necessity of introducing new ones in **Part 5**.

[198] See e.g., Ryan Gallagher and Peter Maass (2014), "Inside the NSA's Secret Efforts to Hunt and Hack System Administrators", *The Intercept* (20 March 2014) <https://theintercept.com/2014/03/20/inside-nsa-secret-efforts-hunt-hack-system-administrators/>.

[199] See e.g., Ryan Singel (2007), "Encrypted Email Company Spills to Feds", *Wired* (7 November 2007) <https://www.wired.com/2007/11/encrypted-e-mai/>; Ryan Singel (2007), "Hushmail to Warn Users of Law Enforcement Backdoor", *Wired* (19 November 2007) <https://www.wired.com/2007/11/hushmail-to-war/>.

INFORMATION BOX 3: FACTORS FOR COURTS AND POLICYMAKERS TO CONSIDER IN EVALUATING POLICY RESPONSES TO ENCRYPTION

In evaluating any of the legal or policy measures described in this report, courts and policymakers will often be required to engage in complex balancing exercises that account for a large number of competing interests and values. While not exhaustive, the following list of factors may provide a helpful starting point in evaluating whether a given measure is both constitutionally sound and contextually appropriate:

- the lawful basis for the measure's use;
- the specific underlying government objective which justifies its use;
- the necessity of the measure in achieving a specific government objective;
- the nature of the actors with the lawful authority and/or the technical ability to conduct the measure in question;
- the cost, difficulty, or resource-intensive nature of the measure, and who bears the associated costs;
- the scope and number of individuals targeted;
- the direct and indirect impact on *Charter*-protected rights and liberties, notably including freedom of expression, freedom from unreasonable search and seizure, and the rights to silence and against self-incrimination;
- the international and extraterritorial impacts of the measure;
- the impact on Canada's foreign policy interests;
- the direct and indirect impact on the internationally recognized human rights of non-Canadians outside of Canada, including to freedom of expression, privacy, security, and other rights;
- the extent to which the measure can or does cause collateral harm to non-targeted individuals and other entities, including both the general public (e.g., to their security or rights) and private actors (e.g., to their economic interests or reputation);
- the steps, if any, that can be taken to minimize and mitigate potential collateral impact;
- the potential chilling effect on legitimate conduct, including the extent to which the measure may impact public trust in the security of digital storage and communications mechanisms or weaken consumer confidence in service providers and IT companies;
- whether the measure requires the active participation of the targeted individual (and if so, whether that conscription impairs the individual's constitutional right to silence and protection against self-incrimination);
- the extent to which the measure requires the active participation of an intermediary or third party (and if so, the impact of this imposition on the third party and its interests);
- whether the measure is undertaken overtly or covertly;
- in the case that the measure is authorized secretly or *ex parte,* the extent to which safeguards exist to protect the affected party (or parties), the public interest, and the rule of law;
- the potential for the use of the measure in question to undermine public trust in legal and democratic institutions, such as robust news reporting embodied in a free press, critical public advocacy as implemented by civil society and other social movement actors, the deliberative political process and the integrity of its elected officials, or to bring the administration of justice into disrepute;
- whether any reasonable alternative measures exist which may achieve the same purpose in a manner which is more minimally impairing of the rights and interests at stake.

Finally, and as with all matters of government surveillance and access to data, policy discussions should be guided by the fundamental and overarching principles of necessity and proportionality.[i]

[i] Necessary and Proportionate Coalition (2014), "International Principles on the Application of Human Rights to Communications Surveillance," launched at the United Nations Human Rights Council in Geneva in September 2013, Final Version (May 2014) <https://necessaryandproportionate.org/principles>.

A. EFFORTS TO LIMIT PUBLIC ACCESS AND USE OF ENCRYPTION TOOLS

Many states have attempted to regulate encryption by restricting or limiting access to the technology outright. The objective of these policy measures is to limit the availability of secure and effective encryption technology for commercial or civilian use, effectively reserving strong encryption for military, intelligence, or other government purposes.

These limits have taken many forms, including outright criminalization and censorship of encryption tools—typically by requiring Internet or mobile service providers to block access to third party applications at the network layer. Prohibitions on the use of certain key lengths, limits on choice of algorithm, or restrictions on the type of encryption system—including proposed bans on end-to-end encryption—also amount to a *de facto* limit on the public availability of strong and effective encryption. These limitations are intended to preclude the use of truly secure encryption technology by the general public, leaving consumers only the options that government (and other third parties) can exploit or circumvent. Some states have also maintained restrictions on the *export* of encryption tools or mechanisms but not on their domestic use. Such restrictions, though foreign-facing, have often operated as a limit on domestic development of encryption tools, as there are often strong economic incentives to develop encryption tools that can be marketed globally and distributed on the Internet. Finally, some government agencies have sought to limit public use of encryption by covertly undermining key protocols and encryption standards. In the past, this has been accomplished by subverting standards-making processes.

Restrictions designed to limit the public availability of encryption tools often fail to meet their objective. Encryption software can be distributed globally on the Internet, which means that local bans will not automatically prevent international availability. The result is that such bans may require extensive surveillance and censorship mechanisms to enforce. Attempts to reduce the widespread public use of encrypted communications have often focused on popular services and devices (e.g., WhatsApp, Telegram, the iPhone). However, denying populations the benefit of these services has generally proven unpopular and difficult to sustain. Censorship of foreign-based encryption services has also often been ineffective in the longer term. While such censorship may result in short-term confusion as users switch to an alternative, or cause a chilling effect on legitimate communications, censorship is unlikely to discourage highly motivated actors.[200] The outcome might then be that while the general public is deprived of access to secure communications, those actively seeking to do wrong—the purported targets of the generalized limitation—will continue to interact securely.

The types of measures explored in this section are inherently disproportionate even when they frequently fail to fully meet their state objectives. They seek to chill the use of secure encryption tools of general application, resulting in reduced security for all users. In general, measures that undermine privacy, free expression and the integrity of communications in a systematic and untargeted manner are problematic from a human rights perspective.[201] In the modern era, no state has advanced the proposition that secure encryption is inherently negative, but instead that dramatic public limits are necessary in order to prevent a small subset of society from interacting securely for criminal purposes. These measures always impose a high collateral cost. They may also impose a significant burden on secure communications providers because they require them to undermine the very core of their service.[202] Finally, many attempts to limit the broader public use of encryption tools have been held, at least in some jurisdictions, to amount to a limit on freedom of expression, particularly where security researchers are restricted from publishing code relating to encryption tools in public.[203]

---

[200] Brad Haynes (2016), "Brazil Judge Briefly Blocks WhatsApp Over Criminal Case", *Reuters* (19 July 2016) <https://www.reuters.com/article/us-brazil-facebook-whatsapp-ruling/brazil-judge-briefly-blocks-whatsapp-over-criminal-case-idUSKCN0ZZ2PQ>; Staff and Agencies (2016), "WhatsApp Officially Un-Banned in Brazil After Third Block in Eight Months", *The Guardian* (19 July 2016) <https://www.theguardian.com/world/2016/jul/19/whatsapp-ban-brazil-facebook>; Luciana Magalhaes (2016), "Brazil's Supreme Court Lifts Block on WhatsApp", *Wall Street Journal* (19 July 2016) <https://www.wsj.com/articles/court-orders-block-to-whatsapp-chat-service-in-brazil-1468952805>.

[201] See e.g., Office of the United Nations High Commissioner for Human Rights (2014), "The right to privacy in the digital age" A/HRC/27/37, (30 June 2014) at para 26; Sarah St Vincent, "Preventing the Police State: International Human Rights Laws Concerning Systematic Government Access to Communications Held or Transmitted by the Private Sector", in Fred H Cate & James X Dempsey, *Bulk Collection: Systematic Government Access to Private-Sector Data* (Oxford Scholarship Online, 2017), <http://www.oxfordscholarship.com/view/10.1093/oso/9780190685515.001.0001/oso-9780190685515-chapter-19>; *S and Marper v United Kingdom*, App No 30563/04 (4 December 2008) (ECHR Grand Chamber).

[202] Case C-360/10, *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v Netlog NV*, [2012] ECR I-0000, (Court of Justice of the European Union, Third Chamber) at paras 46-47.

[203] *Bernstein v Department of Justice*, 922 F.Supp. 1426 (1996, ND Calif); *Bernstein v Department of Justice*, 945 F.Supp. 1279 (1996, ND Calif); aff'd 176 F.3d 1132 (1999, US 9th Circuit).

In the remainder of this section, we outline the spectrum of measures used or contemplated by governments in their attempts to limit the public availability and use of secure encryption, referring to some of the particular contextual challenges that have emerged in respect of each proposal.

i. Criminalization and Encryption Bans

The use or possession of certain kinds of encryption tools by end-users has been explicitly outlawed or subject to significant criminal law restrictions in some foreign jurisdictions, including in countries such as China, India, Senegal, Egypt and Pakistan.[204] In many cases, regulatory measures short of explicit criminalization may "be tantamount to a ban" in practice.[205] For example, in Ethiopia the combination of the facts that the government "criminalizes the manufacture, assembly or import of any telecommunications equipment without a permit" and that it determines legally allowable technical standards together amount to a ban on non-government controlled encryption technology.[206] Such measures have the effect of preventing persons and companies from developing or adopting strong and secure communications technologies that serve to shield communications and stored documents from unlawful access by third parties.

ii. Censorship of Encryption Tools

Internet censorship is also used to restrict public access to encryption software and anonymity tools. In particular, messaging applications offering end-to-end encryption features such as Whatsapp and Signal are frequently blocked by governments. In countries such as Ethiopia, Bahrain, Bangladesh and Uganda, communications platforms and secure messaging tools are routinely censored in response to anti-government protests.[207] In 2017, the Chinese government engaged in major disruption of public access to Whatsapp.[208] These applications are often blocked because encryption tools facilitate free and open communications online and thwart efforts to censor content by authoritarian governments.[209]

This kind of censorship has proven difficult to sustain. For example, in 2016, the Government of Egypt reportedly blocked the Signal application from operating on Egyptian networks, but the application's developers bypassed the censorship within a matter of days.[210] Then, in 2017, Afghan telecommunications companies were ordered by the Afghanistan government to block access to WhatsApp and Telegram, while one major telecommunications company rendered both applications inoperable to its customers.[211] It is not clear whether the blocking order, which appears to have been secretly prompted by Afghanistan's intelligence agency, was intended to be permanent or temporary, but the decision was quickly reversed following a public uproar.[212] In 2016, a Brazilian court ordered all Brazilian telecommunications service providers to block WhatsApp because the

---

[204] Article 19 (2015), "Right to Online Anonymity", Policy Brief (June 2015) <https://www.article19.org/data/files/medialibrary/38006/Anonymity_and_encryption_report_A5_final-web.pdf> at 29.

[205] David Kaye (2015), Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/29/32, <http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/Pages/ListReports.aspx> at paras 40-41.

[206] *Ibid.*

[207] Freedom House (2016), "Silencing the Messenger: Communication Apps Under Pressure," Freedom on the Net 2016 Report <https://freedomhouse.org/report/freedom-net/freedom-net-2016>.

[208] Paul Mozur (2017), "China Disrupts WhatsApp Service in Online Clampdown," *The New York Times* (18 July 2017) <https://nytimes.com/2017/07/18/technology/whatsapp-facebook-china-internet.html>.

[209] Jonathan Zittrain, Robert Faris, Helmi Noman, Justin Clark, Casey Tilton, and Ryan Morrison-Westphal (2017), "The Shifting Landscape of Global Internet Censorship", Berkman Klein Center for Internet & Society Research Publication <http://nrs.harvard.edu/urn-3:HUL.InstRepos:33084425> at 1.

[210] Farid Y. Farid (2016), "No Signal: Egypt blocks the encrypted messaging app as it continues its cyber crackdown", TechCrunch (26 December 2016) <https://techcrunch.com/2016/12/26/1431709/>; Mariella Moon, "Egypt Has Blocked Encrypted Messaging App Signal", *Engadget* (20 December 2016), <https://www.engadget.com/2016/12/20/egypt-blocks-signal/>; Andy Greenberg, "Encryption App 'Signal' Fights Censorship with a Clever Workaround", *Wired* (21 December 2016) <https://www.wired.com/2016/12/encryption-app-signal-fights-censorship-clever-workaround/>.

[211] Mujib Mashal & Fatima Faizi (2017), "Afghanistan Acts to Ban WhatsApp, but Claims Move is Temporary", *New York Times* (3 November 2017) <https://www.nytimes.com/2017/11/03/world/asia/afghanistan-whatsapp-ban.html>.

[212] Mujib Mashal & Fatima Faizi (2017), "Afghanistan Acts to Ban WhatsApp, but Claims Move is Temporary", *New York Times* (3 November 2017) <https://www.nytimes.com/2017/11/03/world/asia/afghanistan-whatsapp-ban.html>; Ezzatullah Mehrdad (2017), "When Citizens Rejected a Ban on WhatsApp and Telegram, Afghan Officials Backed Down", *Global Voices* (15 November 2017) <https://globalvoices.org/2017/11/15/__trashed/>; Reuters Staff (2017), "Afghanistan Will Not Block WhatsApp, Telegram: Spokesman", *Reuters* (6 November 2017) <https://www.reuters.com/article/us-afghanistan-internet/afghanistan-will-not-block-whatsapp-telegram-spokesman-idUSKBN1D61VI>.

company had failed to comply with an order to intercept user messages.[213] WhatsApp's refusal was on the basis of technical infeasibility—because the application employs end-to-end encryption, intercepting the content of user communications would require significant re-engineering of the company's service.[214] Brazil's highest court overturned the order hours after Whatsapp was blocked on the basis that it violated Brazilians' constitutional right to freedom of expression.[215] In overturning the decision, Federal Supreme Court President Ricardo Lewandowski found it was "scarcely reasonable or proportional" to block the application, which at that time was by roughly half of Brazil's 200 million citizens, "including members of the judiciary."[216] Ultimately, blocking of strong encryption tools has significant, and disproportionate, impacts insofar as it inappropriately interferes with the rights of all users.

iii. Limits on Key Length, Choice of Algorithms, or Use of End-to-End Encryption

In some jurisdictions, governments have sought to explicitly prohibit domestic commercial use of cryptographic technologies that exceed a certain key length—essentially mandating that "legal" encryption will not protect users against government attacks or circumvention. Regulations that designate a list of lawful encryption algorithms have similarly been used to facilitate government access to encrypted communications and to weaken the technical protection available to end users. This type of approach was more effective when encryption tools were developed by a small number of entities and were not otherwise widely available to ordinary users. In some countries, these types of rules apply on a sector-by-sector basis. The Government of China, for example, reportedly compels the use of state-approved encryption algorithms and prior regulatory approval is required by those wishing to operate Virtual Private Networks (VPNs) in Pakistan.[217] In India, telecommunications law nominally permits the government to impose licensing conditions on any electronic communications providers. Historically, the Department of Telecommunication has relied upon this authority to impose licensing conditions on Internet service providers so that the deployment of symmetric algorithms using key lengths in excess of 40 bits or their equivalents without prior approval is prohibited.[218] However, in India this low bar has not been applied to "over the top" services (including applications installed directly by users themselves), meaning that tools using higher encryption standards "are currently operating in a grey area" with no explicit prohibition in place.[219]

Essentially, the purpose of these types of regulations is to limit the software that is lawfully available to the public to only those technologies that the government has the ability to easily subvert or circumvent. In many cases such regulations are inherently incompatible with basic consumer security. Where they are imposed at the national level, prohibitions of this type essentially force global platforms to choose between redesigning their services so that these are less secure for all users around the world or risk becoming criminalized in particular jurisdictions.

---

213 Luciana Magalhaes (2016), "Brazil's Supreme Court Lifts Block on WhatsApp", *Wall Street Journal* (19 July 2016), <https://www.wsj.com/articles/court-orders-block-to-whatsapp-chat-service-in-brazil-1468952805>.

214 Brad Haynes (2016), "Brazil Judge Briefly Blocks WhatsApp Over Criminal Case", *Reuters* (19 July 2016), <https://www.reuters.com/article/us-brazil-facebook-whatsapp-ruling/brazil-judge-briefly-blocks-whatsapp-over-criminal-case-idUSKCN0ZZ2PQ>.

215 Luciana Magalhaes (2016), "Brazil's Supreme Court Lifts Block on WhatsApp", *Wall Street Journal* (19 July 2016) <https://www.wsj.com/articles/court-orders-block-to-whatsapp-chat-service-in-brazil-1468952805>.

216 Brad Haynes (2016), "Brazil Judge Briefly Blocks WhatsApp Over Criminal Case", *Reuters* (19 July 2016) <https://www.reuters.com/article/us-brazil-facebook-whatsapp-ruling/brazil-judge-briefly-blocks-whatsapp-over-criminal-case-idUSKCN0ZZ2PQ>; Staff and Agencies (2016), "WhatsApp Officially Un-Banned in Brazil After Third Block in Eight Months", *The Guardian* (19 July 2016) <https://www.theguardian.com/world/2016/jul/19/whatsapp-ban-brazil-facebook>; Luciana Magalhaes (2016), "Brazil's Supreme Court Lifts Block on WhatsApp", *Wall Street Journal* (19 July 2016) <https://www.wsj.com/articles/court-orders-block-to-whatsapp-chat-service-in-brazil-1468952805>.

217 David Kaye (2015), Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/29/32, <http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/Pages/ListReports.aspx> at paras 40-41, citing China, Counter-terrorism Law, art. 15 (initial draft of 8 November 2014) available from <http://chinalawtranslate.com/en/ctldraft>, final 2015 version of the law available here: <http://www.chinalawtranslate.com/bilingual-counter-terrorism-law/?lang=en> and citing Government of Pakistan, Pakistan Telecommunications Authority, "Use of VPNs/Tunnels and/or Non-Standard SS7/VoIP Protocols," 17/1/2010/Enf/PTA (VPN) <www.ispak.pk/Downloads/PTA_VPN_Policy.pdf>.

218 Wolfgang Schulz & Joris van Hoboken (2016), "Human Rights and Encryption," UNESCO Series on Internet Freedom <http://unesdoc.unesco.org/images/0024/002465/246527E.pdf> at 41.

219 Software Freedom Law Centre, India (2017), "FAQ: Legal Position of Encryption in India", *SFLC.in* (11 November 2017) <https://sflc.in/faq-legal-position-encryption-india>.

There are a number of recent examples of this type of proposal. As noted above, Indian law theoretically empowers the Indian government to impose conditions on any electronic communications, including limitations on encryption.[220] A draft regulation was advanced in 2015 by Indian officials who sought to prevent the use of encryption by compelling various entities to maintain and store plaintext versions of any encrypted data for 90 days and to be able to make it available to security agencies on demand.[221] While reports differ as to whether the draft regulation would have applied to all individuals or only to various communications providers or social media sites, it was hastily withdrawn following a far-reaching public outcry.[222] In another attempt, a self-professed right-to-information activist petitioned the Indian judicial system to impose a ban on secure instant messaging applications, including WhatsApp, on the basis that secure communications threaten national security and violate a number of Indian laws that establish the Indian government's authority to intercept communications.[223] The Indian Supreme Court denied the petition but left the door open to a comparable ban initiated by India's telecommunications authority.[224]

In the United Kingdom, the *Investigatory Powers Act (2016)* appeared to grant the Secretary of State the capacity to issue technical capability orders that could effectively ban the use of secure encryption. The technical notices, if issued, would compel service providers to remove any "electronic protection" applied by it or on its behalf to any communications or data.[225] The new powers were highly controversial when initially presented, and the obligation to consider "technical feasibility" when imposing such conditions was added as a result of pressure from the public and from companies such as Facebook—these companies were concerned the regulations would render their current services illegal in the United Kingdom.[226] It remains unclear whether the boundaries of "technical feasibility" will require service providers such as WhatsApp or Signal to completely re-engineer their services in a manner that allows for the interception of plaintext data. Certainly it is technically feasible to create a messaging service that lacks the robust end-to-end encryption of WhatsApp and Signal, and many such services exist. However, doing so would require the provider in question to completely redesign its service and remove core features of its product—in other words, to become an entirely *different* service altogether. In other contexts, European law has precluded the imposition of such far-ranging redesign obligations. For example, in *Netlog v SABAM*, the Third Chamber of the Court of Justice of the European Union held that compelling a social media site (Netlog) to install a content filtering system that would identify and delete copyright infringing materials imposed an excessive and unjustifiable disruption of Netlog's service:

> [S]uch an injunction would result in a serious infringement of the freedom of the hosting service provider to conduct its business since it would require that hosting service provider to install a complicated, costly, permanent computer system at its own expense … it must be held that the injunction to install the contested filtering system is to be regarded as not respecting the requirement that a fair balance be struck between, on the one hand, the protection of the intellectual-property right enjoyed by copyright holders, and, on the other hand, that of the freedom to conduct business enjoyed by operators such as hosting service providers.[227]

---

[220] Wolfgang Schulz & Joris van Hoboken (2016), "Human Rights and Encryption," UNESCO Series on Internet Freedom <http://unesdoc.unesco.org/images/0024/002465/246527E.pdf> at 41.

[221] Ellen Barry (2015), "India Retracts Proposal on Encryption for Social Media Data After Outcry", *New York Times* (22 September 2015) <https://www.nytimes.com/2015/09/23/world/asia/india-withdraws-social-media-data-proposal-after-outcry.html>.

[222] *Ibid*; BBC News (2015), "India Withdraws Controversial Encryption Policy", *BBC News* (22 September 2015) <http://www.bbc.com/news/world-asia-india-34322118>.

[223] Mohul Gosh (2016), "Petition to Ban WhatsApp in India Filed in Supreme Court", *Trak.in* (3 May 2016) <http://trak.in/tags/business/2016/05/03/whatsapp-ban-india>.

[224] Krishnadas Rajagopal (2016), "No Ban on WhatsApp: Supreme Court", (29 June 2016) <http://www.thehindu.com/news/national/No-ban-on-Whatsapp-Supreme-Court/article14408732.ece>.

[225] United Kingdom, *Investigatory Powers Act 2016,* c. 25 at paragraph 253(5)(c).

[226] United Kingdom, *Investigatory Powers Act 2016,* c. 25, sub-section 255(4):

> "In the case of a technical capability notice that would impose any obligations relating to the removal by a person of electronic protection applied by or on behalf of that person to any communications or data, in complying with subsection (3) the Secretary of State must in particular take into account the technical feasibility, and likely cost, of complying with those obligations."

[227] Case C-360/10, *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v Netlog NV*, [2012] ECR I-0000, (Court of Justice of the European Union, Third Chamber) at paras 46-47; Note that the CJEU has acknowledged that less intrusive obligations imposed on service providers (and particularly on ISPs) can be imposed to achieve objectives such as copyright enforcement. Contrast Case C-70/10, *Scarlet Extended SA v Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM)*, [2011] ECR I-11959 (Court of Justice of the European Union, Third Chamber) with *UPC Telekabel Wien v Constantin Film Verleigh*, (27 Maruch 2014) (Court of Justice of the European Union, Fourth Chamber). However, as noted in this section, exceptional access solutions in general are highly intrusive, and impose serious collateral impact.

The changes a provider such as Signal or WhatsApp would need to undertake to render its own services interceptable are arguably significantly farther-reaching and more fundamental in nature than than those envisioned by the content filtering system proposed in Netlog. It is therefore not clear whether technical capability notices could successfully be employed by the Secretary of State to ban end-to-end encryption. To date, the U.K. government has not attempted to impose technical notices to achieve this objective, but in 2017, the media reported that WhatsApp refused a non-binding request from the U.K. government "to build a way to give it access to encrypted messages."[228]

Finally, there was some suggestion in the current Canadian federal government's 2016 National Security Consultation background documents that its authors understood "lawful intercept" capabilities and compelled decryption powers as part of an interconnected and mutually enabling package. For example, one of the "scenarios" they provided in the background report anticipated the possibility of securing lawful intercept powers in order to catch a terrorist actor, but being unable to decrypt her communications once intercepted.[229] These concerns were similarly mirrored in a briefing document prepared by the RCMP, which noted that "these barriers are not mutually exclusive. For example, police investigators may have the technological capability to intercept real-time private communications (data-in-motion) under a *Criminal Code* Part VI judicial authorization, but may in turn be unable to decrypt and read this data."[230] As the RCMP summarized in a 2016 briefing document:

> "In some cases, major IT companies have built mobile and other digital devices that enable individuals to encrypt and decrypt data at the user level, and therefore these companies cannot provide technical assistance to government agencies to decrypt or otherwise remove encrypted data found on lawfully seized devices. At present, there is no Canadian legislation that compels TSPs and IT manufacturers to remove their added encryption in response to a court order, even where it is readily possible for them to do so in the context of a judicially authorized interception of data-in-motion or court order for data-at-rest."[231]

It should therefore be noted that where so-called "lawful intercept" legislation requires service providers to engineer capabilities for access to plaintext records or to maintain the capacity to decrypt historical communications data, it can amount to a *de facto* restriction on the use of certain kinds of encryption technology, including end-to-end encryption models or systems that implement forward secrecy.

Ultimately, while governments may seek to impose key length requirements, limits on choice of algorithm, bans on the use of end-to-end encryption, or other restrictions on the kinds of cryptographic technologies available within their jurisdictions, doing so is likely to weaken the availability of secure products to legitimate businesses and consumers alike. Limiting the use of encryption to technology weak enough for the government to break or circumvent also increases ease of access for criminal actors, foreign governments, and other malicious third parties. Furthermore, requiring such limitations may restrict the availability of globally-used communications tools that are essential for business operations and the secure communication of personal information and other sensitive data.

iv. Export Controls

Export controls do not explicitly prohibit domestic use of encryption, but rather impose licensing obligations as a prerequisite to the export of encryption products. Where such controls have historically played a significant role in state efforts to

---

[228] Rob Price (2017), "WhatsApp Reportedly Refused to Build an Encryption Backdoor for the UK Government", *Business Insider* (20 September 2017) <http://www.businessinsider.de/whatsapp-refused-encryption-backdoor-uk-government-report-2017-9>.

[229] See Public Safety Canada (2016), "Our Security, Our Rights," Background Paper <https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-scrt-grn-ppr-2016-bckgrndr/index-en.aspx> at 61 for a particularly relevant scenario:

> "[Continuing the scenario from above] .... The police were finally able to develop intercept capability and obtain court authority again to intercept the communications of Mr. M. To avoid having his plans discovered, however, Mr. M had encrypted his communications, which were unreadable to the police as a result. In addition, the service provider advised the police that it could not help decrypt the communications. After months of investigative delays and despite court authority to intercept the communications of Mr. M, the police cannot read them to obtain potential evidence. As a result, Mr. M's communications remain protected from law enforcement."

[230] Royal Canadian Mounted Police (2016), "Encryption and Law Enforcement" (obtained under the *Access to Information Act* by Christopher Parsons in 2017), <https://cippic.ca/uploads/ATI-RCMP-Encryption_and_Law_Enforcement-2016.pdf>.

[231] *Ibid.*

limit access to encryption technology, they have essentially been abandoned as a tool to do so by Western governments. The early history of cryptographic policy (particularly throughout the 1990s) was often characterized as a battle over the extent to which export controls could prevent the emerging technology sector from building strong cryptography into software "at the heart of the growing Internet."[232] Historically, such controls were seen as chilling domestic research related to cryptography, to the extent that the controls limited publication and international dissemination of cryptographic research. In this regard, export controls have been found by some courts to constitute an unconstitutional restriction on freedom of expression.[233] Many countries worldwide continue to implement some degree of export (and to a lesser extent, import) controls for encryption.[234]

Internationally, the Wassenaar Arrangement, a multinational agreement among 42 states which regulates the export of "dual-use" technologies, provides a framework for encryption-related export controls.[235] Dual-use technologies can be used for civil and commercial purposes while also having significant military applications or the potential to threaten international and national security.[236] Encryption, despite its widespread implementation across nearly all forms of electronic communication and storage technologies, continues to be classified as a "dual use" good under the Arrangement.[237] While the Wassenaar Arrangement is not strictly binding as a matter of international law, Canada, many European countries, and the United States have been Participating States since its inception in 1996, and are expected to include its list of dual-use items in their respective national lists of items subject to domestic export control policies.[238]

The Wassenaar Arrangement provisions on encryption were significantly loosened when a license exemption list for mass-market cryptography exports was expanded in 2009 to include key lengths of any size.[239] Previously, mass market products

---

[232] Harold Abelson et. al. (2015), "Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications" <https://www.schneier.com/academic/paperfiles/paper-keys-under-doormats-CSAIL.pdf> at 8; for an early history see Whitfield Diffie and Susan Landau (2007), "The Export of Cryptography in the 20th Century and the 21st" (Elsevier, 2007) in Karl De Leeuw and Jan Bergstra, *The History of Information Security* at 733.

[233] *Bernstein v Department of Justice*, 922 F.Supp. 1426 (1996, ND Calif); *Bernstein v Department of Justice*, 945 F.Supp. 1279 (1996, ND Calif); aff'd 176 F.3d 1132 (1999, US 9th Circuit).

[234] See e.g., Bert-Jaap Koops (2013), "Summary of International Crypto Controls," (February 2013) version 27.0 <http://www.cryptolaw.org/cls-sum.htm>.

[235] The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies, "Participating States", (last updated 20 December 2017) <http://www.wassenaar.org/participating-states/>.

[236] The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies (1996) Wassenaar Arrangement Secretariat, Vienna, Austria <http://www.wassenaar.org/>.

[237] This, despite the underlying principle animating the Wassenaar Arrangement – to regulate dual-use technologies without obstructing genuine civil transactions.

See Sarah Andrews (2000), "Who Holds the Key? A Comparative Study of US and European Encryption Policies", (2000) 2 *J of Information, L and Tech* <https://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2000_2/andrews/>, footnote 16.

See also List of Dual-Use Goods and Technologies and Munitions List (Category 5), Compiled by the Wassenaar Arrangement Secretariat (February 2017) <http://www.wassenaar.org/wp-content/uploads/2016/12/List-of-Dual-Use-Goods-and-Technologies-and-Munitions-List-Corr.pdf>.

Specifically, Wassenaar lists cryptography for the purpose of data confidentiality and includes cryptography as having "in excess of 56 bits of symmetric key length or equivalent" (equivalency includes cryptography in excess of 512 bits of asymmetric key length and elliptic curves employing key lengths in excess of 112 bits). This excludes encryption used for authentication, data assurance purposes, or to facilitate digital rights management in the copyright context.

See U.S. Department of Commerce, Bureau of Industry and Security, "Key Length Thresholds" <https://www.bis.doc.gov/index.php/policy-guidance/encryption/2-items-in-cat-5-part-2/a-5a002-a-and-5d002-c-1/ii-key-length>; U.S. Department of Commerce, Bureau of Industry and Security, "Cryptography for Data Confidentiality" <https://www.bis.doc.gov/index.php/2-items-in-cat-5-part-2/a-5a002-a-and-5d002-c-1/i-crypto-for-data-confidentiality>.

[238] Government of Canada (1998), "Discussion Paper: A Cryptography Policy Framework for Electronic Commerce--Building Canada's Information Economy and Society", *Industry Canada* <https://cippic.ca/uploads/GoC-Canadas_Cryptographic_Policy-1998.pdf> at 32:

> "Canada is obliged to adhere to the terms of an international agreement with 32 other nations (the 1996 Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-use Goods and Technologies) that stipulates which products require export permits and which do not, but does not prescribe approval or denial of permits. Making changes to match the most liberal policies elsewhere would set Canada apart from the majority of other nations (particularly the United States and our other national security allies), would be seen as an aggressive move within the Wassenaar Arrangement, and may potentially trigger international pressure to adopt a more restrictive policy."

See also: Sarah Andrews (2000), "Who Holds the Key? A Comparative Study of US and European Encryption Policies", (2000) 2 *J of Information, L and Tech* <https://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2000_2/andrews/>, section 3.2.

[239] Electronic Frontier Foundation (2015), "RE: Comments of the Electronic Frontier Foundation on the Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items, RIN 0694AG49" (20 July 2015) <https://www.eff.org/files/2015/07/21/effwassenaarcomments-1.pdf> at 3-4; United States Department of Commerce (2010), Bureau of Industry and Security, "Encryption Export Controls: Revision of License Exception ENC and Mass Market Eligibility, Submission Procedures, Reporting Requirements, License Application Requirements, and Addition of Note 4 to Category 5, Part 2; Interim Final Rule" (25 June 2010) <https://www.gpo.gov/fdsys/pkg/FR-2010-06-25/pdf/2010-15072.pdf>>; Tim Maurer, Edin Omanovic & Ben Wagner (2014), "Uncontrolled Global Surveillance: Updating Export Controls to the Digital Age", *New America Foundation: Open Technology Institute, Digitale Gesellschaft & Privacy International* (March 2014) <https://cihr.eu/wp-content/uploads/2014/06/Uncontrolled-Surveillance_March-2014.pdf> at 32.

employing cryptography in excess of 64 bits symmetric key length were not exempted.[240] While these changes resolved many of the historical issues associated with export restrictions on encryption, the Arrangement continues to be criticized for its continued inclusion of encryption as a "dual-use" technology. This ongoing classification has a chilling effect on the work of security researchers, open source developers and academics and is unsustainable in principle given that encryption is now ubiquitously used for civil and commercial purposes.[241]

Canada's early approach to export controls on encryption was characterized by some tension. The 1998 National Cryptography Policy recognized that export controls have a restrictive impact on industry.[242] The policy included promises "to ensure that Canadian cryptography manufacturers face a level playing field" by accounting for foreign practices, streamlining the export permit process, and reducing "regulatory drag" on exporters.[243] Regardless of this tension, Canada did implement the Wassenaar Arrangement, and even adopted a relatively restrictive interpretation of exceptions designed to facilitate export of mass market products.[244] Little had changed by 2010, when the federal government undertook a series of consultations related to the information security and cryptography items controlled in the Export Control List (ECL) pursuant to the *Export and Import Permits Act*.[245] The restrictions at that time still required a permit to export encryption goods and technology using key lengths in excess of 56 bits (symmetric) to destinations other than the United States (with some exceptions).[246] The rules were widely criticized by industry, which argued that Canadian vendors suffered a competitive disadvantage—particularly when compared to their American counterparts, whose government had relaxed its approach to the export of cryptographic tools since 2000.[247] As a result of the 2010 consultation, Canada expanded its exemption for mass market encryption, effectively decontrolling cryptographic products and technologies that were marketed to the general public in large volumes.[248] However, following the Wassenaar Arrangement, cryptography items remain listed as "dual-use," under the rationale that such items "could also be used for significant military purposes."[249] To the extent controls for cryptography remain in place, they are administered by Global Affairs Canada's Export Controls Division, in partnership with the CSE.[250]

Export controls can have the effect of weakening security, both directly and indirectly, over the long term. Legacy decisions remain integrated into technical infrastructure, even long after the restrictions have been lifted. This can have the effect of allowing weak encryption to be exploited over the long term in broad and unexpected ways, and in ways that may affect large numbers of users and citizens.[251] Repairing such weaknesses often entails entirely replacing built infrastructure, which can be costly and operationally challenging. Having export control restrictions in place can also impact security at the international level, as domestic companies that operate globally may be deterred from developing products that employ effective security so as to

---

[240] Sarah Andrews (2000), "Who Holds the Key? A Comparative Study of US and European Encryption Policies", (2000) 2 *J of Information, L and Tech* <https://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2000_2/andrews/> at footnote 16.

[241] See e.g. Electronic Frontier Foundation (2015), "RE: Comments of the Electronic Frontier Foundation on the Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items, RIN 0694AG49" (20 July 2015) <https://www.eff.org/files/2015/07/21/effwassenaarcomments-1.pdf>; Tim Maurer, Edin Omanovic & Ben Wagner (2014), "Uncontrolled Global Surveillance: Updating Export Controls to the Digital Age", *New America Foundation: Open Technology Institute, Digitale Gesellschaft & Privacy International* (March 2014) <https://cihr.eu/wp-content/uploads/2014/06/Uncontrolled-Surveillance_March-2014.pdf> at 32.

[242] Speaking Notes on "Canada's Cryptography Policy" (1998) for the Honourable John Manley, Minister of Industry, to the National Press Club (1 October 1998) <http://fas.org/irp/news/1998/10/981001-crypto.htm>.

[243] *Ibid.*

[244] John W. Boscariol (2010), "Canadian Government Launches Consultations on Encryption Controls," (9 March 2010) *McCarthy Tetrault* <http://mccarthy.ca/article_detail.aspx?id=4896>.

[245] Export Controls Division (2010), Department of Foreign Affairs and International Trade (DFAIT), "Export Controls on Information Security (Cryptography) Items" (9 July 2010) on McCarthy Tetrault website <http://mccarthy.ca/pubs/Industry_Consultation_Framework_Paper_July92010.pdf>.

[246] John W. Boscariol (2010), "Canadian Government Launches Consultations on Encryption Controls," (9 March 2010) *McCarthy Tetrault* <http://mccarthy.ca/article_detail.aspx?id=4896>.

[247] *Ibid.*

[248] Note 3 to Group 1, Category 5, Part 2, See: Global Affairs Canada, A Guide to Canada's Export Controls - Groups 1 and 2, (last modified 28 February 2014) <http://www.international.gc.ca/controls-controles/about-a_propos/expor/guide-2011.aspx?lang=eng#group1>, See also Global Affairs Canada, Export Permits for Cryptography Items, Frequently Asked Questions, Category 5 Part 2- Encryption Items, (last modified 1 May 2014) <http://www.international.gc.ca/controls-controles/export-exportation/crypto/FAQ2011.aspx?lang=eng>.

[249] Global Affairs Canada (2014), Export Permits for Cryptography Items, Frequently Asked Questions, Category 5 Part 2- Encryption Items, (last modified 1 May 2014), <http://www.international.gc.ca/controls-controles/export-exportation/crypto/FAQ2011.aspx?lang=eng>.

[250] *Ibid.*

[251] Symantec (2015), "The FREAK Vulnerability; What You Need to Know," *Symantec* (4 March 2015) <https://www.symantec.com/connect/blogs/freak-vulnerability-what-you-need-know>.

sell their products more broadly. On the other hand, one state's domestic export controls are unlikely to prevent foreign states from developing or adopting strong encryption tools altogether, thus undermining domestic companies that must comply with export controls from effectively competing with their foreign competitors on a global stage.

v. Covert Efforts to Undermine Encryption

Pellentesque - In addition to limitations imposed on encryption by more direct means, intelligence agencies have also engaged in covert efforts to weaken encryption standards and tools of general application, as well as to disseminate those compromised tools internationally. This has been accomplished through various means, including direct agency participation in the standards-setting process for the purpose of injecting weaknesses into the very foundation of certain cryptographic tools. Government agencies, or any other party with knowledge of the weaknesses introduced, can subsequently use that knowledge to exploit those systems more easily.

An example that highlights the nature and implications of this method of compromise arises from a case study involving the Canadian CSE, which was complicit in efforts led by its United States' counterpart, the NSA, to develop and disseminate at least one deliberately flawed cryptographic standard. Documents provided by former NSA contractor Edward Snowden to journalists revealed that the NSA and CSE successfully weakened a random number generator standard called DUAL EC DRBG in 2006.[252] Cryptographically secure computational methods for random number generation are an integral building block of any effective encryption scheme. A flawed number generator—particularly one with a *known* flaw—can render encryption techniques that rely on it vulnerable to attack by making it easier for third parties to determine the private key and subsequently decrypt the message. Other methods of weakening encryption may involve inserting vulnerabilities into the hardware systems upon which cryptographic systems are run, or actively promoting standards which are otherwise known to be vulnerable to cryptanalytic attacks.

The DUAL EC DRBG example is indicative of the wide-ranging damage that can occur when intelligence agencies covertly weaken security protocols. DUAL EC DRBG was not only undermined by intelligence agencies, but immense effort was undertaken to legitimize and propagate the weakened number generator, including by the same governments whose intelligence agencies had weakened it. DUAL EC DRBG was approved by the United States' National Institute for Science and Technology (NIST) as a recommended random number generator as a result of NSA influence.[253] The CSE also ran the international committee at the International Organization for Standardization (ISO) that was responsible for evaluating DUAL EC DRBG.[254] Some "behind-the-scenes" activity from the head of the Canadian delegation and the CSE laid the groundwork for the NSA to rewrite the draft standard; the agency eventually became "the sole editor."[255] The CSE similarly leveraged its role as steward of the Canadian government's defensive capabilities to ensure that the flawed standard was included in a list of approved algorithms for Canadian and U.S. government procurement.[256]

As a result, DUAL EC DRBG was incorporated into a range of products, including those from the prominent security company RSA (which was later reported to have received $10 million from the NSA in exchange for adopting the standard);[257] into operating systems such as Microsoft Windows Vista,[258] and in a version of OpenSSL.[259] Researchers had noted issues with the algorithm for several years, and had begun publicly raising alarm about the possibility that it had been intentionally subverted in

---

[252] Nicole Perlroth, Jeff Larson, and Scott Shane (2013), "N.S.A. Able to Foil Basic Safeguards of Privacy on Web" (5 September 2013) *New York Times*, <http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html>.

[253] *Ibid.*

[254] *Ibid.*

[255] *Ibid.*

[256] Omar El Akaad (2014), "The strange connection between the NSA and an Ontario tech firm", *Globe and Mail* (20 January 2014) <http://www.theglobeandmail.com/technology/business-technology/the-strange-connection-between-the-nsa-and-an-ontario-tech-firm/article16402341/>.

[257] Joseph Menn (2013), "Exclusive: Secret contract tied NSA and security industry pioneer", *Reuters* (20 December 2013) <https://www.reuters.com/article/us-usa-security-rsa-idUSBRE9BJ1C220131220>.

[258] Bruce Schneier (2007), "Dual_EC_DRBG Added to Windows Vista", *Schneier on Security* (17 December 2007) <https://www.schneier.com/blog/archives/2007/12/dual_ec_drbg_ad.html>.

[259] Steve Marquess (2013), "Flaw in Dual EC DRBG (no, not that one)", Email, OpenSSL Foundation (19 December 2013) <https://marc.info/?l=openssl-announce&m=138747119822324>.

2007.[260] Nonetheless, the standard persisted for years despite serious and known flaws—its International Organization for Standardization (ISO) status not revoked, and agencies such as CSE maintained the standard as part of their cybersecurity recommendations. In short, intelligence agencies knowingly propagated and legitimized an encryption tool they knew put users at risk. When the interference was publicly confirmed in 2013, many computer scientists commented that the revelation was likely to erode trust in both standards bodies and the U.S.[261] security industry as a whole.

The DUAL EC DRBG story is just one example of the ways in which signals intelligence agencies have been exposed as engaging in clandestine attempts to undermine and weaken encryption tools upon which the public relies.[262] In 2013, documents from former NSA contractor Edward Snowden revealed a profoundly secretive program named BULLRUN—an NSA program described as an "aggressive, multi-pronged effort to break widely used Internet encryption technologies"—as well as the U.K. GCHQ's BULLRUN-inspired counterpart, EDGEHILL.[263] While information about these programs was shared with select members of counterpart agencies in foreign states,[264] the information was so highly sequestered that departments within the agency's *own* government remained unaware of the resulting deficiencies, and were perhaps even encouraged to use the compromised encryption technology by their own intelligence agencies.[265]

In 2017, the Canadian federal government tabled Bill C-59, introducing comprehensive reforms to the CSE's legal framework. This included a proposal to expand the Establishment's mandate in ways which could have significant implications for the security of global encryption tools. In particular, Bill C-59 included a new "active cyber operations" mandate for the CSE, allowing it to "carry out activities on or through the global information infrastructure 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."[266] While these cyber operations activities cannot be "directed" at Canadians, persons in Canada, or any portion of the global information infrastructure in Canada, this limitation would do little to prevent covert efforts to undermine encryption standards and tools which are inherently global, and rarely reside in any single physical jurisdiction.[267] In other words, no meaningful legislative bar exists, nor are any proposed, that would prevent the CSE from engaging in covert activities to subvert encryption systems, algorithms, tools and standards necessary to preserve the security and integrity of global

---

[260] Matthew Green (2015), "Hopefully the last post I'll ever write on Dual EC DRBG", (14 January 2015) <https://blog.cryptographyengineering.com/2015/01/14/hopefully-last-post-ill-ever-write-on/>.

[261] See e.g., Matthew Green (2013), "On the NSA", *A Few Thoughts on Cryptographic Engineering* (6 September 2013) <https://blog.cryptographyengineering.com/2013/09/06/on-nsa/>.

[262] For earlier examples of intelligence agencies working to encourage the standardization of weak encryption, see Arild Faeraas (2014), "Sources: We Were Pressured to Weaken the Mobile Security in the 80's", *Aftenposten* (9 January 2014) <https://www.aftenposten.no/verden/i/Olkl/Sources-We-were-pressured-to-weaken-the-mobile-security-in-the-80s>.

Similarly, the A5/1 algorithm allowed for 64 bit key lengths, but the last 10 bits were secretly and arbitrarily set to '0' in all keys, reducing the effective key length to 54 bits. See Marc Briceno, Ian Goldberg & David Wagner (1998), "A Pedagogical Implementation of A5/1", *Smartcard Developer Association* <http://www.scard.org/gsm/a51.html>; James Bamford (1982), *The Puzzle Palace: Inside the National Security Agency, America's Most Secret Intelligence Organization*, (Penguin, 1982) <https://cryptome.org/nsa-v-all.htm>; Arthur Sorkin (1984), "Lucifer, A Cryptographic Algorithm", 8(1) *Cryptologia* 22 <https://dx.doi.org/10.1080/0161-118491858746>.

[263] Jeff Larson, Nicole Perlroth and Scott Shane (2013), "Revealed: The NSA's Secret Campaign to Crack, Undermine Internet Security", *ProPublica* (5 September 2013) <https://www.propublica.org/article/the-nsas-secret-campaign-to-crack-undermine-internet-encryption>.

[264] James Ball, Julian Borger and Glenn Greenwald (2013), "Revealed: how US and UK spy agencies defeat internet privacy and security", *The Guardian* (6 September 2013) <https://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security>.

[265] Jeff Larson, Nicole Perlroth and Scott Shane (2013), "Revealed: The NSA's Secret Campaign to Crack, Undermine Internet Security", *ProPublica* (5 September 2013) <https://www.propublica.org/article/the-nsas-secret-campaign-to-crack-undermine-internet-encryption>:

> "The full extent of the N.S.A.'s decoding capabilities is known only to a limited group of top analysts from the so-called Five Eyes: the N.S.A. and its counterparts in Britain, Canada, Australia and New Zealand. Only they are cleared for the Bullrun program … Unlike some classified information that can be parcelled out on a strict "need to know" basis, one document makes clear that with Bullrun, "there will be NO 'need to know.' "Only a small cadre of trusted contractors were allowed to join Bullrun."

[266] Proposed s. 20, *Communications Security Establishment Act* in Bill C-59 (*An Act respecting national security matters*), First Reading June 20, 2017, First Session, Forty-second Parliament. A parallel 'defensive cyber operations' power could be leveraged to similar ends for the purpose of protecting federal government networks or information or private sector infrastructure designated as important (Proposed s 19).

[267] Proposed s. 23, *Communications Security Establishment Act* in Bill C-59 (*An Act respecting national security matters*), First Reading June 20, 2017, First Session, Forty-second Parliament. See: Christopher Parsons, Lex Gill, Tamir Israel, Bill Robinson, and Ronald Deibert (2017), "Analysis of the Communications Security Establishment Act and Related Provisions in Bill C-59 (An Act respecting national security matters), First Reading", The Citizen Lab and the Canadian Internet Policy and Public Interest Clinic (18 December 2017) <https://citizenlab.ca/wp-content/uploads/2018/01/C-59-Analysis-1.0.pdf>.

communications. While such efforts have potentially been historically justified as being in support of the agency's foreign intelligence mandate, the broader scope proposed in Bill C-59 may have an exacerbating effect.[268]

Attempts to undermine encryption are problematic in light of their wide-ranging and systemic impact. Covert attempts to subvert standards bodies can also greatly undermine trust and lead to a disproportionate chilling effect. Individuals may find it increasingly difficult to rely on the integrity of communications systems upon repeated revelations that the underlying protocols that keep these systems secure might be compromised.

B. MEASURES GENERALLY TARGETING INTERMEDIARIES

The most frequent targets of legislative intervention in the encryption debate have undoubtedly been service providers, manufacturers, and other intermediaries involved in the development, distribution, and sale of consumer technology. These intermediaries include commercial actors responsible for securing data at rest (e.g., laptop and mobile device manufacturers) as well as those responsible for encrypting data in transit (e.g., telecommunications service providers, as well as companies providing "over the top" services like instant messaging tools).

In this section, we review a variety of legal, political, and economic measures which are used to target these intermediaries. Though there are points of considerable overlap with the previous section—which explored rules of more general application which are designed to limit the public's access to strong encryption technology writ large—the policy responses described here tend to be slightly more targeted. For example, they may apply specifically to a particular type of intermediary (e.g., telecommunications service providers), a particular form of encrypted data (e.g., data stored and encrypted at rest on a device), or a particular investigative objective (e.g., the ability to decrypt messages in transit). However, in many cases they will be just as likely to have far reaching implications for public safety and security, the economy, and human rights.

First, we discuss the debate surrounding what has come to be known as "exceptional access." This terms includes a spectrum of proposals, all united by the view that intermediaries should be legally required to design their technology in such a way that the government will always have the ability to access a plaintext version of encrypted data. Next, we discuss voluntary efforts undertaken by various private companies or intermediaries that, in effect, broaden the state's ability to access otherwise encrypted data. We then discuss the issue of mandatory decryption capabilities for telecommunications service providers, largely through an examination of the current Canadian context and various failed attempts to expand these obligations through both regulatory and legislative means. Finally, we discuss other forms of mandatory orders that can be used to legally compel intermediaries and other third parties to participate in government efforts to overcome encryption, including both production orders and assistance orders under the Canadian *Criminal Code.*

While the policy responses in this section are diverse, the challenges they raise share several common themes. First, technological measures that facilitate specialized government access to the plaintext form of encrypted data will also inherently increase the ease by which criminals, foreign states, and malicious third parties can access that data. Second, they may entail extraordinary technical, financial, and operational resources from the third party, and impose undue financial and operational burdens on targeted service providers (as well as their customers, who will ultimately bear the financial costs and increased security risks). These measures also pose serious practical challenges in terms of implementation. The most extreme policy options in this category—including so-called "exceptional access" schemes—would require almost unfathomable resources to impose, coordinate, and enforce effectively. Encryption policy operates in a complex policy ecosystem internationally, is subject to global market forces, and decisions made in Canada will impact—and be impacted by—the behaviour of foreign governments abroad. The impact of Canadian policy decisions in this sphere are also limited by the government's ability to exercise jurisdiction over international technology firms. Finally, measures constraining the abilities of intermediaries to secure their data and that of their users will almost always raise serious issues of necessity and proportionality.[269] Though these types of measures may appear to be limited to a specific case or a targeted investigation, in practice there may be significant collateral impacts on the rights of non-targeted individuals and ordinary consumers. No government has made a transparent and evidence-based case that the

[268] See Christopher Parsons, Lex Gill, Tamir Israel, Bill Robinson, and Ronald Deibert (2017), "Analysis of the *Communications Security Establishment Act* and Related Provisions in Bill C-59 (An Act respecting national security matters), First Reading", The Citizen Lab and the Canadian Internet Policy and Public Interest Clinic (18 December 2017) <https://citizenlab.ca/wp-content/uploads/2018/01/C-59-Analysis-1.0.pdf>.

[269] See Necessary and Proportionate Coalition (2014), "International Principles on the Application of Human Rights to Communications Surveillance," launched at the United Nations Human Rights Council in Geneva in September 2013, Final Version (May 2014) <https://necessaryandproportionate.org/principles>.

benefits of systematically weakening encryption technology outweigh these costs. In many cases, the governments' desired outcomes may be entirely achievable without any involvement of the intermediary.[270]

i. Exceptional Access: A Backdoor By Any Other Name?

Many governments, and particularly governments that espouse support for strong human rights records and robust democratic institutions, will at times replace calls for outright bans on secure encryption with a stated aspiration that service providers develop "exceptional access" for state agencies that simultaneously guarantee the security of encryption systems with respect to any others. There are many problems with the concept of "exceptional access" encryption systems, even where such systems operate as intended. These challenges relate to cost, complexity, and the realities of globalization. With regard to this last point, exceptional access obligations imposed onto global communications platforms will inevitably also assist states which seek to use any such exceptional access powers to carry out human rights abuses. However, the most significant challenge posed by exceptional access proposals is that there is simply no technical way to create an encryption system that is secure against everyone except authorized state agencies. Once a backdoor is created, there is no practical guarantee that only state agencies will walk through it. This fundamental flaw makes exceptional access systems an inherent threat to persons who rely on encrypted communications products.

Many governments began to accept the need for robust commercial encryption as the Internet began to play an increasingly important role in modern life and commerce. However, this acceptance was accompanied by proposals for new technical systems which were secure against all unauthorized actors save for law enforcement and intelligence agencies. Various means of achieving this objective have been proposed over the years. None of the proposals to date have been successful in accomplishing both these goals simultaneously.

The most prominent attempt to create an exceptional access regime involved a key escrow system called the "Clipper Chip," which the U.S. government sought to introduce by various means in the early 1990s. The proposal involved channelling commercial encryption through a microchip that employed an initially classified, NSA-controlled cryptographic algorithm called SKIPJACK. The microchip used a backdoor system called "Law Enforcement Access Field" (LEAF) which was intended to grant state agencies (but not others) access to any communications encrypted using the chip.[271] The Clipper Chip was ultimately rejected as a means of providing secure communications subject to exceptional state access following substantial resistance from civil society and the technical community. Before the Clipper Chip was rejected on policy grounds, however, a researcher demonstrated a way to interfere with the LEAF Field, which let anyone potentially tamper with the backdoor.[272] In effect, the Clipper Chip would have made communications less secure for law-abiding citizens on the basis that criminals would have been provided with an easy means of communicating without state scrutiny.

The failure of the Clipper Chip dampened calls for exceptional access systems for a period of time. However, calls for exceptional access began to recur with the resurgence of the "going dark" narrative. Those calling for such a system include U.S. Senators[273] prominent prosecutors from around the world,[274] and the Federal Bureau of Investigation[275] as well as prominent

---

[270] In **Part 5** of this report, we provided a detailed examination of alternative policy measures and investigative techniques available to governments which do not require systematically weakening consumer technology in this manner.

[271] Danielle Kehl, Andi Wilson, and Kevin Bankston (2015), "Doomed to Repeat History? Lessons from the Crypto Wars of the 1990s", New America Open Technology Institute <https://static.newamerica.org/attachments/3407-doomed-to-repeat-history-lessons-from-the-crypto-wars-of-the-1990s/Crypto%20Wars_ReDo.7cb491837ac541709797bdf868d37f52.pdf> at 5.

[272] Matt Blaze (1994), "Protocol Failure in the Escrowed Encryption Standard", (20 August, 1994) <http://www.crypto.com/papers/eesproto.pdf>.

[273] See e.g., Sen. Dianne Feinstein and Sen. Richard Burr, "A bill To require the provision of data in an intelligible format to a government pursuant to a court order, and for other purposes," 114th Congress 2nd Session <https://www.burr.senate.gov/imo/media/doc/BAG16460.pdf>; Dustin Volz, Mark Hosenball, and Joseph Menn (2016), "Push for encryption law falters despite Apple case spotlight," *Reuters* (27 May 2016) <https://www.reuters.com/article/usa-encryption-legislation/push-for-encryption-law-falters-despite-apple-case-spotlight-idUSL2N18O0BM>.

[274] Cyrus R. Vance Jr. et. al. (2015), "When Phone Encryption Blocks Justice", *The New York Times (Opinion)* (11 August 2015) <https://www.nytimes.com/2015/08/12/opinion/apple-google-when-phone-encryption-blocks-justice.html>.

[275] See e.g., Michael Kan (2017), "FBI director floats international framework on encrypted data access," *Computer World* (23 March 2017) <https://www.computerworld.com/article/3184478/security/fbi-director-floats-international-framework-on-encrypted-data-access.html>; Eric Tucker (2016), "Comey: FBI wants 'adult conversation' on device encryption", *Associated Press* (31 August 2016) <https://apnews.com/7d57f576e3f74b6ca4cd3436fbebf160>; Spencer Ackerman (2015), "FBI chief wants 'backdoor access' to encrypted communications to fight Isis", *The Guardian* (8 July 2015) <https://www.theguardian.com/technology/2015/jul/08/fbi-chief-backdoor-access-encryption-isis>.

British[276] and Australian[277] political leaders. These calls have tended to lack detail and, instead, simply declare that service providers or security researchers must find some way to create exceptional access systems that are truly secure. When pressed for examples of potentially successful systems of this type, the response inevitably introduces a host of insurmountable technical and policy challenges. The majority of exceptional access proposals involve some variation of a key escrow or key retention mechanism similar in principle to that which animated the Clipper Chip system.[278] Key escrow systems involve cryptographic systems where the decryption key is held by the government, some other third party, or split between several parties, often with limits on the ability of individual parties to recover the key independently.[279] In a key retention system (a closely related model) the communications or storage provider itself retains either a copy of all individual keys created by its customers, or an institutional level decryption key that can decrypt any of its customers' communications, files, or devices.

Some officials have pointed to various existing technical models as a proof of concept that secure exceptional access systems are possible. For example, FBI Director Christopher Wray has repeatedly pointed to an interactive communications platform called Symphony. Symphony provides collaborative communications solutions similar to Slack or Semaphor but is designed for financial institutions.[280] Financial institutions are heavily regulated and required to keep copies of certain internal communications and to make these available to regulators on demand.[281] Such institutions are effectively precluded from using ephemeral messaging systems with forward secrecy as these do not provide some mechanism for long-term and auditable storage of messages. Symphony, the messaging platform in question, provides customized solutions to meet this regulatory environment.[282] As an enterprise system, Symphony allows individual clients to control their decryption keys at the institutional level.[283] In response to pressure from state and federal law makers and regulators, four banks in New York State agreed to provide independent entities of their choosing with a copy of their internal Symphony decryption key (often, this independent third party will be the bank's lawyer).[284] This system has since been pointed to by Wray, Deputy Attorney General Rod Rosenstein, and others

[276] See e.g., Natasha Lomas, "We want to limit use of e2e encryption, confirms UK minister", *TechCrunch* (5 June 2017) <https://techcrunch.com/2017/06/05/we-want-to-limit-use-of-e2e-encryption-confirms-uk-minister/>; Matt Burgess (2015), "Surveillance bill will only ban 'strong' encryption", *Wired* (3 November 2015) <https://www.wired.co.uk/article/surveillance-bill-ban-strong-encryption-apple-imessage>.

[277] Though the Australian government has made statements to the effect that they do not intend to "require" a backdoor, this is difficult to reconcile with the government's other positions on encryption.

See e.g., Nick Evershed (2017), "Australia's plan to force tech giants to give up encrypted messages may not add up," *The Guardian* (14 July 2017) <https://www.theguardian.com/technology/2017/jul/14/forcing-facebook-google-to-give-police-access-to-encrypted-messages-doesnt-add-up>; Robert Merkel (2017), "When is 'not a backdoor' just a backdoor? Australia's struggle with encryption", *The Conversation* (14 June 2017) <https://theconversation.com/when-is-not-a-backdoor-just-a-backdoor-australias-struggle-with-encryption-79421>.

[278] Ellen Nakashima and Barton Gellman (2015), "As Encryption Spreads, US Grapples with Clash Between Privacy, Security", *Washington Post* (10 April 2015) <https://www.washingtonpost.com/world/national-security/as-encryption-spreads-us-worries-about-access-to-data-for-investigations/2015/04/10/7c1c7518-d401-11e4-a62f-ee745911a4ff_story.html>:

> "The split-key approach floated by Rogers is a variant on that old approach and is intended to resolve some of the policy objections. Storing a master key in pieces would reduce the risk from hackers. A court could oversee the access."

[279] Abelson et. al. (19970, "The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption," (May 1997) <https://www.schneier.com/academic/paperfiles/paper-key-escrow.pdf>.

[280] Ellen Nakashima (2018), "FBI chief calls encryption a 'major public safety issue'", *The Washington Post* (9 January 2018); Chris Bing (2018), "The FBI Director thinks this company found an answer to 'going dark'", *CyberScoop* (8 March 2018) <https://www.cyberscoop.com/christopher-wray-encryption-symphony-key-escrow/>.

[281] 17A-4 LLC, (2018), "Securities and Exchange Commission, FINRA, Commodity Futures Trading Commission & Dodd-Frank Act: Rule & Regulation Summary", 17A-4 LLC (last accessed 4 May 2018), < https://www.17a-4.com/regulations-summary/>.

[282] Richard Stiennon (2016), "Critical Components of a Secure Communications and Collaboration Solution", *Symphony Communications* (2016) <https://go.symphony.com/hubfs/white-papers/it-harvest-critical-components.pdf?submissionGuid=f95f0221-8d46-46b3-9c0a-70861c57087e>.

[283] *Ibid*; Chris Bing (2018), "The FBI Director thinks this company found an answer to 'going dark'", *CyberScoop* (8 March 2018) <https://www.cyberscoop.com/christopher-wray-encryption-symphony-key-escrow/>; Symphony, "Symphony Enterprise Edition: Regulatory Compliance Features", *Symphony Communications* <https://symphony.com/blog/item/symphony-enterprise-edition-regulatory-compliance-features>:

> "Many "end-to-end" encrypted messaging tools targeted at the consumer market do not provide organizational-level key control and therefore cannot support the regulatory retention needs of financial institutions. One important distinction of Symphony's "end-to-end" security is that firms deploying our messaging technology retain the ability to archive their employees' communications by controlling their keys at an organizational level."

[284] Penny Crosman, (2015), "Regulator's New Aim: Keeping a Back Door into the Bank", *American Banker* (22 July 2015) <https://www.americanbanker.com/news/regulators-new-aim-keeping-a-back-door-into-the-bank> and Arik Hesseldahl, (2015), "Messaging Service Symphony Dodges Regulatory Action Ahead of Launch", *Recode* (14 September 2015) <https://www.recode.net/2015/9/14/11618550/messaging-service-symphony-dodges-regulatory-action-ahead-of-launch>.

as an example of the broader vision for assuring law enforcement access to encrypted communications.[285] However, while this system (which is essentially a key escrow model) might solve a legal challenge facing financial institutions, it does nothing to address the technical, constitutional, and security problems that lie at the heart of exceptional access proposals in general.

The legal obligations to which Symphony responds would be constitutionally impermissible if imposed on individuals at large. As regulated entities, banks operate under strict obligations to retain auditable copies of certain communications. Such strict regulatory obligations could only be constitutionally permissible in the highly regulated environment that such entities operate under, one where courts have recognized reduced expectations of privacy and, as a result, diminished constitutional protections for communications.[286] Most relevant, perhaps, institutional entities such as financial companies are limited in their ability to assert the right to silence when compelled to provide an encryption key or password for regulatory compliance purposes. Individuals operate under a markedly different legal landscape insofar as they are under *no* obligation to record their private phone calls, emails, instant messages, or other digital interactions. The constitutionality of imposing any such generalized obligation with respect to the content of individual communications would be highly questionable.[287] Similarly, where individuals are compelled to participate in an investigation of their own alleged criminal conduct by providing passwords or encryption keys to their communications, accounts or devices, the constitutional right against self-incrimination is engaged. Finally, imposing these types of key escrow obligations onto an institutional client does not raise any of the chilling effects inherent in more generalized communications systems that are demonstrably insecure. Symphony is a platform for regulated, not personal, communications, meaning employees may already be inherently cautious in deciding what they choose to say on Symphony. From a technical perspective, Symphony also fails to achieve the scale necessary real-time or on-demand decryption of data belonging to a large user base.[288] As a general model for exceptional access to the full ecosystem of encrypted communications data, Symphony presents an inappropriate analogy.[289] Those advocating for secure encryption have never argued that these types of escrow or backdoor systems are impossible, only that such systems unacceptably undermine security and, by extension, human rights and trust in communications networks.[290] In this respect, Symphony presents all of the other negative implications that are indicative of exceptional access schemes in general.

Exceptional access systems introduce outsized technical vulnerabilities by design. The rhetoric surrounding such proposals consistently pitches exceptional access solutions as a moderate middle ground, allowing citizens and businesses to secure their data while ensuring that the government can always decrypt information for investigative purposes. However, the idea that creating a system of specialized or exceptional access for law enforcement is possible without creating collateral risk to the security, civil liberties, or economic interests of end users defies an overwhelming body of technical evidence and common sense to the contrary. As the computer security expert Bruce Schneier has explained, it is fundamentally impossible for

---

[285] Chris Bing (2018), "The FBI Director thinks this company found an answer to 'going dark'", *CyberScoop* (8 March 2018) <https://www.cyberscoop.com/christopher-wray-encryption-symphony-key-escrow/>:

> "In most cases today, the custodian tends to be a general law firm that already represents the Symphony client who is granted special access to the key box."

[286] Note these expectations or privacy are reduced, but not non-existent. See *Los Angeles v Patel*, (2015) 576 US __ (Supreme Court of the United States): As implied in Patel, the privacy interests of the regulated entity subjected to an administrative search are separate and distinct from those of affected customers. It should further be noted that whereas some forms of metadata have been characterized as 'business records' in the United States, this characterization has been questioned challenged by many (see for example *US v Jones*, (2012) 565 US 400 (Supreme Court of the United States), per Sotomayer, J, concurring; *US v Carpenter*, Docket No 16-402 (Supreme Court of the United States, decision pending) and, moreover, has never been extended to the content of communications.

Finally, it should be noted that under Canadian law, courts have firmly and consistently rejected the notion that individuals lose the substantially high privacy interests associated with their communications simply because a third party service provider is associated with their transmission (see: *R v Duarte*, [1990] 1 SCR 30; *R v TELUS Communications Co*, 2013 SCC 16; *R v Marakah*, 2017 SCC 59; *R v Jones*, 2017 SCC 60); see specifically: *R v Cole*, 2012 SCC 53 (employees' personal interactions on work computers retain privacy interest vis à vis the state despite employer control of and access to computer).

[287] Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland v Ireland*, (8 April 2014)(Court of Justice of the European Union, Grand Chamber); Joined Cases C-203/15 and C-698/15, *Watson v Secretary of State for the Home Department (United Kingdom)*, (21 December 2016)(Court of Justice of the European Union, Grand Chamber). See also: *Cash Converters Canada Inc v Oshawa (City)*, 2007 ONCA 502.

[288] Specifically, the Symphony decryption key is held by a trusted third party and made available to regulators in isolated instances such as when an audit occurs. By contrast, law enforcement and other state agencies seek 'on demand' access to large volumes of individual accounts on a daily basis. See: Charlie Savage (2018), "Justice Dept. Revives Push to Mandate a Way to Unlock Phones", *The New York Times* (24 March 2018) <https://www.nytimes.com/2018/03/24/us/politics/unlock-phones-encryption.html>; Susan Landau (2017), "Punching the Wrong Bag: The Deputy AG Enters the Crypto Wars", *Lawfare* (27 October 2017) <https://www.lawfareblog.com/punching-wrong-bag-deputy-ag-enters-crypto-wars>.

[289] As Symphony notes, its systems were not modified in any way to address the concerns of New York State regulators.

See David Gurle, "Bank-DFS Agreement", *Symphony Communications* <https://symphony.com/blog/item/bank-dfs-agreement>.

[290] Ellen Nakashima (2018), "FBI chief calls encryption a 'major public safety issue'", *The Washington Post* (9 January 2018); Chris Bing (2018), "The FBI Director thinks this company found an answer to 'going dark'", *CyberScoop* (8 March 2018) <https://www.cyberscoop.com/christopher-wray-encryption-symphony-key-escrow/>.

technologists to build a system "that only works for people of a certain citizenship, or with a particular morality, or only in the presence of a specified legal document."[291] Backdoor systems built to catch criminals are equally available to criminals themselves.[292] It is precisely on this basis that the European Parliament has proposed regulations which would require end-to-end encryption in some cases and forbid the imposition of mandatory government backdoors.[293] Even many policing and investigative agencies have acknowledged that solutions to their "going dark" challenges should not come at the cost of undermining the security of encryption standards, as doing so leaves individuals more vulnerable to cyber criminals.[294]

Technical problems with exceptional access systems have been extensively documented elsewhere over the last three decades and this report does not aspire to undertake an exhaustive survey of all proposed implementations or their corresponding technical critiques. There is, in fact, an unwavering consensus within the technical community that any exceptional access system will undermine encryption security by dramatically increasing complexity and related opportunities for exploitation.[295] We simply reiterate this consensus and outline its underlying tenets. While some members of the technical community have sought to identify exceptional access systems that are "as secure as possible" in early 2018,[296] nothing has disturbed the long-standing consensus that backdoors and similar proposals fundamentally weaken the security of communications products and endanger users. This position is virtually as unanimous among computer scientists as the existence of climate change is among environmental scientists.[297] In reality, computer scientists, software engineers, and cryptographers already face significant difficulties in providing a baseline degree of security for communication and storage systems in a constantly evolving digital landscape. The deliberate introduction of vulnerabilities to facilitate government access would further add system complexities and introduces additional new vectors for third party exploitation, weakening the security provided to individuals, businesses, and governments alike. Essentially, system complexity increases the likelihood of implementation errors and chance of security vulnerabilities,[298] whereas exceptional access systems add significant complexity *specifically intended to facilitate access* and consequently establishing an additional entry point to secure.[299] Exceptional access systems, in other words, are inherently less secure, more difficult to use and maintain, and expose users to more serious risks. In

---

[291] Bruce Schneier (2016), "Business Report How an Overreaction to Terrorism Can Hurt Cybersecurity", *MIT Technology Review* (25 January 2016) <https://www.technologyreview.com/s/545716/how-an-overreaction-to-terrorism-can-hurt-cybersecurity/>.

[292] In a related example, a system built into Vodaphone's Greek mobile network in order to facilitate lawfully authorized wiretapping was exploited by unknown adversaries and subsequently used to intercept the phone calls of Greece's Prime Minister, Athens' Mayor, and several other high-ranking officials.

See Vassilis Prevelakis and Diomidis Spinellis (2007) "The Athens Affair", *IEEE Spectrum* (29 June 2007) <https://spectrum.ieee.org/telecom/security/the-athens-affair>.

[293] See Parliament of Europe, Draft Report on the proposal for a regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) 2017/0003(COD) <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2f%2fEP%2f%2fNONSGML%2bCOMPARL%2bPE-606.011%2b01%2bDOC%2bPDF%2bV0%2f%2fEN> at 74 (Amendment 116 Proposal for a regulation Article 17 – paragraph 1 a (new)):

> "The providers of electronic communications services shall ensure that there is sufficient protection in place against unauthorised access or alterations to the electronic communications data, and that the confidentiality and safety of the transmission are also guaranteed by the nature of the means of transmission used or by state-of-the-art end-to-end encryption of the electronic communications data. Furthermore, when encryption of electronic communications data is used, decryption, reverse engineering or monitoring of such communications shall be prohibited. Member States shall not impose any obligations on electronic communications service providers that would result in the weakening of the security and encryption of their networks and services."

[294] Examples of various law enforcement positions in support of maintaining robust encryption can be found in Part 2 of this report in the subsection entitled "Encryption is Integral to Public Safety, Security, and Other Interests."

[295] Susan Landau, "Building on Sand Isn't Stable: Correcting a Misunderstanding of the National Academies Report on Encryption", *Lawfare* (25 April 2018) <https://lawfareblog.com/building-sand-isnt-stable-correcting-misunderstanding-national-academies-report-encryption>.

[296] Charlie Savage (2018), "Justice Dept. Revives Push to Mandate a Way to Unlock Phones", *The New York Times* (24 March 2018) <https://www.nytimes.com/2018/03/24/us/politics/unlock-phones-encryption.html>; National Academy of Sciences (2018), "Decrypting the Encryption Debate: A Framework for Decision Makers", Committee on Law Enforcement and Intelligence Access to Plaintext Information Computer Science and Telecommunications Board, *The National Academies Press* (Prepublication, 2018) <https://www.nap.edu/catalog/25010/decrypting-the-encryption-debate-a-framework-for-decision-makers>.

[297] See Cory Doctorow (2016), "The FBI wants a backdoor only it can use – but wanting it doesn't make it possible," (24 February 2016) *The Guardian* <https://www.theguardian.com/technology/2016/feb/24/the-fbi-wants-a-backdoor-only-it-can-use-but-wanting-it-doesnt-make-it-possible>:

> "The thing about this controversy is that it isn't one. Independent cryptographers are virtually unanimous in their view that you can't properly secure a system while simultaneously ensuring that it ships with a pre-broken mode that police can exploit."

[298] Ronald L. Rivest (2008), "On the notion of 'software independence' in voting systems," Phil Tran R Soc A (2008) 366, 3759–3767 <http://rsta.royalsocietypublishing.org/content/roypta/366/1881/3759.full.pdf>.

[299] Meredith Whittaker and Ben Laurie (Association for Computing Machinery) (2016), "Wanting It Bad Enough Won't Make It Work: Why Adding Backdoors and Weakening Encryption Threatens the Internet", *Huffington Post* (9 December 2016) <http://www.huffingtonpost.com/acm-the-association-for-computing-machinery/wanting-it-bad-enough-won_b_8762322.html>.

many cases, these systems also create a centralized point of failure and create particularly attractive and high-value targets for malicious third parties.[300]

Some technical experts have argued that service providers already need to have the capacity to securely store certain types of keys as most service providers rely on authentication keys to ensure that their respective products are securely updated or to lock specific device functionality.[301] They have argued that such companies could secure keys retained or held in escrow to comply with a legislated exceptional access system.[302] However, even large and sophisticated companies have found it difficult to adequately secure institutional-level keys.[303] For example, in 2016, Microsoft inadvertently leaked a "golden key" which it had created for its Secure Boot mechanism. Secure Boot is a firmware component that validates elements of the operating system as they are initially loaded to ensure these are created by a trusted manufacturer.[304] With Microsoft's institutional key, any party with access to a mobile device could effectively bypass Secure Boot and load malicious software onto that device.[305] In the Symphony example outlined above, this risk of exposure is exacerbated, as the "golden key" is held not only by the primary company (the financial institution) but also by a second trusted party, doubling the risk of exposure.[306] Exceptional access systems are also generally inherently incompatible with the concepts of forward secrecy and end-to-end encryption, both of which have proven to be central features of contemporary secure systems in ways that are specifically obviated by exceptional access requirements. Finally, it is also important to recognize that "global" decryption keys are different from other keys in several important respects. First, the very presence of such decryption keys creates a valuable target for cybercriminals, hostile intelligence agencies, and opportunistic intruders alike.[307] For example, the Snowden leaks indicated a sophisticated and multi-lateral attempt launched by the NSA to compromise cryptographic keys associated with billions of mobile device SIM cards by attacking the network of their manufacturer, Gemalto.[308] Further, as noted computer scientist Susan Landau explains, access to decryption keys is certain to be in high demand. They are likely to be used many times per day, and will need to be accessible to multiple individuals within the

---

[300] Harold Abelson et. al. (2015), "Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications" (2015) <https://www.schneier.com/academic/paperfiles/paper-keys-under-doormats-CSAIL.pdf> at 2; David Kaye (2015), Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/29/32, 29th session of the Human Rights Council <http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/Pages/ListReports.aspx> at 15.

[301] National Academy of Sciences (2018), "Decrypting the Encryption Debate: A Framework for Decision Makers", Committee on Law Enforcement and Intelligence Access to Plaintext Information Computer Science and Telecommunications Board, *The National Academies Press* (Prepublication, 2018) <https://www.nap.edu/catalog/25010/decrypting-the-encryption-debate-a-framework-for-decision-makers>.

[302] National Academy of Sciences (2018), "Decrypting the Encryption Debate: A Framework for Decision Makers", Committee on Law Enforcement and Intelligence Access to Plaintext Information Computer Science and Telecommunications Board, The National Academies Press (Pre-publication, 2018) <https://www.nap.edu/catalog/25010/decrypting-the-encryption-debate-a-framework-for-decision-makers>; Susan Landau (2017), "Punching the Wrong Bag: The Deputy AG Enters the Crypto Wars", *Lawfare* (27 October 2017) <https://www.lawfareblog.com/punching-wrong-bag-deputy-ag-enters-crypto-wars>; Susan Landau, "Building on Sand Isn't Stable: Correcting a Misunderstanding of the National Academies Report on Encryption", *Lawfare* (25 April 2018) <https://lawfareblog.com/building-sand-isnt-stable-correcting-misunderstanding-national-academies-report-encryption>.

See also: Steven Levy, "Cracking the Crypto War", *Wired* (25 April 2018), <fhttps://www.wired.com/story/crypto-war-clear-encryption/>:

> "The strength of Ozzie's system lies in its simplicity. Unlike Clinton Brooks, who relied on the government to safeguard the Clipper Chip's encrypted keys, Ozzie is putting his trust in corporations …. He argues that the security of the entire mobile universe already relies on the protection of keys—those vital keys used to verify operating system updates, whose compromise could put billions of users at risk."

But see Matthew Green, "A Few Thoughts on Ray Ozzie's 'Clear' Proposal" *Cryptography Engineering* (26 April 2018) <https://blog.cryptographyengineering.com/2018/04/26/a-few-thoughts-on-ray-ozzies-clear-proposal/>:

> "So let's be clear. Ozzie's proposal relies fundamentally on the ability of manufacturers to secure extremely valuable key material for a massive number of devices against the strongest and most resourceful attackers on the planet."

[303] Susan Landau, "Building on Sand Isn't Stable: Correcting a Misunderstanding of the National Academies Report on Encryption", *Lawfare* (25 April 2018) <https://lawfareblog.com/building-sand-isnt-stable-correcting-misunderstanding-national-academies-report-encryption>; Matthew Green, "A Few Thoughts on Ray Ozzie's 'Clear' Proposal" *Cryptography Engineering* (26 April 2018) <https://blog.cryptographyengineering.com/2018/04/26/a-few-thoughts-on-ray-ozzies-clear-proposal/>.

[304] Rafal Sosnowski (Microsoft Dubai Security PFE Team) (2016), "Diving into Secure Boot", (14 March 2016) <https://blogs.technet.microsoft.com/dubaisec/2016/03/14/diving-into-secure-boot/>.

[305] Tom Mendelsohn (2016), "Secure Boot snafu: Microsoft leaks backdoor key, firmware flung wide open", *Ars Technica* (11 August 2016) <https://arstechnica.com/information-technology/2016/08/microsoft-secure-boot-firmware-snafu-leaks-golden-key/>.

[306] Chris Bing (2018), "The FBI Director thinks this company found an answer to 'going dark'", *CyberScoop* (8 March 2018) <https://www.cyberscoop.com/christopher-wray-encryption-symphony-key-escrow/>.

[307] Matthew Green, "A Few Thoughts on Ray Ozzie's 'Clear' Proposal" *Cryptography Engineering* (26 April 2018) <https://blog.cryptographyengineering.com/2018/04/26/a-few-thoughts-on-ray-ozzies-clear-proposal/>.

[308] Kim Zetter (2015) "Gemalto Confirms It Was Hacked But Insists the NSA Didn't Get Its Crypto Keys", *Wired* (25 February 2015) <https://www.wired.com/2015/02/gemalto-confirms-hacked-insists-nsa-didnt-get-crypto-keys/>.

company, and perhaps within the various agencies or trusted third parties authorized to conduct the decryption process when lawfully compelled.[309] Each of these individuals and parties present an additional point of potential compromise.

Creating exceptional access systems also raise questions of globalization—which nations will have the privilege of lawfully decrypting content, and which will not? Indeed, some experts have argued that "the greatest impediment to exceptional access may be the complexities of legal jurisdiction."[310] Policy measures which would require service providers that operate globally to conform to specific governments' exceptional access requirements are fraught with practical- and principal-based complications. On a practical level, implementing policies of this type can be costly and difficult exercise s which are made exponentially more complicated when service providers must design for interoperability at an international scale. Perhaps more importantly, however, many countries around the world lack the comparatively robust procedural rights, legal, and political accountability mechanisms, and human rights protections by which countries such as Canada must abide. The safety of a key escrow or backdoor system "depends on the integrity of the person, department or system charged with safeguarding the private keys" or otherwise entrusted with access to the system.[311] Yet even in Canada, government agents sometimes abuse their trusted status to conduct surveillance on those who are not suspected of actual wrongdoing, such as journalists, marginalized communities, and human rights advocates.[312] If states such as Canada impose exceptional access, countries with much more problematic human rights records or histories of abuse are likely to follow suit,[313] and it may be difficult in principle to deny such attempts:

> "The UK government promises legislation this fall to compel communications service providers, including US-based corporations, to grant access to UK law enforcement agencies, and other countries would certainly follow suit. China has already intimated that it may require exceptional access. If a British-based developer deploys a messaging application used by citizens of China, must it provide exceptional access to Chinese law enforcement?"[314]

---

[309] Susan Landau (2017), "Punching the Wrong Bag: The Deputy AG Enters the Crypto Wars", *Lawfare* (27 October 2017) <https://www.lawfareblog.com/punching-wrong-bag-deputy-ag-enters-crypto-wars>.

[310] Harold Abelson et. al. (2015), "Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications" (2015) <https://www.schneier.com/academic/paperfiles/paper-keys-under-doormats-CSAIL.pdf> at 3.

[311] David Kaye (2015), Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/29/32 <http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/Pages/ListReports.aspx> at 16.

[312] See e.g.: **Journalists:** Karen Seidman and Paul Cherry (2016), "Montreal police monitored iPhone of La Presse journalist Patrick Lagacé," *The Montreal Gazette* (1 November 2016) <http://montrealgazette.com/news/local-news/montreal-police-monitored-iphone-of-la-presse-journalist-patrick-lagace>; Benjamin Shingler (2016), "After Patrick Lagacé, other Montreal journalists worry they, too, were spied on," *CBC News* (2 November 2016) <http://www.cbc.ca/news/canada/montreal/montreal-police-patrick-lagace-1.3832412>; **Women's rights organizations:** Christabelle Sethna and Steve Hewitt (2009), *Clandestine Operations: The VWC, the Abortion Caravan and the RCMP*, Canadian Historical Review 90, 3 (2009): 463-496; **Campus groups:** Steve Hewitt (2002), Spying 101: The RCMP's Secret Activities at Canadian Universities, 1917-1997, University of Toronto Press; **Anti-racist groups:** Laurent Bastien Corbeil (2015), "RCMP tracked Toronto activists with fake Facebook profile," *The Toronto Star* (July 27 2015)<https://www.thestar.com/news/gta/2015/07/27/rcmp-tracked-toronto-activists-with-fake-facebook-profile.html; **Environmental activists:** Mike Chisholm and Jenny Uechi (2013), "CSIS spying on citizens at alarming rate, FOIs reveal," *Vancouver Observer* (26 February 2013) <http://www.vancouverobserver.com/politics/investigations/canadian-security-intelligence-service-spying-citizens-alarming-rate-fois?page=0,0>; **Indigenous activists:** Jorge Barrera (2016), "Akwesasne under surveillance by military counter-intelligence unit: documents," *APTN* (19 February 2016) <http://aptnnews.ca/2016/02/19/akwesasne-under-surveillance-by-military-counter-intelligence-unit-documents/>; Joe Freisen (2008), "CSIS turning to natives in search of information," *Globe and Mail* (28 November 2008) <https://beta.theglobeandmail.com/news/national/csis-turning-to-natives-in-search-of-information/article1066882/?ref=http://www.theglobeandmail.com>; Canadian Press (2013), "Canada's spy agency kept close watch on rapidly growing First Nations protest movement: documents," *National Post* (11 August 2013) <http://nationalpost.com/news/canada/canadas-spy-agency-kept-close-watch-on-rapidly-growing-first-nations-protest-movement-documents>; Canadian Press (2013), "Canada's spy agency helped prepare all-of-government approach in case Idle No More protests 'escalated': secret files," *National Post* (23 March 2014) <http://nationalpost.com/news/canada/canadas-spy-agency-helped-prepare-all-of-government-approach-in-case-idle-no-more-protests-escalated-secret-files>; Canadian Press (2014), "Canadian Forces spent virtually all of 2013 watching Idle No More protesters," *National Post* (1 June 2014) <http://nationalpost.com/news/canada/canadian-forces-spent-virtually-all-of-2013-watching-idle-no-more-protesters>; Canadian Journalists for Free Expression, "Under the Microscope: Cindy Blackstock," <http://www.cjfe.org/under_the_microscope_cindy_blackstock>; **Other human rights advocates:** *Canadian Civil Liberties Association (Corporation of) v Canada (Attorney General)*, [1998] 40 OR (3d) 489 (CA); **Communists:** Nora T. Lamontagne and Justin Ling (2015), "Inside Canada's Five-Year-Long Anti-Terror Investigation of a Group of Quebec Communists," *Vice* (19 March 2015) <https://www.vice.com/en_ca/article/4w7kvq/inside-canadas-five-year-long-anti-terror-investigation-of-a-group-of-young-communists-235>; **Veterans' advocates:** Richard J. Brennan (2010), "Watchdog slams 'alarming' breach of veteran's privacy," *The Toronto Star* (8 October 2010) <https://www.thestar.com/news/canada/2010/10/08/watchdog_slams_alarming_breach_of_veterans_privacy.html>; **Anarchists:** Sarah R. Champagne (2016), "La haute direction du SPVM a cautionné GAMMA," *Le Devoir* (4 November 2016) <http://www.ledevoir.com/societe/actualites-en-societe/483805/sc-gamma>; **Muslims:** see generally Baljit Nagra (2017), *Securitized Citizens: Canadian Muslims' Experiences of Race Relations and Identity Formation Post-9/11* (University of Toronto Press: 2017); **Other general abuse:** Donalee Moulton (2017), "Newfoundland and Labrador privacy conviction sends noteworthy message", *The Lawyer's Daily* (6 September 2017) <https://www.thelawyersdaily.ca/other/articles/4536>; John Hawes (2013), "Canadian cop claims he didn't know cyber-stalking was illegal," *Naked Security* (28 June 2013) <https://nakedsecurity.sophos.com/2013/06/28/canadian-cop-claims-he-didnt-know-cyber-stalking-was-illegal/>.

[313] See for discussion of the potential "ripple effects" of domestic encryption policy: Ryan Budish, Herbert Burkert, and Urs Gasser (2018), "Encryption Policy and Its International Impacts: A Framework for Understanding Extraterritorial Ripple Effects" Aegis Series Paper No. 1804, Hoover Institution Essay <https://cyber.harvard.edu/node/100169>.

[314] Harold Abelson et. al. (2015), "Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications" (2015) <https://www.schneier.com/academic/paperfiles/paper-keys-under-doormats-CSAIL.pdf> at 3.

Even if a state succeeds in preserving exceptional access to itself, or to filter foreign requests to global service providers through its domestic legal apparatus, foreign state agencies denied direct access could try to exploit the vulnerabilities created by whichever backdoor mechanism was ultimately adopted. Even presuming an encryption backdoor can be justified domestically on the basis that it facilitates lawful access to otherwise encrypted communications, it cannot be justified in terms of the human rights violations such a backdoor is guaranteed to facilitate abroad.

In sum, calls for exceptional access systems appear to present a "solution" premised in politics, not reality. This solution obscures or ignores the technical challenges inherent in any attempt to secure communications systems from unauthorized access. Exceptional access may provide a compelling rhetorical package for state agencies, placing the burden on service providers or the technical community to invent a way of decrypting data for government agents while denying access to all others while ignoring the feasibility of achieving this outcome. Yet they also come at a radically disproportionate cost to security and human rights, at a time where the technical community is already at a significant disadvantage in their attempts to secure a data from a host of unauthorized actors. Rhetoric aside, an exceptional access legal mandate is no different from any of the other bans on secure encryption explored in the previous section. In some respects, exceptional access can be worse, as it creates a known point of failure that any criminal, foreign state (be it an ally or enemy), or opportunistic intruder can exploit.

ii. Voluntary Private Sector Collaboration

Relationship-building with telecommunication service providers, Internet service providers and other technology companies is one component of Western governments' strategy for addressing the encryption issue, and is the second prong of the Canadian federal government's strategic considerations in addressing the "going dark problem."[315] In Canada, the RCMP has stated that it "engages with security managers from the five largest [domestic] TSPs on law enforcement challenges such as those in relation to interception of judicially authorized private communications, but further outreach at a senior level in concert with Five Eyes allies would be beneficial."[316] The Canadian government also passed legislation which may encourage intermediaries to collaborate with law enforcement voluntarily, such as by providing immunity from civil and criminal liability for companies that preserve or disclose data at the request of a law enforcement official even in the absence of a warrant.[317] However, as the Supreme Court established in *R v. Spencer*, where an individual has a reasonable expectation of privacy in information held by third party like a telecommunications provider or information technology company, such a request amounts to a search and generally requires prior judicial authorization.[318]

In some cases voluntary cooperation with the private sector to address challenges posed by encryption has been an effective strategy for law enforcement agencies. The RCMP, for example, point out that "certain TSPs and IT companies, such as BlackBerry, are actively supportive of law enforcement efforts vis-a-vis interception and encryption in relation to their networks and products."[319] In one high profile organized crime investigation culminating in a case called *R v. Mirarchi*, BlackBerry came under public scrutiny when it was reported that the company had facilitated message decryption capabilities for the RCMP. The record of the hearing revealed that BlackBerry had provided the RCMP with a key that had been subsequently used to decrypt "roughly one million PIN-to-PIN BlackBerry messages" in connection with the investigation in question.[320] According to a document created by the CSE and introduced as evidence at trial, the key disclosed by BlackBerry to the RCMP could be used by

---

[315] Royal Canadian Mounted Police (2016), "Encryption and Law Enforcement" 2016 brief (obtained under the *Access to Information Act* by Christopher Parsons in 2017) at 3 <https://cippic.ca/uploads/ATI-RCMP-Encryption_and_Law_Enforcement-2016.pdf>.

[316] *Ibid.*

[317] See s. 188.2, s. 487.0195(2) Criminal Code R.S.C., 1985, c. C-46. Additionally, s 188.2 of the *Criminal Code* grants a similar immunity to anyone assisting law enforcement in carrying out a wiretap. A telecommunications company might thereby be encouraged to assist law enforcement decrypt customer communications in an excessive or intrusive manner if it reasonably believed such assistance fell within the wiretap authorization being implemented.

[318] *R v Spencer*, 2014 SCC 43 at para 66.

[319] Royal Canadian Mounted Police (2016), "Encryption and Law Enforcement" 2016 brief (obtained under the *Access to Information Act* by Christopher Parsons in 2017) at 3 <https://cippic.ca/uploads/ATI-RCMP-Encryption_and_Law_Enforcement-2016.pdf>.

[320] Justin Ling and Jordan Pearson (2016), "Canadian Police Obtained BlackBerry's Global Decryption Key" *Vice/Motherboard* (14 April 2016) <https://news.vice.com/article/exclusive-canada-police-obtained-blackberrys-global-decryption-key-how>; see also documents in Volume 2 of *R v Mirarchi*, QCCA File No 500-10-006048-159, Appellant's Factum, January 22, 2016, obtained by Mark Phillips available at CIPPIC, "Report Calls for Greater Transparency, Proactive Control of IMSI Catchers" <https://cippic.ca/news/report_calls_for_proactive_transparency_and_control_of_imsi_catchers>.

the latter to decrypt messages of all other, non-targeted BlackBerry PIN-to-PIN messaging users and operate as a "global" decryption key.[321] It appears that prior to this hearing, the existence of such a "global key" was not known to the general public.[322]

Voluntary collaboration between the private sector, law enforcement, and intelligence agencies comes with a potential risk of reputational damage to the service provider and may seriously erode consumer trust. This is particularly so where that collaboration is initially conducted in secret and where it has the potential to raises novel legal and ethical issues. Indeed, when BlackBerry cooperated with the RCMP in the *Mirarchi* case, the Crown was "reluctant to disclose any [BlackBerry] involvement, stating that to do so may have a negative commercial impact on the company. Such disclosure … would affect relations between RIM and police investigators. … [the RCMP] also spoke of negative publicity."[323] BlackBerry's testimony during the hearing explicitly acknowledged the threat to its reputation and to consumer trust if its voluntary disclosure of its secret decryption key to Canadian law enforcement was revealed to the public:

> "...I verily believe that the disclosure of the global encryption key … would not only potentially impact relationships with BlackBerry end-users and law enforcement criminal investigations in Quebec as well as the rest of Canada, it would potentially impact relationships with other BlackBerry end-users and law enforcement criminal investigations globally for all foreign countries that BlackBerry operates and provides communication services; and
>
> BlackBerry is known for its high level of security and I verily believe that the disclosure of the global encryption key … could negatively impact BlackBerry's commercial reputation and adversely affect global business resulting in significant economic damage. BlackBerry values security and its reputation for secure communications is critical for the continued success of the company."[324]

Any failure to reveal information concerning the use of BlackBerry's key would almost inevitably undermine the accused's *Charter*-protected right to full disclosure, which should not be trumped by concerns over negative publicity.[325] Indeed, the *Mirarchi* case was ultimately dropped despite the severity of the charges at issue, with the Crown citing challenges in meeting its disclosure obligations as a motivating factor in seeking a stay.[326] It was never made clear whether the RCMP obtained Blackberry's decryption key further to a mandatory court order, by voluntary disclosure from BlackBerry, or by some other means.

When private sector firms collaborate with law enforcement and intelligence agencies behind closed doors it not only threatens consumer trust, but also raises questions about the extent to which such companies may be misrepresenting the overall security of their products—are all products offering the security benefits communicated to customers? Are only certain versions of products capable of securing communicates from third party decryption? Under what circumstances does the company modify their products to accommodate state decryption desires?

iii. Mandatory Decryption Requirements for TSPs

Telecommunications service providers (TSPs) have been routinely involved in lawful access debates in Canada and have particular mandatory decryption requirements in excess of many other types of service providers. TSPs (including mobile

---

[321] R-25, 9: Communications Security Establishment, "Security of Blackberry Pin to Pin messaging," (document originally signed by Toni Moffa, Deputy Chief IT Security) at 280, Volume 2 of R v Mirarchi, QCCA File No 500-10-006048-159, Appellant's Factum, January 22, 2016, obtained by Mark Phillips available at CIPPIC, "Report Calls for Greater Transparency, Proactive Control of IMSI Catchers" <https://cippic.ca/news/report_calls_for_proactive_transparency_and_control_of_imsi_catchers>.

[322] R-25, 18: Affidavit of Alan William Treddenick at (sworn 24 November 2015, Ottawa) at 376 ib Volume 2 of R v Mirarchi, QCCA File No 500-10-006048-159, Appellant's Factum, January 22, 2016, obtained by Mark Phillips available at CIPPIC, "Report Calls for Greater Transparency, Proactive Control of IMSI Catchers" <https://cippic.ca/news/report_calls_for_proactive_transparency_and_control_of_imsi_catchers>.

> "I verily believe the BlackBerry global encryption key that is used to scramble its BlackBerry Messenger Service (hereinafter, BBM) and PIN to Pin messaging service is not known to the general public."

[323] *R v Mirarchi*, 2015 QCCS 6628 at paras 45 and 166.

[324] R-25, 18: Affidavit of Alan William Treddenick at (sworn 24 November 2015, Ottawa) at 376 in Volume 2 of *R v Mirarchi*, QCCA File No 500-10-006048-159, Appellant's Factum, January 22, 2016, obtained by Mark Phillips available at CIPPIC, "Report Calls for Greater Transparency, Proactive Control of IMSI Catchers" <https://cippic.ca/news/report_calls_for_proactive_transparency_and_control_of_imsi_catchers>.

[325] *R v Stinchcombe*, [1991] 3 S.C.R. 326.

[326] Paul Cherry (2017), "Montreal Mafia: Project Clemenza screeches to a halt as cases stayed," (17 July, 2017) *Montreal Gazette* <http://montrealgazette.com/news/local-news/montreal-mafia-project-clemenza-screeches-to-a-halt-as-cases-stayed>.

telephony, wireline telephony, and Internet access providers) operate pursuant to significant regulatory obligations over their operations and in accordance with strictly regimented government licensing requirements. In the past, these licensing conditions have been used to regulate critical issues in the encryption debate and to try to bypass the democratic legislative process.

Government-issued licenses are often required as a precondition to operate or to access inputs that are essential to providing a telecommunications service. Inputs include spectrum needed to provide mobile connectivity, and permissions to establish landing sites for international cables. Licenses to access these responses often include restrictions that ensure interoperable technical standards, that allocate and coordinate scarce public resources (e.g., radio spectrum), or that impose public policy obligations—including mandatory decryption and other lawful access and intercept capabilities.[327] In Canada, these lawful access rules take the form of the Solicitor General's Enforcement Standards for Lawful Interception of Telecommunications (SGES).[328]

The SGES are a package of standards that were developed in secret by Public Safety Canada (operating at the time as the Solicitor General's office) in the early 1990s and which have been updated periodically (the most recent known update having taken place in 2015). They establish a set of services and technical capabilities that law enforcement and security services view as necessary to facilitate the lawful interception of communications.[329] Broadly, these standards establish access, collection, interception and decryption conditions. Standard 12 of the SGES is directly relevant to the encryption debate, and states:

> "If network operators/service providers initiate encoding, compression or encryption of telecommunications traffic, law enforcement agencies require the network operators/service providers to provide intercepted communications en clair."[330]

The government's annotation for this standard reads:

> "Law enforcement requires that any type of encryption algorithm that is initiated by the service provider must be provided to the law enforcement agency unencrypted. This would include proprietary compression algorithms that are employed in the network. This does not include end to end encryption that can be employed without the service provider's knowledge."[331]

These standards have, to date, been imposed on telecommunications service providers which have acquired spectrum licenses for the specific purpose of providing retail mobile voice telephony.[332] However, a government spokesperson stated in 2013 that the SGES might be extended in the future to other types of radio-based communications[333] and other types of spectrum

---

[327] For example, the Canadian government has noted that it "does not currently require that [Fixed Service Satellite] providers provide lawful intercept capabilities," but the licensing documentation explicitly notes "that compliance with a requirement to provide lawful intercept capability may be imposed via a licence condition or another legislative provision at any point in time in the future."

See Industry Canada (2015), "Procedure for the Submission of Applications to License Fixed Earth Stations and to Approve the Use of Foreign Satellites in Canada," (April 2015) Client Procedure Circular CPC-2-6-01 <https://www.ic.gc.ca/eic/site/smt-gst.nsf/vwapj/CPC-2-6-01-Issue-5-EN.pdf/$file/CPC-2-6-01-Issue-5-EN.pdf>.

[328] Public Safety Canada (2008), National Security Technology Division, "Solicitor General's Enforcement Standards for Lawful Interception of Telecommunications - Compliance Table", obtained by Tamir Israel, (current as of 17 November 2008) <https://cippic.ca/uploads/ATI-SGES_Annotated-2008.pdf>.

[329] Christopher Parsons (2013), "Lawful Access is Dead; Long Live Lawful Intercept!" (13 February 2013) <www.christopher-parsons.com/lawful-access-is-dead-long-live-lawful-intercept/>; Christopher Parsons (2015), "The Governance of Telecommunications Surveillance: How Opaque and Unaccountable Practices and Policies Threaten Canadians", *Telecom Transparency Project*, version 1.5, (may 2015) <http://www.telecomtransparency.org/wp-content/uploads/2015/05/Governance-of-Telecommunications-Surveillance-Final.pdf> at 10; Colin Freeze & Rita Trichur (2013), "Ottawa sought broader access to smartphone user data, records show," *The Globe and Mail* (13 September 2013) <http://www.theglobeandmail.com/technology/mobile/ottawa-sought-broader-access-tosmartphone-user-data-records-show/article14343991/>.

[330] Public Safety Canada (2008), National Security Technology Division, "Solicitor General's Enforcement Standards for Lawful Interception of Telecommunications - Compliance Table", obtained by Tamir Israel, (current as of 17 November 2008), <https://cippic.ca/uploads/ATI-SGES_Annotated-2008.pdf>.

[331] *Ibid.*

[332] Christopher Parsons (2015), "The Governance of Telecommunications Surveillance: How Opaque and Unaccountable Practices and Policies Threaten Canadians", *Telecom Transparency Project*, version 1.5 (May 2015) <http://www.telecomtransparency.org/wp-content/uploads/2015/05/Governance-of-Telecommunications-Surveillance-Final.pdf>. See also: Industry Canada (2015), "Procedure for the Submission of Applications to License Fixed Earth Stations and to Approve the Use of Foreign Satellites in Canada," (April 2015) Client Procedure Circular CPC-2-6-01 <https://www.ic.gc.ca/eic/site/smt-gst.nsf/vwapj/CPC-2-6-01-Issue-5-EN.pdf/$file/CPC-2-6-01-Issue-5-EN.pdf>.

[333] Christopher Parsons (2013), "Lawful Access is Dead; Long Live Lawful Intercept!" (13 February 2013) <www.christopher-parsons.com/lawful-access-is-dead-long-live-lawful-intercept/>.

clients are now notified upon application that lawful intercept obligations may be imposed on them at one point in the future.[334] Based on the 2015 version of the SGES, the decryption requirements:

- Only apply to encryption imposed by the TSP itself to its own communication services, as opposed to encryption imposed by third party services accessed by users on the TSP's network;
- May constitute "bulk" or "blanket" requirements, meaning that the obligation to decrypt, or to maintain decryption capabilities, is system-wide and not case by case;
- Do not require the TSP to adopt a specific *type* of encryption system in order to facilitate government access, and does not require TSPs to develop new capabilities to decrypt communications they do not otherwise have the ability to decrypt.

The current SGES does not preclude TSPs from employing end-to-end encryption, a significant limit on the scope of the obligation. Nonetheless, the imposition of a blanket decryption capability of even this more limited type through a secretive and unilateral licensing mechanism remains problematic. Blanket obligations in general can be an issue (in contrast to case-by-case decryption obligations based on specific grounds) in that such obligations can encourage TSPs to proactively design or constrain their services in ways that render compliance more efficient or cost effective. This, in turn, can detrimentally constrain service innovation and limit the adoption of more secure mechanisms. Blanket standardization can also have a normative effect by incentivizing affected companies to resist departures from the status quo or from adopting contemporary or best-practice technologies in order to facilitate status quo compliance.[335]

Regulatory conditions like the SGES also evolve over time, driven by ever-shifting government priorities. Such changes may take place secretly and without public consultation. The Canadian government has previously signalled its willingness to use licensing requirements to extend decryption obligations beyond mobile service providers to other types of licensed entities.[336] More controversially, in 2012 there was a government attempt to expand the scope of SGES.[337] The proposed change in language would have removed the term "circuit-switched voice telephony" from the lawful intercept condition and redefined licensees to include "a service provider using an interconnected radio-based transmission facility for compensation."[338] This change, proposed in the absence of any legislated framework or democratic process, would have dramatically altered the relationship between law enforcement and communications intermediaries. Indeed, this attempt to expand decryption obligations occurred at the same time as the government was attempting to pass controversial legislation (former Bill C-30, *Protecting Children from Internet Predators Act*) that would have achieved the same effect as the proposed license changes.[339] The government eventually

---

[334] Industry Canada (2015), "Procedure for the Submission of Applications to License Fixed Earth Stations and to Approve the Use of Foreign Satellites in Canada," (April 2015) Client Procedure Circular CPC-2-6-01 <https://www.ic.gc.ca/eic/site/smt-gst.nsf/vwapj/CPC-2-6-01-Issue-5-EN.pdf/$file/CPC-2-6-01-Issue-5-EN.pdf>.

[335] As an example, the presence of the SGES obligation might have been the driving force behind an attempt by Rogers Communications and Alcatel-Lucent (a major Canadian-based service provider and an equipment manufacturer, respectively) to undermine the implementation of end-to-end encryption in mobile services. At a standards organization, the two companies proposed that an end-to-end encryption protocol slated for inclusion in the emerging 4G mobile protocol be implemented with a pseudo-random-number generator in lieu of an actual random-number generator. Were the attempt successful, Canadian companies such as Rogers would have maintained their ability to provide intercepted communications to law enforcement in decrypted format, consistent with historical practices set out in the SGES. Put another way, even though the SGES decryption standard imposed no obligation on Rogers to undermine end-to-end encryption standards, the company attempted to do so for what appear to be reasons of business convenience. The result is a weakened cryptography standard that is easier for any party to break, not just Rogers or the police. Even a less intrusive blanket decryption requirement, then, can potentially operate to weaken the development and adoption of stronger, non-prohibited encryption by normalizing a set of existing sub-optimal conditions.

See: Steven J. Murdoch (2016), "Insecure by Design: Protocols for Encrypted Phone Calls", (2016) 49(3) *IEEE Computer Magazine* 25 <http://sec.cs.ucl.ac.uk/users/smurdoch/papers/ieeecomp16encryptedphone.pdf>.

[336] Christopher Parsons (2013), "Lawful Access is Dead; Long Live Lawful Intercept!" (13 February 2013) <www.christopher-parsons.com/lawful-access-is-dead-long-live-lawful-intercept/>.

[337] Industry Canada (2012), "Consultation on a Licensing Framework for Mobile Broadband Services (MBS) — 700 MHz Band," (April 2012) <http://www.ic.gc.ca/eic/site/smt-gst.nsf/eng/sf10363.html>.

[338] Industry Canada (2012), "Consultation on a Licensing Framework for Mobile Broadband Services (MBS) — 700 MHz Band," (April 2012) <http://www.ic.gc.ca/eic/site/smt-gst.nsf/eng/sf10363.html> at 108.

[339] The proposed changes to the SGES, once publicly revealed, were presented as "an interim measure until full implementation of the [lawful access] legislation" (referring to Bill C-30, which never became law)."

See Christopher Parsons (2015), "The Governance of Telecommunications Surveillance: How Opaque and Unaccountable Practices and Policies Threaten Canadians", *Telecom Transparency Project*, version 1.5 (2015) <http://www.telecomtransparency.org/wp-content/uploads/2015/05/Governance-of-Telecommunications-Surveillance-Final.pdf> at 11.

abandoned the effort on both fronts after internal debate and pushback from industry actors.[340] However, the case study represents a clear example of how regulatory tools like the SGES can be used to bypass important democratic safeguards.

The federal government has also proposed legislation to extend decryption obligations from various wireline and wireless telecommunications carriers (e.g., Rogers and Bell) to other types of digital intermediaries and service providers (e.g., Google, Facebook, and Twitter). As of this report's publication, such legislation has never been successfully passed into law. This debate over lawful access in Canada has stretched for over a decade, with similar proposals repeatedly reintroduced as Bill C-47 (*Technical Assistance for Law Enforcement in the 21st Century Act*) in 2009, then Bill C-52 (*Investigating and Preventing Criminal Electronic Communications Act*) in 2010.[341] Like these predecessors and the failed changes to the SGES discussed aboe, Bill C-30, which was proposed in 2012, would have extended the mandatory decryption obligation to a much broader range of technical actors, including email providers, social media networks, cloud service providers, and other entities that were not subject to any licensing regime.[342] Serious technical, practical, and legal issues arise when states seek to extend these obligations beyond traditional TSPs and to a broader range of "over the top" service providers.

The decryption obligation in Bill C-30 would have only applied to encryption applied by the TSP itself. Sub-section 6(3) of the proposed Bill read:

> "If an intercepted communication is encoded, compressed, encrypted or otherwise treated by a telecommunications service provider, the service provider must use the means in its control to provide the intercepted communication in the same form as it was before the communication was treated by the service provider."[343]

This obligation would not have required TSPs to decrypt communications which were encrypted by another, unrelated party. So, for example, a Certificate Authority (an entity responsible for issuing and authenticating digital certificates used to identify websites to visitors and encrypt traffic between the visitor and the site itself) might have the means within its control to forge a certificate used by Google to encrypt traffic with its own customers (or between those customers using Google services). This forged key could then be used by law enforcement to decrypt such communications in real-time.[344] However, because Google is the TSP that actually applies the encryption in this scenario, the rule in former Bill C-30 could not have required the Certificate Authority to "use the means in its control to provide the intercepted communication in the same form as it was before the communication was treated by the service provider."[345]

Second, under the proposed law, a service provider would have only been obligated to use means "within its control." Returning to the above scenario, Google uses perfect forward secrecy when encrypting communications to or from its servers meaning, among other things, that decryption keys are automatically discarded immediately after each interaction.[346] This means

---

[340] Colin Freeze & Rita Trichur (2013), "Ottawa sought broader access to smartphone user data, records show," *The Globe and Mail* (13 September 2013) <http://www.theglobeandmail.com/technology/mobile/ottawa-sought-broader-access-tosmartphone-user-data-records-show/article14343991/>.

[341] Bill C-47, *Technical Assistance for Law Enforcement in the 21st Century Act*, 2nd Sess, 40th Parl, 1st Reading (18 June 2009), <http://www.parl.ca/Content/Bills/402/Government/C-47/C-47_1/C-47_1.PDF>, proposed sub-sections 6(3) and 6(4); Bill C-52, *Investigating and Preventing Criminal Electronic Communications Act*, 3rd Sess, 40th Parl, 1st Reading (1 November 2010), <http://www.parl.ca/Content/Bills/403/Government/C-52/C-52_1/C-52_1.PDF>, proposed sub-sections 6(3) and 6(4); Bill C-30, *Protecting Children from Internet Predators Act*, 1st Sess, 41st Parl, 1st Reading (14 February 2012) <http://www.parl.ca/Content/Bills/411/Government/C-30/C-30_1/C-30_1.PDF>, proposed sub-sections 6(3) and 6(4).

[342] See definitions of "telecommunications service" and "telecommunications service provider." Proposed sub-section 2(1) of Bill C-30, *Ibid*, is indicative. The extension of some of Bill C-30's obligations, including its decryption obligations, to entities other than telecommunications common carriers (generally, entities that provide access to the Internet) was particularly controversial. By contrast, the United States Communications Assistance for Law Enforcement Act (CALEA), provides a similar decryption obligation but only applies it telecommunications carriers and perhaps some Voice Over IP providers. See 47 USC § 1002.

Bill C-30, *Protecting Children from Internet Predators Act*, 41st Parl, 1st Reading (14 February 2012) <http://www.parl.ca/Content/Bills/411/Government/C-30/C-30_1/C-30_1.PDF>.

[343] Bill C-30, *Protecting Children from Internet Predators Act*, 41st Parl, 1st Reading (14 February 2012) <http://www.parl.ca/Content/Bills/411/Government/C-30/C-30_1/C-30_1.PDF>, proposed sub-section 6(3).

[344] John Leyden (2011), "Inside 'Operation Black Tulip': DigiNotar hack analysed", *The Register* (6 September 2011) <https://www.theregister.co.uk/2011/09/06/diginotar_audit_damning_fail/>; Dan Goodin (2015), "Symantec employees fired for issuing rogue HTTPS certificate for Google", *Ars Technica* (21 September 2015) <https://arstechnica.com/information-technology/2015/09/symantec-employees-fired-for-issuing-rogue-https-certificate-for-google/>.

[345] Bill C-30, *Protecting Children from Internet Predators Act*, 41st Parl, 1st Reading (14 February 2012) <http://www.parl.ca/Content/Bills/411/Government/C-30/C-30_1/C-30_1.PDF>, proposed sub-section 6(3).

[346] For a more detailed description of forward secrecy, see Part 1 of this report. For the purposes of this provision, the key relevant feature of a system using forward secrecy is the fact that session keys are only kept ephemerally and automatically discarded immediately after use.

that if the government had intercepted a communication between two Google customers, and later invoked proposed sub-section 6(3) of Bill C-30 or a comparable provision, Google would have no means "within its control" to decrypt these communications, as it does not keep the decryption keys it would need to carry out such an operation. A number of Canadian courts have held that ephemeral storage or temporary caching by an intermediary for the purpose of facilitating a communication does not amount to "control" and, therefore, the temporary storage of encryption keys by Google would not bring these keys "within its control" in a legal sense even if Google were able to extract these keys in a technical or practical sense.[347]

Third, proposed sub-section 6(4) of Bill C-30 explicitly stated that, in meeting its obligations under proposed sub-section 6(3), a service provider would not have been obligated to "develop or acquire decryption techniques or decryption tools." Returning to our scenario once again, if a law enforcement agency approached Google *before* intercepting the same communications between the two Google customers mentioned above and asked Google to develop a new mechanism that would permit it to keep the encryption keys that its systems regularly discard, Google could rely on proposed sub-section 6(4) to refuse the demand.

These same limitations would also have prevented Bill C-30 from applying to other controversial scenarios such as the *Apple v FBI* dispute, where the FBI sought a court order compelling Apple to develop a new mechanism for bypassing the strong encryption it included in modern iPhones. However, Bill C-30's decryption mechanism remained profoundly controversial for the broad range of services to which it would have applied if the legislation had passed in law. In addition, applying even a narrowly tailored decryption mandate to an open-ended multiplicity of Internet services is likely to have complex impacts on evolving services that are inherently characterized by rapid innovation.

iv. Other Forms of Mandatory Participation by Third Parties

There are some circumstances in which an individual or intermediary may be compelled by court order to provide access to encrypted records, credentials, keys, or other information to facilitate a law enforcement investigation. Where such orders are directed at the subject of a criminal investigation, their *Charter* rights to silence and against self-incrimination will generally be engaged. However, third parties generally do not have such recourse. In this section we discuss two of the primary mechanisms used in these contexts, production orders and assistance orders.

a) Production Orders

Canadian law enforcement agencies can compel a third person, including both individuals and corporate entities, to disclose documents and records using a production order. The wording of the *Criminal Code* production order provision clarifies that this authority may be used "to prepare and produce a document containing data that is in their possession or control at that time" the order is received.[348] A production order does not require the service provider to design their technology in such a way that it facilitates law enforcement access to "useful" information. For example, if the information sought about a user is only available to a service provider is in encrypted form, a production order would not require the service provider to actively engineer a new mechanism to subvert its security measures in order to acquire that information in plaintext form.

The *Criminal Code* provisions also protect persons under investigation from being targeted by such an order on the basis that doing so would interfere with their right against self-incrimination.[349] Similarly, while third persons are not excused from production order compliance on the basis that the documents revealed may "tend to incriminate them or subject them to a proceeding or penalty," section 487.0196 of the *Criminal Code* ensures that such records cannot be used or received in evidence to incriminate them in subsequent criminal proceedings.[350] This model is similar to the approach in countries such as Belgium that allow a judge or certain other officials to require third parties to provide access to plaintext records to the extent they are able to

---

[347] See CIPPIC, Memorandum of Law (2012), *TELUS Communications Co v Her Majesty the Queen*, SCC File No 34252 <https://cippic.ca/uploads/TCCvHMQ-FACTUM.pdf> at paras 20-24; *R v TELUS Communications Co*, 2013 SCC 16 at paras 40-41.

[348] s. 487.014 (1) *Criminal Code* R.S.C., 1985, c. C-46.

[349] s. 487.014 (4) *Criminal Code* R.S.C., 1985, c. C-46.

[350] See also *R v Nedelcu*, 2012 SCC 59.

do so, but which protect criminally accused persons and other closely-linked individuals (e.g., spouses) from compelled participation.[351]

In theory, the production order powers could potentially be used to compel a third party to provide access to a static decryption key.[352] Depending on the design of the third party's technical infrastructure, such keys could be used to decrypt more data, related to more individuals, than would be necessary in the course of a single investigation. For example, the "global" decryption key for BlackBerry PIN-to-PIN technology referenced in *R v. Mirarchi* implicated the security of all non-enterprise BlackBerry communications, far exceeding the investigative needs of the case at issue.[353] Using a production order to obtain "global" decryption keys would create a clear problem of overbreadth and an opportunity for abuse, furnishing law enforcement with a decryption capability against all non-targeted individuals. In the absence of appropriate safeguards, it could also allow for the key to be re-used in the course of later, unrelated investigations without independent authorization. This, in turn, undermines the integrity of implicated communications and is generally disproportionate.

b) Assistance Orders

The *Criminal Code* includes broadly-worded provisions that are designed to compel third parties (including companies involved in data storage and communications) to assist law enforcement agencies in carrying out lawfully authorized surveillance. Orders which conscript third parties in this manner are inherently likely to raise issues of necessity and proportionality, may jeopardize consumer trust, or could impose a significant burden on private actors. Section 487.02 of the *Criminal Code* empowers a judge who authorizes electronic surveillance to order any person to provide any assistance "if the person's assistance may reasonably be considered to be required to give effect to the authorization or warrant."[354] In theory, these powers could be used to compel a private actor to to take certain kinds of measures to bypass encryption in support of law enforcement activities. The subjects of such orders are often uninvolved third parties, and as a result neither they, nor the actual target of the investigation, are likely to be shielded by virtue of the general protection against self-incrimination. Very few safeguards currently exist in the assistance order context, with one Supreme Court of Canada decision holding that even substantial (though not prohibitive) cost does not preclude a court from compelling a service provider from rendering assistance on the basis that such assistance is merely a cost of doing business.[355] Current Canadian jurisprudence lacks a sophisticated mechanism for assessing necessity and proportionality considerations in such contexts, and courts have been somewhat unsympathetic to arguments regarding undue burden. For example, arguments that the warrant sought in *R v. Telus Communications Co.* inappropriately shifted the costs associated with state surveillance to Telus customers were rejected.[356] In *Equustek,* the Supreme Court of Canada also suggested that Canadian courts are willing to go quite far in imposing positive obligations on uninvolved third parties to assist the state, though latitude for such foreign territorial impacts ceases where it demonstrably impacts on human rights.[357]

Given the open-ended language in the *Criminal Code*, the nature and scope of an assistance order will vary depending on the context of an investigation. One example involves a case in which the FBI sought access to the encrypted emails of a U.S. resident who was using a Canadian email service provider based in British Columbia (i.e., Hush Communications Inc. or "Hushmail").[358] Hushmail had designed its email services with strong security features and marketed them accordingly. As a result

---

[351] Art. 9, *Loi du 28 novembre 2000 relative à la criminalité informatique* (Belgium); Art. 156 Code d'Instruction Criminelle (Belgium).

[352] Though there are no examples of such an application, the Canadian government's 1998 Cryptography Policy included a statement (which applies equally to the following section on assistance orders) that:

> "we also need to make it clear that warrants and assistance orders also apply to situations where encryption is encountered - to obtain the decrypted material or decryption keys,"

See Speaking Notes on "Canada's Cryptography Policy" (1998) for the Honourable John Manley, Minister of Industry, to the National Press Club (1 October 1998) <http://fas.org/irp/news/1998/10/981001-crypto.htm>. See also: Christopher Parsons and Tamir Israel (2015) "Canada's Quiet History Of Weakening Communications Encryption", *Citizen Lab* (11 August 2015) <https://citizenlab.ca/2015/08/canadas-quiet-history-of-weakening-communications-encryption/>.

[353] *R v Mirarchi*, QCCA File No 500-10-006048-159, Appellant's Factum, January 22, 2016, Vol. II at 133 <>https://cippic.ca/uploads/Mirarchi_QCCA_Appellant_Factum/2-VOL_II.pdf>

[354] s. 487.02 *Criminal Code* RSC 1985, c. C-46.

[355] *R v TELUS Communications Co*, 2013 SCC 16.

[356] *Ibid* at paras 127, 193.

[357] *Google Inc v Equustek Solutions Inc*, 2017 SCC 34.

[358] Ryan Singel (2007), "Encrypted E-mail Company Spills to Feds," (11 July, 2007) *Wired*<https://www.wired.com/2007/11/encrypted-e-mai/>.

of technical design and business choices made by the company, only users had access to the decrypted versions of the email messages. To facilitate FBI access, a British Columbia court issued an order which compelled Hushmail to develop and engineer an entirely new mechanism which would allow the company to extract a single user's decryption key from the decryption mechanism itself.[359] Hushmail could do so because the mechanism in question was controlled by the company, and hosted and operated on Hushmail's own infrastructure.[360] Hushmail was then obligated to obtain the targeted individual's key and use it to decrypt the target's emails through this newly-developed exploit.[361] While at face value this response may have appeared to be a targeted solution (i.e., it only affected one individual), such orders deputize the engineering capabilities of a service provider against their own users in a profound way, and undermine user confidence in a critical security mechanism—the password interface—which requires high level of trust.[362]

Orders that appear targeted in nature can also have systemic consequences. In the United States, one of several orders Apple received under the *All Writs Act* of 1789 (a legal mechanism that is somewhat similar in substance to assistance orders under s. 487.02 of the Canadian *Criminal Code*) sought to compel the company to develop and electronically sign new software to bypass security encryption measures built into the iPhone 5C.[363] This order would have allowed the FBI to unlock a work phone belonging to one of the 2015 San Bernardino shooters. The request was legally contested by Apple as well as by other major Silicon Valley companies and prominent civil liberties organizations.[364] The FBI ultimately withdrew its request on the basis that they had successfully unlocked the phone without Apple's assistance.[365] Were the order upheld, however, it would have had far-ranging impacts. Once the tool created by Apple for the purpose of bypassing its secure encryption mechanism was developed, it could potentially be leveraged by other state entities (whether in the United States or abroad) as well as expose consumers to serious new technical vulnerabilities. In effect, this targeted order could have risked creating a systemic vulnerability.[366] Some experts have also pointed out that the U.S. government has the ability to seek similar forms of technical assistance orders through the secretive United States Foreign Intelligence Surveillance Court (FISC).[367]

Another example of a seemingly targeted mechanism that in practice has systemic impacts is found in a controversial draft law that was circulated for consultation by China's State Cryptography Administration in early 2017. Article 20 of the draft law would grant the Chinese government new authority to compel private companies to offer "decryption technology support" on a case-by-case basis for the purpose of national security and criminal investigations, to maintain the secrecy of that cooperation,

---

[359] *Ibid*.

[360] *Ibid*.

[361] *Ibid*.

[362] See similar concerns in the context of Apple's end-to-end messaging app:

Wired Staff Security (2015), "Apple's iMessage Defense Against Spying has One Flaw", *Wired* (9 August 2015) <https://www.wired.com/2015/09/apple-fighting-privacy-imessage-still-problems/>.

[363] Order Compelling Apple Inc. to Assist Agents in Search, US District Court for the Central District of Columbia (16 February 2016) online at Electronic Frontier Foundation <https://www.documentcloud.org/documents/2714001-SB-Shooter-Order-Compelling-Apple-Asst-iPhone.html>; Government's Motion to Compel Apple Inc. to Comply with this Court's February 16, 2016 Order Compelling Assistance in Search, US District Court for the Central District of Columbia (19 February 2016) online at Electronic Frontier Foundation (2016) <https://www.eff.org/files/2016/03/02/fbi-apple-govt-motion-to-compel.pdf>.

[364] Apple Inc. (2016), "Amicus Briefs in Support of Apple," (2 March 2016) <https://www.apple.com/newsroom/2016/03/03Amicus-Briefs-in-Support-of-Apple/>.

[365] Ellen Nakashima (2016), "FBI paid professional hackers one-time fee to crack San Bernardino iPhone", *The Washington Post* (12 April 2016) <https://www.washingtonpost.com/world/national-security/fbi-paid-professional-hackers-one-time-fee-to-crack-san-bernardino-iphone/2016/04/12/5397814a-00de-11e6-9d36-33d198ea26c5_story.html?utm_term=.01b7f7644665>.

[366] Joseph Bonneau (2016), "A Technical Perspective on the Apple iPhone Case", *Electronic Frontier Foundation* (19 February 2016) <https://www.eff.org/deeplinks/2016/02/technical-perspective-apple-iphone-case>.

Note that even when governments attempt to keep such vulnerabilities secret, they may be independently discovered, stolen, or leaked. See e.g.: Scott Shane, Nicole Perlroth, and David E. Sangernov (2017), "Security Breach and Spilled Secrets Have Shaken the N.S.A. to Its Core", *New York Times* (17 November 2017) <https://www.nytimes.com/2017/11/12/us/nsa-shadow-brokers.html>; Bruce Schneier (2017), "Who Is Publishing NSA and CIA Secrets, and Why?", *Lawfare* (27 April 2017) <https://www.lawfareblog.com/who-publishing-nsa-and-cia-secrets-and-why>; Bruce Schneier (2016), "The NSA is Hoarding Vulnerabilities", *Schneier on Security* (26 August 2016) <https://www.schneier.com/blog/archives/2016/08/the_nsa_is_hoar.html>.

[367] See Marcy Wheeler (2017), "Ron Wyden is Worried the Government Will Use FISA Process to Force Companies to Make Technical Changes", *Empty Wheel* (24 October 2017) <https://www.emptywheel.net/2017/10/24/ron-wyden-is-worried-the-government-will-use-fisa-process-to-force-secret-technical-changes/>; Marcy Wheeler (2017), "The Government is Secretly Hiding Its Crypto Battles in the Secret FISA Court" *Empty Wheel* (15 November 2017) <https://www.emptywheel.net/2017/11/15/yup-the-government-is-secretly-fighting-the-crypto-wars-in-the-fisa-court/>; Aaron Mackey and Andrew Crocker, "Proposal to Restrict Technical Assistance Demands Before Secret Surveillance Court Raises More Questions About Section 702", Electronic Frontiers Foundation (25 October 2017) <https://www.eff.org/deeplinks/2017/10/proposal-restrict-technical-assistance-demands-secret-surveillance-court-raises>.

and to face penalties for non-compliance.[368] In countries where broad powers to mandate private sector assistance are proposed, it is not always clear that design imperatives which categorically prevent service providers from accessing plaintext data will serve as a sufficient justification for non-compliance. In other words, in practice such broad powers may amount to a *de facto* ban on secure technologies like end-to-end encryption. Where there is legislative ambiguity about the scope of potential assistance powers, the result may be a "race to the bottom" for digital security, insofar as some service providers may weaken products proactively in anticipation that they will be required to do so at a later time in one or more jurisdictions.

C. MEASURES TARGETING SPECIFIC INDIVIDUALS & DEVICES

Certain measures are designed to circumvent encryption by directly targeting a specific individual or device. In some cases, these measures require the targeted individual to participate in the state's efforts to secure access to private data—whether by requiring an individual to surrender a password, to decrypt the data themselves using a private key or password they possess, or to turn over data in an unencrypted form. This conscriptive dimension has important implications for the constitutional rights at stake. In this section, we review the legal frameworks through which an individual may be mandated to participate in this process involuntarily—whether by court order in a criminal proceeding, as part of a search incident to arrest, or at the border, or in the private law context. Finally, we survey the legal problems that arise when courts draw prejudicial inferences from the use of encryption technology. We also note residual situations where an individual may be legally required to provide a password or private key, including conditions imposed on bail or sentencing and civil orders for the preservation of evidence.

i. Compelled Decryption and/or Key Disclosure

Some governments have the legal authority to compel individuals to provide access to encrypted data, be it on a particular device, network, or account. In certain cases these powers can be independently exercised by law enforcement officers whereas in others they follow an order by a criminal court. In some cases, a distinction is made between orders for the more targeted decryption of a particular file, as compared to the compelled disclosure of a decryption key, with the latter being more susceptible to overbroad application.[369] In the United Kingdom, Part III of the *Investigatory Powers Act* allows high-ranking law enforcement and intelligence agents to serve notice on an individual to compel the production of decrypted data under penalty of fine or imprisonment.[370] In South Africa, police, intelligence officials, and other high-level government actors can apply to a designated judge for a "decryption direction," which mandates decryption assistance or the disclosure of a decryption key. The law allows the court to invoke the participation of any person who possesses the key, with penalties for non-compliance which include large fines and up to ten years imprisonment.[371] Similar provisions (carrying the threat of up to two years in prison) were controversially adopted in Australia after 9/11 despite heavy criticism from civil society.[372]

Canadian criminal and constitutional law has taken a different approach than that of the United Kingdom or Australia. In its recent 2016 National Security Consultation Green Paper, the Canadian government affirmed that "no provisions specifically designed to compel decryption are found in the *Criminal Code,* the *CSIS Act* or in other Canadian laws. In other words, there is no law in Canada designed to require a person or organization to decrypt their communications."[373] The United States similarly lacks an explicit legal regime for compelled decryption. However, policing powers of general application have been invoked in various attempts to compel data decryption in both countries. It is useful to discuss the two in parallel given the considerable overlap in the legal reasoning between the two jurisdictions.

---

[368] Yuan Yang (2017), "China's cyber security law rattles multinationals," (30 May 2017) *Financial Times* <https://www.ft.com/content/b302269c-44ff-11e7-8519-9f94ee97d996?mhq5j=e1>; Covington & Burling LLP (2017), "China Releases Draft Encryption Law for Public Comment" (9 May 2017) <https://www.cov.com/-/media/files/corporate/publications/2017/05/china_releases_draft_encryption_law_for_public_comment.pdf> at 3.

[369] David Kaye (2015), Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/29/32, 29th session of the Human Rights Council <http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/Pages/ListReports.aspx> at 16-17.

[370] s. 49 and Schedule 2, *Regulation of Investigatory Powers Act 2000* (United Kingdom), c. 23.

[371] s. 21, s. 51, *Regulation of Interception of Communications and Provision of Communication-Related Information Act* (South Africa), No. 24286, 22 January 2003, Act No. 70, 2002.

[372] s. 3LA, *Crimes Act 1914* (Australia); see e.g. Electronic Frontiers Australia, "Cybercrime / Computer Crime Legislation" (30 November 2001) <https://www.efa.org.au/Issues/Privacy/cybercrimeact.html>.

[373] Public Safety Canada (2016), "Our Security, Our Rights," (2016) Background Paper <https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-scrt-grn-ppr-2016-bckgrndr/index-en.aspx> at 61.

INFORMATION BOX 4: FLAWED INCENTIVES AND PENALTIES FOR SILENCE

No matter how many safeguards are put in place, compelled decryption laws create inherently flawed incentive structures. Where individuals are charged with serious offences, the penalty associated with non-disclosure of a password is likely to be significantly less than that for the offence for which the decrypted evidence was initially sought. For example, under the United Kingdom's *Regulation of Investigatory Powers Act, t*he penalty for refusing to comply with a compelled decryption order is a fine or imprisonment up to two years—or up to five years for national security and child indecency cases.[i] Conversely, many individuals innocent of the crime for which they are being investigated may nonetheless choose not to cooperate with law enforcement or a court order. This may be due to fear that disclosure will result in a "fishing expedition" which reveals evidence of criminal acts that the state would otherwise not have independent grounds to believe had taken place, or be due to broader reasons of principle. In the U.K. for example, the first person convicted and sentenced to imprisonment under the *IPA* was a 33-year old "science hobbyist" with schizophrenia and no previous criminal record who "claim[ed] a belief in the right to silence."[ii] In a disturbing U.S. case, a suspect who claimed to have forgotten his password has been imprisoned for over two years (and remains imprisoned for an indefinite term) at the time of this report's publication despite American Fifth Amendment jurisprudence on the issue.[iii]

i Section 53, *Regulation of Investigatory Powers Act 2000,* c 23, Part III.

ii Christopher Williams (2009), "UK jails schizophrenic for refusal to decrypt files," (24 November 2009) The Register <https://www.theregister.co.uk/2009/11/24/ripa_jfl/>.

iii See *Motion to Vacate Order of Contempt in United States of America v Apple Macpro Computer et. al.* (28 August 2017), No. 15-mj-850 <https://www.documentcloud.org/documents/3986024-15-Mj-850-Req.html>; Catalin Cimpanu, "Man Who Refused to Decrypt Hard Drives Still in Prison After Two Years," (2 September, 2017) Bleeping Computer <https://www.bleepingcomputer.com/news/legal/man-who-refused-to-decrypt-hard-drives-still-in-prison-after-two-years/>.

A principled legal analysis of compelled decryption in Canada requires a contextual approach which considers all the relevant *Charter* rights at stake and accounts for the broader political, economic, and social implications of interfering with the protections offered by secure communications tools. Canadian courts have established that the data stored on personal electronic devices and the private communications transmitted between them invite an extremely high expectation of privacy, representing one of the most tightly protected spheres under section 8 of the *Charter*.[374] Nonetheless, there have been calls for an explicit legal power that could be invoked to compel individuals to decrypt information in the course of a criminal investigation. For example, in 2016 the Canadian Association of Chiefs of Police passed a resolution calling for new "legislative means for public safety agencies inclusive of law enforcement, through judicial authorization, to compel the holder of an encryption key or password to reveal it to law enforcement."[375]

Yet legislative proposals that would instruct Canadian law enforcement to simply "get a warrant" in order to compel password disclosure ignore a key set of constitutional issues. While no Canadian Supreme Court jurisprudence speaks directly to the potential lawfulness of compelled decryption powers, privacy is clearly not the only right at stake. In addition to the section 8 *Charter* protection against unreasonable search and seizure, compelled decryption will potentially implicate rights included in paragraph 11(c) of the *Charter* (which protects a person facing a criminal charge from being compelled to testify against him or herself),[376] section 13 of the *Charter* (which guards against the use of compelled evidence to incriminate an individual),[377] and section 7 (which protects the right to silence upon detention and in the pre-trial context[378] and which recognizes the principle

---

[374] *R v Morelli*, 2010 SCC 8; *R v Cole*, 2012 SCC 53; *R v Vu*, 2013 SCC 60; *R v Spencer*, 2014 SCC 43; *R v Fearon*, 2014 SCC 77; *R v TELUS Communications Co*, 2013 SCC 16; *R v Marakah*, 2017 SCC 59; *R v Jones*, 2017 SCC 60.

[375] Canadian Association of Chiefs of Police (2016), Resolution 2016-03, "Reasonable Law to Address the Impact of Encrypted and Password-protected Electronic Devices" <https://cacp.ca/resolution.html?asst_id=1197> at 19-20.

[376] *R v Noble*, [1997] 1 SCR 874.

[377] *R v Henry*, [2005] 3 SCR 609; *R v Noël*, [2002] 3 SCR 43.

[378] See *R v Hebert*, [1990] 2 SCR 151 at 178; *R v Singh*, 2007 SCC 48 at paras 43 et seq.

against self-incrimination as a component of "fundamental justice").[379] In the 2017 case *R v. Jones*, the Supreme Court noted the intimate link and complex interplay between these rights, specifically pointing out that the section 8 analysis regarding unreasonable search and seizure "should be informed by, and reconciled with, the principle against self-incrimination."[380]

The Supreme Court has more generally affirmed that "the state is not entitled to use its superior power to override the suspect's will and negate his choice to speak to the authority or to remain silent" and that statements which have been obtained in violation of that requirement should not be admitted.[381] Court-ordered password disclosure would stand in stark contrast to the foundational principle, recognized in both common law and in *Charter* jurisprudence, that individuals need not participate in securing evidence which would ultimately lead to their conviction; that burden rests with the Crown. As Iacobucci J wrote in *R. v. S. (R.J.)*:

> "Conceptually, it would seem that if there is any single organizing principle in the criminal process, it is the right of the accused to resist any effort to force him to assist in his own prosecution. It provides substance to the common law ideal of a fair trial through an adversarial or accusatorial process. The parties to a criminal prosecution are seen as competitors and the trial the competition. There is a principle against self-incrimination in Canada which is part of fundamental justice."[382]

The Quebec Court of Appeal recognized the application of this principle in Canada in the 2010 case *R c. Boudreau-Fontaine*. In that instance, a justice of the peace ordered an individual to produce passwords to decrypt a previously seized laptop as part of an investigation into the breach of his probation conditions.[383] Doyon J.A., writing for the Court of Appeal, noted both that the evidence was essential to the case and that the authorities had failed to seek out non-conscriptive alternative methods of accessing the data.[384] He went on to explain:

> " ... In other words, the justice of the peace was commanding the appellant to give essential information with the specific intent of having him incriminate himself. I cannot see how the criminal law can allow such an order. … this order raises the issues of the right to silence, the right to be presumed innocent, the right not to be conscripted against oneself, and the protection against self-incrimination. Commanded to participate in the police investigation and to give crucial information, contrary to his constitutional rights, the respondent made a statement (identification of his password) that is inadmissible and that renders the subsequent seizure of the data unreasonable. In short, even had the seizure been preceded by judicial authorization, the law will not allow an order to be joined compelling the respondent to self-incriminate.
>
> … Without necessarily being detained, the respondent was compelled to participate in his self-incrimination and was given no choice in the matter: he had to help the police officers convict him. This approach is unacceptable."[385]

Indeed, despite calls for new compelled decryption powers by organizations like the CACP, other members of the law enforcement community have expressed both concern and skepticism in response—including RCMP Commissioner Bob Paulson:

> "We're going to order someone to give us their password? … I don't know. I don't see that. I don't see a state where, you know, the police are ordering people to give up information. It would be like ordering a statement. I'm not a lawyer, but I do know, and I do understand, the dangers of

---

[379] *R v S (RJ)*, [1995] 1 SCR 451 at 512.

[380] *R v Jones,* 2017 SCC 60 at 31.

[381] *R v Hebert*, [1990] 2 SCR 151.

[382] *R v S (RJ)*, [1995] 1 SCR 451 at 512 [emphasis ours].

[383] *R c Boudreau-Fontaine*, 2010 QCCA 1108.

[384] *Ibid* at para 42.

[385] *Ibid* at paras 39 and 41.

> conscripted evidence, and the idea that the state is forcing one of its citizens to say or do anything, right? That's at odds with how I understand what we do."[386]

Canadian criminal law is not an outlier on the issue of compelled password disclosure. Under Belgian law, while third parties can be compelled to produce decrypted versions of encrypted files (not unlike a Canadian production order), that power does not extend to individuals subject to a criminal investigation and cannot be used to violate an individual's right against self-incrimination.[387] While the German government is legally permitted to deploy a wide range of other means to access encrypted data, individuals are protected from being compelled to participate in that process in accordance with the principle against self incrimination.[388] Though the United States Supreme Court has not directly addressed the issue of compelled decryption of communications or stored data, analysts from the U.S. Congressional Research Service conducted a review of lower court cases and concluded in 2016 that "there is a strong argument that the Fifth Amendment would bar the government from compelling an individual to disclose his passcode to the government."[389] It should be noted, however, that in the United States the law surrounding self-incrimination has focused on a fairly categorical approach to determining whether the compelled act or information is truly "testimonial" in nature. This aspect of "testimoniality" has historically allowed U.S. courts to distinguish between "compelled testimony," which exists only as a "product of the mind," and the involuntary seizure of DNA evidence or of a lockbox key (for example), which are not afforded the same constitutional protections.[390] In this regard, U.S. jurisprudence has generally suggested that the protection against self-incrimination should only apply to memorized, alphanumeric passphrases, rather than to the full range of mechanisms from which a private key may be derived—such as fingerprints, which have been

---

[386] Dave Seglins Robert Cribb and Chelsea Gomez (2016), "Should police be able to force you to hand over your digital passwords?," CBC News, (18 November 2016) <http://www.cbc.ca/news/investigates/police-power-privacy-encryption-1.3856375>.

[387] Art. 9, *Loi du 28 novembre 2000 relative à la criminalité informatique* (Belgium); Art. 156 Code d'Instruction Criminelle (Belgium).

[388] See summary at Library of Congress (2016), "Government Access to Encrypted Communications: Germany," <https://www.loc.gov/law/help/encrypted-communications/germany.php>:

> "[T]here is no legal basis that would compel the user to turn over an encryption or network key, in particular with regard to the nemo tenetur principle. The nemo tenetur principle, derived from the general right of personality found in the German Basic Law and from section 136, para. 1, sentence 1 of the German Code of Criminal Procedure, states that a suspect may not be compelled to cooperate in an investigation that would incriminate him/herself."

[389] Richard M. Thomson II & Chris Jaikaran (2016), "Encryption: Select Legal Issues," Congressional Research Service (3 March 2016) at 12 — the authors notably make specific reference to *In re Grand Jury Subpoena Duces Tecum* Dated March 25, 2011, 670 F.3d 1335 (11th Cir. 2004); *In re Boucher*, No. 2:06-mj-91, 2007 WL 4246473 (D. Vt. 2007); *United States v Kirschner*, 823 F. Supp. 2d 665, 666 (E.D. Mich. 2010); *Commonwealth v Baust*, No. 14-1439 (Va. 2d Jud. Cir. 2014).

However, courts in the United Kingdom have generally held otherwise and have so far upheld compelled decryption laws on the basis of this distinction. See *R v S & Anor*, [2008] EWCA Crim 2177 at paras 20 and 25:

> "On analysis, the key which provides access to protected data, like the data itself, exists separately from each appellant's "will". Even if it is true that each created his own key, once created, the key to the data, remains independent of the appellant's "will" even when it is retained only in his memory, at any rate until it is changed. If investigating officers were able to identify the key from a different source (say, for example, from the records of the shop where the equipment was purchased) no one would argue that the key was not distinct from the equipment which was to be accessed, and indeed the individual who owned the equipment and knew the key to it. Again, if the arresting officers had arrived at the premises in Sheffield immediately after S had completed the process of accessing his own equipment enabling them to identify the key, the key itself would have been a piece of information existing, at this point, independently of S himself and would have been immediately available to the police for their use in the investigation. ... "The key or password is, as we have explained, a fact."

Note: Putting aside implications for the right against self-incrimination, the court's logic here is fundamentally flawed. Neither the key nor the plaintext data sought have independent existence. The key is derived from the password once S enters it into his computer. The plaintext data is *only* generated once it is decrypted with the key. Once S completes his task, the plaintext is replaced with encrypted data and the key is no longer cached on the computer. There *is* no key to obtain from a different source from which investigators could identify the key. Certainly, if police opportunistically arrived after the key was derived from S's password, they might have been able to access it. But one could just as easily say the same about *any* item of incriminating knowledge—had the police entered while S was recounting criminal exploits to a colleague, or explaining to said colleague the location of incriminating evidence might be located, this information would surely have been immediately available to law enforcement. However, the right against self-incrimination does not rest on such opportunistic probabilities.

[390] See generally N. Dalla Guarda (2014), "Digital Encryption and the Freedom from Self-incrimination: Implications for the Future of Canadian Criminal Investigations and Prosecutions" Criminal Law Quarterly, Vol. 61, No. 1 (Jun 2014), p. 119-142; See also Richard M. Thomson II & Chris Jaikaran (2016), "Encryption: Select Legal Issues," Congressional Research Service (3 March 2016) at 9, noting that:

> "During the current decryption debate, many have attempted to employ this key/combo metaphor to access smartphones. This key/combo distinction appears to have originated in a dissent by Justice John Paul Stevens in the 1988 case Doe v. United States. There, Justice Stevens noted that while a suspect "may in some cases be forced to surrender a key to a strongbox containing incriminating documents," he cannot be "compelled to reveal the combination to his wall safe—by word or deed." His argument was premised on the idea that requiring someone to give up a safe combination required him to "use his mind to assist the prosecution in convicting him of a crime," whereas giving up a safe key would not. The Doe majority appeared to accept this dichotomy when noting in a footnote that "we do not disagree with the dissent that '[t]he expression of the contents of an individual's mind' is testimonial communication for the purposes of the Fifth Amendment." This dichotomy was later affirmed in Hubbell."

deemed "non-testimonial."[391] In practice, this distinction has only so far arisen where a fingerprint-based lock screen was involved, though other biometric identifiers are increasingly being used to unlock devices.[392]

This narrow and literal analysis of "testimoniality" onto the electronic device context by distinguishing between memorized, alphanumeric passwords and biometric lock schemes fails to take a purposive and contextual approach to the law. Accepting this distinction would allow an individual's constitutional rights to be profoundly altered based on technical design choices made by private technology companies, and in a manner which is likely to appear entirely arbitrary to end users,[393] rather than upon any contextual and principled basis. As the Supreme Court of Canada acknowledged in *R v Telus Communications*, "technical differences inherent in new technology should not determine the scope of protection afforded to private communications."[394] Furthermore, this transposition inappropriately structures the legal debate around the concept of testimony, rather than the fundamental core of the right against self-incrimination—namely, the question of whether the individual has been forced to participate in an investigation against herself.

In short, the issue of compelled password disclosure is an emerging problem in Canadian law that extends far beyond the general issues related to search and seizure of electronic devices in the criminal law context. Strong constitutional protections appear to generally prohibit the practice, but the issue remains somewhat unresolved without explicit guidance from the Supreme Court. To the extent that the law of self-incrimination continues its traditional focus on compelled participation, the *Charter* is likely to preclude the practice, regardless of what form the unlocking mechanism takes.

---

[391] See *Virginia v Baust*, No. CR14-1439 (Va. Cir. Ct. Oct. 28, 2014); *State of Minnesota v. Diamond,* No. 10-CR-14-1286, Minnesota Court of Appeal A15-2075 (January 17, 2017); but see also *In re Application for a Search Warrant* (Case Number 170M81), United States District Court for the Northern District of Illinois Eastern Division (February 16, 2017) opinion and order by Magistrate Judge M. David Weisman:

> "By using a finger to unlock a phone's contents, a suspect is producing the contents on the phone. With a touch of a finger, a suspect is testifying that he or she has accessed the phone before, at a minimum, to set up the fingerprint password capabilities, and that he or she currently has some level of control over or relatively significant connection to the phone and its contents. The government cites United States v. Wade, for the proposition that the Fifth Amendment privilege against self-incrimination offers no protection against compulsion to submit to fingerprinting. (Gvt. Mem. at2) (citing Wade,388 U.S. 218,223). This case, however, was decided in 1967, prior to the existence of cell phones, and in the context of utilizing fingerprinting solely for identification purposes. In the context of the Fifth Amendment, this Court finds these two starkly different scenarios: using a fingerprint to place someone at a particular location, or using a fingerprint to access a database of someone's most private information … The considerations informing the Court's Fourth Amendment analysis of a cell phone's role in modern day life, we believe raise Fifth Amendment concerns as well. We do not believe that a simple analogy that equates the limited protection afforded a fingerprint used for identification purposes to forced fingerprinting to unlock an Apple electronic device that potentially contains some of the most intimate details of an individual's life (and potentially provides direct access to contraband) is supported by Fifth Amendment jurisprudence."

See also Riana Pfefferkorn (2017), "Minnesota v. Diamond, Microsoft Ireland, and User-Hostile Path Dependence in the Law", *Center for Internet and Society* (19 January 2018) <https://cyberlaw.stanford.edu/blog/2018/01/oh-so-everybody%E2%80%99s-legal-expert-now-minnesota-v-diamond-microsoft-ireland-and-user>.

[392] While voice-printing and facial recognition software may also eventually become relevant, at present they involve even greater risks to security and are likely to require distinct legal analyses altogether on the basis that the expectation of privacy in (and the legal protections ultimately afforded to) these identifiers is less settled in law.

See David Talbot (2012), "Securing Your Voice", *MIT Technology Review* (27 August 2012) <https://www.technologyreview.com/s/428970/securing-your-voice/>; Fitz Tepper (2016), "Your voice is your password with Sesame's Alexa app", *TechCrunch* (8 May 2016) <https://techcrunch.com/2016/05/08/your-voice-is-your-password-with-sesames-alexa-app/>; Duc Nguyen (2009), "Your Face is NOT Your Password", Black Hat 2009, Washington D.C., <https://www.blackhat.com/presentations/bh-dc-09/Nguyen/BlackHat-DC-09-Nguyen-Face-not-your-password-slides.pdf>; Christopher Mims (2017), "Why Your Face Will Soon Be the Key to All Your Devices," *Washington Post* (20 August 2017) <https://www.wsj.com/articles/why-your-face-will-soon-be-the-key-to-all-your-devices-1503223200?mod=e2twd>.

[393] See Lex Gill (2018), "Law, Metaphor, and the Encrypted Machine", forthcoming in the Osgoode Hall Law Journal, 55:2 (Spring 2018) on SSRN <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2933269> at 27:

> "Perhaps most troublingly of all, the reliance on a court's distinction between 'testimony' and 'non-testimony' has the effect of putting the constitutional liberties of those who use encryption software at the mercy of opaque commercial interests and in the hands of those who make design decisions about consumer electronics. It is not hyperbolic to say that a decision by a major company like Google, Apple, Facebook or Microsoft to move away from passphrase-based keys and toward biometric ones could fundamentally erase the protection against compelled decryption under the Fifth Amendment for large numbers of people."

[394] *R v Telus Communications Co*, 2013 SCC 16 at para 5.

INFORMATION BOX 5: USING FINGERPRINTING POWERS TO UNLOCK CELL PHONES, A CANADIAN CASE STUDY

The fact that law enforcement might be legally entitled to secure an individual's fingerprints for the purpose of identification or evidence does not mean they are entitled to do so for the purpose of unlocking a device. Law enforcement in Canada are empowered to seek fingerprints of a suspect or accused person through a warrant, either overtly or covertly,[i] and to take the fingerprints of a person in lawful custody and who is charged or convicted of an indictable offence or in other serious cases.[ii] The use of 3-dimensional molds and other methods of faking a fingerprint have been previously used to successfully circumvent fingerprint-based protection schemes on modern smartphones.[iii] However, applying a legislative scheme intended to facilitate the collection of fingerprint records for the purpose of identifying individuals in an entirely different context and for an entirely different purpose (i.e., accessing private electronic communications and other data) is highly problematic from a legal perspective.[iv]

This tension was recognized by the Ontario Court of Justice in 2016 when it denied an application for a fingerprint impression warrant for the purpose of unlocking a mobile device. The application was denied in part on the basis that it sought "an order that would compel a suspect to actively participate in an ongoing investigation," which "would appear to offend the common law principle that no one can be compelled to aid the police in their investigation and against *Charter of Rights and Freedoms* provisions against self-incrimination."[v] Such an application could not have been contemplated at the time Parliament adopted s. 487.092 of the Criminal Code in 1996, and the Court went on to note that the purpose of the application was fundamentally different than that which was originally intended by the legislature:

> "This Impression Warrant application does not seek to seize a tangible impression of a body part, the finger, but rather to use the finger to obtain an electronic digital signal to generate a binary code that corresponds to the binary code stored in the device and thereby gain access to the device's memory; in other words to facilitate a continuation of the search. The motive behind the application, then, is to facilitate a search as distinct from making a seizure."[vi]

The application was ultimately rejected and the decision was not appealed in this case.

[i] s. 487.092 (1), s. 487.01, *Criminal Code* RSC 1985, c. C-46.
[ii] *Identification of Criminals Act*, RSC 1985, c. I-1.
[iii] Russell Brandom (2016), "Your phone's biggest vulnerability is your fingerprint", *The Verge* (2 May 2016) <https://www.theverge.com/2016/5/2/11540962/iphone-samsung-fingerprint-duplicate-hack-security>.
[iv] *R v Rodgers*, 2006 SCC 15, at paras 35-40 (DNA collection power created for identification cannot be used for broader investigative purposes).
[v] *Re: Impression Warrant Application* (s.487.092), 2016 ONCJ 197 at para 15.
[vi] *Re: Impression Warrant Application* (s.487.092), 2016 ONCJ 197 at paras 9-12.

ii. Search Incident to Arrest

"Search incident to arrest" is a common law exception to the general rule that warrantless searches are *prima facie* unreasonable in the context of the section 8 *Charter* guarantee against "unreasonable search and seizure."[395] The exception grants law enforcement the extraordinary power to conduct physical searches of a person and objects in their possession at the time of arrest without a warrant or reasonable grounds.[396] Law enforcement need only have a reasonable basis for a search, so long as that search remains truly incidental to the arrest in question.[397] In a 2014 decision called *Fearon,* the Supreme Court attempted to clarify the search incident to arrest power in cases involving electronic devices (in that instance, a mobile phone) and sought to modify the test given the privacy-invasive potential of such searches.[398] The majority in *Fearon* set out conditions pursuant to which law enforcement may conduct warrantless searches of electronic devices in an individual's possession once he or she has

[395] *R v Stillman*, [1997] 1 SCR 607 at para 33.

[396] *Ibid.*

[397] *R v Fearon*, 2014 SCC 77 at para 22.

[398] *R v Fearon*, 2014 SCC 77.

been arrested. The majority proposed a series of safeguard measures specific to the electronic device context in recognition of the heightened privacy interest inherent in electronic devices like phones and laptops,[399] namely, that such a search is conducted only where the underlying arrest is lawful, that it is "truly incidental to the arrest," that the manner in which it is carried out is narrowly tailored to its purpose, and that details of the search are properly documented by the officer.[400]

However, the phone in *Fearon* was neither password-protected nor encrypted when it was searched. As a result, the Court did not directly address whether any circumstance could arise where law enforcement could lawfully compel a password from an arrested person in order to facilitate the search of a device. Notably, the idea that an individual's constitutionally protected expectation of privacy is dependent on the use of a passwords was explicitly rejected. Justice Cromwell wrote for the majority:

> "...some courts have suggested that the protection s. 8 affords to individuals in the context of cell phone searches varies depending on whether an individual's phone is password-protected ... I would not give this factor very much weight in assessing either an individual's subjective expectation of privacy or whether that expectation is reasonable. An individual's decision not to password protect his or her cell phone does not indicate any sort of abandonment of the significant privacy interests one generally will have in the contents of the phone ... Cell phones—locked or unlocked—engage significant privacy interests."[401]

In other words, mobile computing devices engage a heightened expectation of privacy *regardless* of whether the device is secured using a password or encryption. This is in contrast to the Ontario Court of Appeal's earlier decision in the same case, which suggested that individuals might *only* have a heightened expectation of privacy on arrest where a phone is password-protected.[402] However, while the Ontario Court of Appeal suggested police might require warrant to unlock password-protected phones on arrest,[403] the Supreme Court found that despite the heightened privacy interest inherent in the mobile devices of arrestees, prior authorization from a judge to conduct a search is not always required.[404]

However, section 8 protections against unreasonable search and seizure are not the only *Charter*-protected rights at issue when a government agent seeks to compel an individual to disclose a password. Individuals also have a right to silence on arrest or detention and, as described in the previous subsection, the compelled disclosure of a password in such circumstances would plainly violate those rights. In the same way that an accused person cannot be forced by police to provide the whereabouts of a body or the names of her co-conspirators in questioning, the right to silence and against self-incrimination (afforded by both the common law and the *Charter*) should, in theory, ensure that she cannot be required to disclose a device password known only to her. Such a position would be in keeping with the view that *Charter* rights should not be read in isolation, and with the Supreme Court's recent remark in *Jones* that the principle against self-incrimination should inform the scope and parameters of other *Charter* protections, including the right against unreasonable search and seizure.[405] To this end, while the majority's comments in *Fearon* may serve to illuminate the relationship between the presence of a password and the reasonable expectation of privacy analysis under section 8, they do not offer a comprehensive view of the constitutional rights involved in compelled password disclosure in the search incident to arrest context.

While it is therefore unlikely that a police officer would be able require an individual to provide his or her password on arrest, the Supreme Court's decision in *Fearon* left the door open to a range of other measures that might be deployed to unlock

---

[399] *Ibid* at paras 51-53, 58:

> "It is well settled that the search of cell phones, like the search of computers, implicates important privacy interests which are different in both nature and extent from the search of other 'places' ... Cell phones ... engage significant privacy interests. ... the search of a cell phone has the potential to be a much more significant invasion of privacy than the typical search incident to arrest."

[400] *Ibid.*

[401] *Ibid* at para 53.

[402] *R v Fearon*, 2013 ONCA 106, 114 O.R. (3d) 81 at paras 73 and 75; *R v Fearon*, 2014 SCC 77 at para 110.

[403] *R v Fearon*, 2013 ONCA 106, 114 O.R. (3d) 81 at paras 73 and 75.

[404] *R v Fearon*, 2014 SCC 77.

[405] *R v Jones*, 2017 SCC 60 at paras 29-31.

mobile devices.[406] In particular, the potential for a legal distinction to be made between fingerprint-based passwords and those which exist only as a "product of the mind" remains problematic in the search incident to arrest context. Particularly where passwords are derived from biometrics such as fingerprints or facial scans, police might view it as within their rights on arrest to exploit biometric identifiers in order to unlock a device immediately on arrest. Recent Supreme Court jurisprudence related to the search incident to arrest doctrine compounds this possibility. For example, in a Supreme Court decision related to sexual assault called *Saeed*, the majority found that an individual could be subject to a warrantless penile swab "incident to arrest" for the purpose of preserving DNA evidence which had been alleged to belong to the complainant.[407] Whereas law enforcement are permitted to conduct reasonable grounds-based strip searches on arrest,[408] access to bodily samples generally requires prior judicial authorization under the *Criminal Code*.[409] However, the majority found that the swab was a valid exercise of the search incident to arrest power.[410] This determination was justified on the basis that the prohibition on obtaining DNA samples extended only to the accused's *own* DNA (and not the complainant's, which was the stated object of the search)[411] and that the loss or deterioration of that DNA evidence was a sufficiently pressing concern to justify the intrusion. The dissent in *Saeed* disputed the ability of law enforcement to "ask that individual to violate his or her own bodily integrity by collecting potentially self-incriminatory evidence from that most private of areas."[412] In this light, *Saeed* may signal a problematic willingness on the part of the Court to use the search incident to arrest power to compel individuals to participate in their own incrimination more generally, and in ways the law would not otherwise allow, even with a warrant. When viewed alongside *Fearon*, it is possible to imagine certain cases where law enforcement could attempt to justify the forced provision of a password by analogy to the facts in *Saeed*, particularly if the evidence in question is seen to "belong" to a victim or complainant and the preservation of evidence appears to be at issue.

However, such an interpretation would be problematic on several bases. First at least one Canadian court has rejected the idea that whether the particular mechanism used to lock a device is a fingerprint or passphrase should play a determinative role in setting out an individual's *Charter* rights.[413] In light of an individual's *Charter* rights to silence and against self-incrimination, the extremely high expectation of privacy inherent to personal electronic devices, and the need for rights-limiting powers of the state to be clearly prescribed by law, the ability of law enforcement to compel an individual to assist in decrypting a device following his or her arrest is not likely—with or without a warrant.[414] In addition, the majority in *Saeed* failed to consider the degree to which the principle against self-incrimination should inform the scope of protection offered by section 8 when an individual is given a choice between participating in his own incrimination or submitting to a forced penile swab conducted by an officer.[415] Courts assessing the protections allotted an individual compelled to provide her password on arrest will need to address this impact. Similarly, the Supreme Court has recognized that a more nuanced approach is required when considering section 8 protections in relation to data "belonging" to another but residing on the mobile device of a recipient accused of a crime.[416]

iii. Border Searches and Questioning

Compelled password disclosure and device searches raise unique legal considerations and operates differently in the cross-border context than in the course of ordinary criminal investigations. Despite lacking explicit legislative authority to do so,

---

[406] Tamir Israel (2014), "Supreme Court Gives Green Light to Searches of Mobile Devices on Arrest", *CIPPIC* (11 December 2014) <https://cippic.ca/news/SCC_gives_thumbs_up_to_mobile_device_searches_on_arrest>.

[407] *R v Saeed*, 2016 SCC 24.

[408] *R v Golden*, 2001 SCC 83.

[409] 487.05, 487.06 *Criminal Code* RSC 1985, c. C-46; *R v Saeed*, 2016 SCC 24 at para 148; *R v Stillman*, [1997] 1 SCR 607.

[410] *R v Saeed*, 2016 SCC 24.

[411] *Ibid* at paras 67-69.

[412] *Ibid* at para 152.

[413] See discussion at Box 5 of *Re: Impression Warrant Application (s.487.092)*, 2016 ONCJ 197.

[414] See *R c Boudreau-Fontaine*, 2010 QCCA 1108 and "Compelled Decryption and/or Key Disclosure."

[415] *R v Jones*, 2017 SCC 60 at paras 29-31.

[416] *R v Marakah*, 2017 SCC 59.

the Canadian Border Services Agency (CBSA) has requested device passwords from a number of individuals in recent years[417] and asserts that it has the legal authority to compel password disclosure when conducting a search—CBSA holds that it has this authority regardless of whether the password in question is biometric or stored only in the traveller's mind.[418] The most recent publicly available version of the CBSA's guidelines for electronic device searches, which was obtained by the British Columbia Civil Liberties Association in 2015, remained effective at least as of March 2017.[419]

The CBSA has consistently maintained that it is authorized to conduct searches of the data stored on digital devices (e.g., laptops, phones, and tablets) on the same legal basis it relies on to search other "goods" under the *Customs Act*.[420] While section 8 of the *Charter* protects individuals from unreasonable search and seizure, courts have held that individuals enjoy attenuated constitutional protections at the border. Travellers are routinely subject to suspicionless search and forced to answer questions upon leaving or entering a country—activities that would be considered serious constitutional infringements outside of the cross-border context. Additionally, Canadian courts have recognized that border control activities present a less stigmatizing context than policing activities conducted in the ordinary course of life. Having one's effects subjected to a search when crossing a border is viewed as routine and, hence, does not carry the same stigma as it would were one to be singled out for search while walking down the street.[421] Border control activities are therefore subject to far fewer safeguards in light of the reduced privacy that individuals can reasonably expect when seeking to enter or leave a country and the less stigmatizing context in which border control activities arise.[422]

However, the border is not a "*Charter*-free zone" and some restrictions do apply to the CBSA's border control activities. The CBSA is gien significant deference in cases where border searches are less intrusive and focused on achieving border control objectives clearly linked to customs and immigration. However, the *Charter* imposes progressively more rigorous safeguards as a search becomes more intrusive, and as the criminal jeopardy of the traveller becomes a live concern. In *R v. Simmons* the Supreme Court of Canada held that the more intrusive a border search becomes, "the greater must be the justification and the greater the degree of constitutional protection."[423] *Simmons* established a three-stage framework which is used to characterize the "type" of border search being conducted based on its progressive level of intrusiveness:

> "First is the routine of questioning which every traveller undergoes at a port of entry, accompanied in some cases by a search of baggage and perhaps a pat or frisk of outer clothing. No stigma is attached to being one of the thousands of travellers who are daily routinely checked in that manner upon entry to Canada and no constitutional issues are raised. It would be absurd to suggest that a person in such circumstances is detained in a constitutional sense and therefore entitled to be advised of his or her right to counsel. The second type of border search is the strip or skin search of the nature of that to which the present appellant was subjected, conducted in a private room, after a secondary examination and with the permission of a customs officer in authority. The third and most highly intrusive type of search is that sometimes referred to as the body cavity search, in which customs officers have recourse to medical doctors, to X−rays, to emetics, and to other highly invasive means."[424]

Under this framework, generalized and suspicionless searches can occur in the lower, less intrusive tier, but higher tier searches must be premised on reasonable grounds that they will produce evidence of a specific offence. The CBSA and the government have argued that searches of electronic devices fall into the non-intrusive lower categories of the *Simmons*

---

[417] See e.g., *Leslie v Canada (Public Safety and Emergency Preparedness)*, 2017 FC 119 at 12 and 21; *R v Sandhu*, 2016 BCPC 397 at 54; *Ward v Canada (Public Safety and Emergency Preparedness)*, 2014 FC 568 at 7 [in that case, an account password].

[418] Canadian Border Services Agency (2015), Operational Bulletin PRG-2015-31, "Examination of Digital Devices and Media at the Port of Entry - Interim Guidelines," (accessed through FOI by British Columbia Civil Liberties Association) <https://bccla.org/wp-content/uploads/2016/08/CBSA-FOI-Docs.pdf> at 5.

[419] *Ibid;* Matthew Braga (2017), "What happens when a Canadian border agent asks to search your phone?" (3 March 2017) *CBC* <http://www.cbc.ca/news/technology/border-phone-laptop-search-cbsa-canada-cbp-us-1.4002609>.

[420] See e.g., *R v Gibson,* 2017 BCPC 237; *R v Moroz*, 2012 ONSC 5642 at para 20.

[421] *R v Simmons*, [1988] 2 SCR 495 at para 27.

[422] *Ibid*; see also e.g., *R v Whittaker*, 2010 NBPC 32 at para 10, 2010.; *R v Moroz*, 2012 ONSC 5642 at paras 9-16.

[423] *R v Simmons*, [1988] 2 SCR 495 at para 28.

[424] *Ibid* at para 27.

framework, and are hence analogous to a "search of baggage and perhaps a pat or frisk of outer clothing"—a search they are permitted to conduct without a warrant or even particular suspicion.[425] The majority of lower court decisions have confirmed the CBSA's approach,[426] though a recent Manitoba decision has called this view into question.[427]

Yet the treatment of electronic device searches as non-invasive fails to take into account the intimate nature of information stored on electronic devices. These digital records are fundamentally different in both qualitative and quantitative terms than what can be stored in a briefcase, handbag, or car trunk. Additionally, the treatment of data stored on digital devices as analogous to other physical goods is inconsistent with a long line of Supreme Court decisions affirming the high expectation of privacy inherent in personal electronic devices and the highly invasive nature of digital searches. The Supreme Court has repeatedly stated that personal electronic devices cannot be treated by the law as simple "containers" full of information in law,[428] and in the case where encryption has transformed the data in question, the analogy is even more suspect.[429] Moreover, while a traveller's reasonable expectation of privacy at the border is diminished, it is by no means non-existent.[430]

The added dimension of compelled password disclosure in the cross-border context further complicates matters. At border crossings, individuals are regularly compelled to answer questions pertaining to border control matters. The Ontario Court of Appeal summarized this particular legal context in *R v. Jones* as follows:

> "No one entering Canada reasonably expects to be left alone by the state, or to have the right to choose whether to answer questions routinely asked of persons seeking entry to Canada....Travellers reasonably expect that they will be questioned at the border and will be expected to answer those questions truthfully. Put simply, the premise underlying the principle against self-incrimination, that is, that individuals are entitled to be left alone by the state absent cause being shown by the state, does not operate at the border....The state is expected and required to interfere with the personal autonomy and privacy of persons seeking entry to Canada. Persons seeking entry are expected to submit to and cooperate with that state intrusion in exchange for entry into Canada."[431]

Travellers have an explicit legislative obligation to truthfully answer questions posed by border officials under both the *Customs Act* and the *Immigration and Refugee Protection Act*.[432] The CBSA's 2015 policy asserts that the practice of charging non-compliant individuals for hindering (under 153.1 of the *Customs Act*) or obstruction (under 129(1)(d) of the *Immigration and Refugee Protection Act*) "appear[s] to be legally supported" from the agency's perspective.[433] The CBSA's position may be premised on the view that questions related to passwords and mandatory password disclosure are constitutionally permitted practices because the primary objective of such questions is to facilitate "border control" and not criminal investigation.

---

[425] *Ibid*; see also e.g., *R v Whittaker*, 2010 NBPC 32; *R v Moroz*, 2012 ONSC 5642; *R v Gibson*, 2017 BCPC 237.

[426] *R v Whittaker*, 2010 NBPC 32, 2010 at para 8 et seq; *R v Moroz*, 2012 ONSC 5642 at para 20; *R v Saikaley*, 2012 ONSC 6794 at para 70; *R v Leask*, 2008 ONCJ 25 (Ont. C.J.).

[427] See *Vaillancourt v Her Majesty et al*, 2017 MBQB 95 [as of this report's publication, this case appears to have been settled].

[428] *R v Vu*, 2013 3 SCR 657 at paras 45, 51; *R v Fearon*, 2014 3 SCR 621 at para 51; *R v Jones*, 2011 ONCA 632 at paras 47-49.

[429] See Lex Gill (2018), "Law, Metaphor, and the Encrypted Machine", forthcoming in the Osgoode Hall Law Journal, 55:2 (Spring 2018) on SSRN <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2933269> at 24-25:

> "....the container metaphor fails to represent the technical process of encrypting data. This is because ... encryption does not create a "barrier" between the outside world and the plaintext. There is no intelligible data hidden "inside" of an encrypted file or machine—rather, encryption renders data unintelligible, transformed and rearranged by a mathematical process. There can be no plaintext version of the data somehow enclosed within, because (to quote Gertrude Stein) there's no "there" there at all.
>
> … [the political metaphor of device-as-container] serves two dual functions: it obfuscates the testimonial aspect of disclosing a private key, and it rejects the notion that there is any qualitative difference in the kind or scope of information stored on digital devices compared to what might otherwise be physically stored or discovered."

[430] *R v Simmons*, [1988] 2 SCR 495; *R v Nagle*, 2012 BCCA 373.

[431] *R v Jones*, [2006] 81 OR (3d) 481 (ON CA) at para 30.

[432] *Customs Act*, RSC, 1985, c 1 (2nd Supp); *Immigration and Refugee Protection Act,* SC 2001, c 27.

[433] Canadian Border Services Agency (2015), Operational Bulletin PRG-2015-31, "Examination of Digital Devices and Media at the Port of Entry - Interim Guidelines," (accessed through FOI by British Columbia Civil Liberties Association) <https://bccla.org/wp-content/uploads/2016/08/CBSA-FOI-Docs.pdf> at 6.

It should be noted that an individual's right to silence and counsel are not engaged when border officials conduct routine searches for border control purposes, as these *Charter* rights are only engaged where an individual is "detained" in the criminal and constitutional law sense. Upon criminal detention at the border, this latitude ends and border agents must fully respect an individual's right to counsel and right to silence. The three-tiered *Simmons* framework provides a benchmark for determining the moment at which the shift from a regulatory to a criminal context occurs.[434] If electronic device searches were characterized under the more invasive "second" or "third" *Simmons* tiers (analogous to a strip search or cavity search), then a traveller would theoretically be able to rely on their right to counsel and right to silence in order to refuse decryption assistance to the CBSA.[435] By contrast, because electronic device searches have been characterized as generally falling into the "first" tier, and because first-tier *Simmons* searches do not constitute detention in the constitutional sense, a traveller may be unable to rely on her or her right to silence in order to avoid answering password-related questions.[436] At least one provincial court has found that being compelled to provide a password at this "less invasive" stage of an electronic device search does not engage the right against self-incrimination, despite the fact that the disclosure of a password resulted in direct criminal consequences for the traveller—and despite the fact that by the time the CBSA sought the password in that case, there was a clear possibility of criminal jeopardy.[437] The resulting status quo is extremely permissive—the CBSA believes it can search electronic devices and demand passwords in the absence of rigorous constitutional limitations.

The broad latitude afforded to border-motivated searches is not intended to operate as a general tool for facilitating ordinary law enforcement objectives. However, determining the point at which a search conducted for *Customs Act* purposes crosses over into the territory of a criminal detention (and thus triggers the individual's *Charter* rights) can be ambiguous in practice. The CBSA's 2015 policy cautions that the CBSA's officers "must be cognisant of where the regulatory examination crosses over to the realm of a criminal investigation" when conducting electronic device searches.[438] The guidelines further clarify that:

> "Examination of digital devices and media must **always** be performed with a clear nexus to administering or enforcing CBSA-mandated program legislation that governs the cross-border movement of people and goods, plants and animals. CBSA officers shall not examine digital devices and media with the sole or primary purpose of looking for evidence of a criminal offence under any Act of Parliament."[439]

In practice, this distinction is unhelpful, particularly where the search of electronic devices is concerned, as information on such devices is not neatly categorized into that which may be relevant for regulatory investigations into customs and immigration offences and that which is not.[440] This becomes even more complex where the CBSA conducts a search pursuant to a law enforcement "tip" made to the CBSA—that is, in situations where police lack the requisite grounds to conduct their own search but are aware an individual is about to travel. One lower court has held that despite this kind of direct connection to an ongoing criminal investigation (and by extension, clear criminal jeopardy to the individual) the resulting search of that individual's electronic device constituted a valid, first-level "routine" activity and thus implicated no additional constitutional protection for the accused.[441] Such decisions are constitutionally problematic because they let law enforcement evade the ordinary protections afforded to individuals under the *Charter* (e.g., the right to counsel) at the border, even where the alleged offence in question has no meaningful nexus to the border search context. While a nexus to a CBSA objective may persist, the pre-textual nature of the searches may irredeemably colour this objective, rendering the search inherently "criminal" in terms of the constitutional protections it attracts.[442] Moreover, to the extent that the CBSA maintains the position that it has the legal authority arrest and charge individuals for refusing to provide a password, such a threat might, at least in theory, constitute a "specific criminal

---

[434] *R v Simmons*, [1988] 2 SCR 495 at para 27.

[435] *Ibid* at para 35 et seq.

[436] *Ibid*; *R v Sekhon*, [2009] BCCA 187; *R v Nagle*, 2012 BCCA 373.

[437] *R v Buss*, 2014 BCPC 16.

[438] Canadian Border Services Agency (2015), Operational Bulletin PRG-2015-31, "Examination of Digital Devices and Media at the Port of Entry - Interim Guidelines," (accessed through FOI by British Columbia Civil Liberties Association) <https://bccla.org/wp-content/uploads/2016/08/CBSA-FOI-Docs.pdf> at 3-4.

[439] *Ibid* at 3-4 [original emphasis].

[440] In the criminal law context the Supreme Court has affirmed that searches are not "fishing expeditions." See *R v Mann*, 2004 SCC 52.

[441] *R v Moroz*, 2012 ONSC 5642.

[442] *R v Nolet*, 2010 SCC 24, para. 25; *R v Ladouceur*, 2002 SKCA 73.

jeopardy" sufficient on its own to trigger a state of detention (and consequently, the individual's *Charter* rights on detention, including that to silence and against self-incrimination).[443]

Though the 2015 CBSA policy states that the agency will take a "restrained approach" and shall not arrest a traveller on the basis of refusal to provide a password alone, their actual practice is less clear.[444] At least one traveller has been charged with obstruction of justice for refusing to provide a password to a personal electronic device, and in a 2017 Alberta Court of Queen's Bench decision, a senior CBSA official stated that individuals who refuse to disclose a password can be "subject to arrest."[445] Practically speaking it is important to note that even if the CBSA's interpretation of its authority to compel password disclosure is ultimately affirmed, there is simply no legal basis upon which to claim that a traveller has an actual obligation to *know* her or his password at the time of border crossing. However—and as with any refusal to disclose—failure to know a password may result in a more invasive search justified on the basis of heightened suspicion, seizure of the device in question, or other negative consequences for the traveller, including deportation in the case of non-citizens.

In sum, the appropriate standard for search of electronic devices (and the associated issues related to compelled password disclosure) at borders remain an emerging issue in Canadian law. While lower courts have generally taken a very permissive approach, current CBSA practice may not ultimately conform to the protections guaranteed by the *Charter*.

INFORMATION BOX 6: REQUESTS FOR PASSWORDS TO SOCIAL MEDIA AND OTHER NON-DEVICE PASSWORDS AT BORDERS?

The CBSA's 2015 policy for the search of electronic devices extends only to the data stored at rest on the traveller's device(s). The CBSA appears to be of the belief that it lacks the authority to access remote content or demand passwords for remotely stored data, including information on accounts (e.g., social media, etc.) accessible through the device being searched.[i] In addition to the fact that including remotely stored data would involve a radical stretch of the definition of "goods" under the *Customs Act,* there are practical reasons for this limitation (e.g., concerns about "remote wipe" features, which can remotely delete data from a device). It is nonetheless possible that there may be some situations where the CBSA could attempt to justify compelling password disclosure to data stored remotely—for example in an attempt to verify an individual's identity using a social media account in the immigration context.[ii]

[i] Canadian Border Services Agency (2015), Operational Bulletin PRG-2015-31, "Examination of Digital Devices and Media at the Port of Entry - Interim Guidelines," (accessed through FOI by British Columbia Civil Liberties Association) <https://bccla.org/wp-content/uploads/2016/08/CBSA-FOI-Docs.pdf> at 5:

> "Prior to examination of digital devices and media, and where possible, CBSA officers shall disable wireless and internet connectivity (i.e. set to airplane mode) to limit the ability of the device to connect to remote hosts or services. This will reduce the possibility of triggering remote wiping software; inadvertently accessing the Internet or other data stored externally; or changing version numbers or dates."

[ii] See s. 16(3) of the *Immigration and Refugee Protection Act* (S.C. 2001, c. 27):

> "(3) An officer may require or obtain from a permanent resident or a foreign national who is arrested, detained, subject to an examination or subject to a removal order, any evidence — photographic, fingerprint or otherwise — that may be used to establish their identity or compliance with this Act."

---

[443] *R v Buss*, 2014 BCPC 16.

[444] Canadian Border Services Agency (2015), Operational Bulletin PRG-2015-31, "Examination of Digital Devices and Media at the Port of Entry - Interim Guidelines," (accessed through FOI by British Columbia Civil Liberties Association) <https://bccla.org/wp-content/uploads/2016/08/CBSA-FOI-Docs.pdf> at 6.

[445] Jack Julian (2015), "Quebec resident Alain Philippon to fight charge for not giving up phone password at airport", *CBC News* (4 March 2015) <http://www.cbc.ca/news/canada/nova-scotia/quebec-resident-alain-philippon-to-fight-charge-for-not-giving-up-phone-password-at-airport-1.2982236>; Brett Ruskin (2016), "Alain Philippon pleads guilty over smartphone password border dispute", *CBC News* (15 August 2016) <http://www.cbc.ca/news/canada/nova-scotia/alain-philippon-to-plead-guilty-cellphone-1.3721110>; *R v Canfield*, 2017 ABQB 350 at para 44.

iv. Drawing Prejudicial Inferences from the Use of Encryption

Canadian courts have generally recognized that the constitutional rights of an accused person to silence and against self-incrimination bar both law enforcement and the courts from compelling assistance in the process of decrypting a device or file. However, in at least one case the fact that encryption was used to protect the accused's device (combined with the fact that the accused declined to provide a password) was found to give rise to a negative inference about the nature of the data stored thereon, contributing to the individual's conviction.[446] Such a finding is tantamount to an assertion that innocent individuals "have nothing to hide" and antithetical to the foundations of the criminal justice system, which is rooted in the presumption of innocence and which requires proof beyond a reasonable doubt in order to deprive an individual of his or her liberty.[447] The fact that information is either non-existent or unreadable due to the use of encryption technology cannot rationally form the basis for a prejudicial inference or a finding of guilt.[448] The Supreme Court has also recognized that the mere exercise of one's rights cannot provide a basis for reasonable suspicion.[449] It is neither logical (nor is it likely to be constitutionally permissible) to draw negative inferences solely from the fact that communications records or data stored on a device is encrypted. Where forensic analysis or exploitation techniques conducted by law enforcement later yield evidence of additional criminal acts, there is no bar to laying further charges against the accused.[450]

Taken to extremes, narratives which draw false parallels between the use of encryption and criminality or terrorism have been used by authoritarian governments as a basis to imprison human rights defenders in a number of high-profile cases.[451] This kind of presumption becomes even more tenuous as many storage and communication services now implement some form of encryption (including end-to-end encryption) by default. There are myriad economic, political, and safety reasons for individuals to protect their data using encryption tools, and countless reasons—including market demand, technical innovation, and respect for human rights—for technology companies to develop products that encrypt user data effectively.

Courts must also consider these myriad reasons when faced with a question of whether to hold the developers of encryption technology responsible for the alleged behaviour of their users (or some subset thereof). In early 2018, the U.S. Department of Justice (operating with support from the Australian Federal Police and the RCMP) indicted the Chief Executive Officer of a Canadian company called Phantom Secure and four associates "on charges that they knowingly and intentionally participated in a criminal enterprise that facilitated the transnational importation and distribution of narcotics through the sale

---

[446] See e.g. the reference to "use of encrypted phones" to impute suspicion in *R v Gosk*, 2016 ONSC 2185 at para 10; testimony from law enforcement associating the use of encryption with suspicious behaviour in *R v Cyr*, 2014 ABQB 214 at para 114: "he had only seen this level of encryption on devices for government, military and criminal organization members."

[447] Notably, the federal government has recently proposed legislation modifying a number of offences under the *Criminal Code* to remove the possibility for these kinds of evidentiary shortcuts.

See Department of Justice (2017), "Charter Statement - *Bill C-51: An Act to amend the Criminal Code and the Department of Justice Act and to make consequential amendments to another Act*," (Tabled in the House of Commons, 6 June 2017) <http://www.justice.gc.ca/eng/csj-sjc/pl/charter-charte/c51.html>:

> "These presumptions are statutory "short-cuts" that allow the Crown's proof of one fact to be taken as, or "presumed" to be, proof of another fact that is required to make out the offence, unless the presumption is rebutted by the accused. Court decisions have concluded that some presumptions have the capacity to unjustifiably limit section 11(d) rights since they relieve the Crown of proving certain elements of an offence beyond a reasonable doubt, and so infringe the presumption of innocence."

[448] See *R v Singh*, 2014 MBPC 52 at para 130:

> "The Crown suggesting that the lack of information or further detection was because of the use of encrypted phones is nothing but speculation and cannot be relied upon by the court."

[449] See e.g., *R v Chehil*, 2013 SCC 49 at para 44; *R v Noble*, [1997] 1 SCR 874 at 72.

[450] See e.g., *R v Gryba*, 2015 SKQB 372; *R v Burke*, 2015 SKPC 173 at para 17.

[451] See e.g., Danny O'Brien (2015), "The Zone 9 Bloggers are Free: but Ethiopia Still Thinks Digital Security is Terrorism", *Electronic Frontier Foundation* (26 October 2015) <https://www.eff.org/deeplinks/2015/10/zone-9-bloggers-are-free-ethiopia-still-thinks-encryption-terrorism>; Amnesty International (2017), "Director of Amnesty International Turkey must be released from incommunicado detention" (6 July 2017) <https://www.amnesty.org/en/latest/news/2017/07/director-of-amnesty-international-turkey-must-be-released-from-incommunicado-detention/>; Nil Köksal (2018), "'Terrifying': How a Single Line of Computer Code Put Thousands of Innocent Turks in Jail", *CBC News* (22 January 2018) <http://www.cbc.ca/news/world/terrifying-how-a-single-line-of-computer-code-put-thousands-of-innocent-turks-in-jail-1.4495021>; David Kaye, 2017, Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression on His Mission to Turkey, A/HRC/35/22/Add3,(21 June 2017) <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G17/170/40/PDF/G1717040.pdf?OpenElement> at para 54 (tens of thousands of individuals in Turkey have been dismissed or arrested due to their use of encrypted messaging application ByLock, which the government claims is linked with the Gülenist movement).

and service of encrypted communications."[452] This is the first time the U.S. government has targeted a private company in this manner. An overbroad ruling in this case could have significant consequences for developers of secure communications technology because it raises the spectre of liability for those providing secure technologies which simply happen to be used by those who have committed a criminal offence.[453] This may have a chilling effect on the development of secure technology (especially by smaller companies) on the basis that such features may make them attractive to parties under government investigation.

v. Other forms of Mandatory Disclosure by Targeted Individuals

In this section, we note two residual circumstances in which an individual may be compelled to provide a password or access to the plaintext stored on an otherwise encrypted device. The first is where the obligation is imposed as a condition imposed on an individual at bail or upon sentencing. The second is where mandatory decryption or key disclosure forms part of a valid civil order for the preservation of evidence, generally referred to as an "Anton Piller order."

a) Conditions on Bail and Sentencing

In some cases, individuals may be required by a court to provide passwords to devices and accounts as a condition of bail, sentencing, or in relation to a recognizance or terrorism peace bond. For example, in a recent Ontario case, an individual was required to provide his probation officer "with any encryption codes and/or encryption passwords necessary to permit the random inspection of any electronic device(s) for the purpose of monitoring his compliance with the provisions of this order."[454] While such measures have the capacity to be highly privacy-invasive, they are beyond the scope of this report on the basis that they raise different constitutional and policy concerns.

b) Civil Orders for the Preservation of Evidence

In the context of civil litigation, an individual or corporate party may, under certain exceptional conditions, seek an *ex parte* order for the seizure and safekeeping of evidence (including evidence stored on the defendant's networks and digital devices) under certain exceptional conditions. This form of extraordinary relief, which is often called an Anton Piller order, is meant to preserve evidence, as opposed to serving the purposes of ordinary discovery. Given its inherently invasive nature, such orders have been described as one of the two "nuclear weapons" of civil law.[455] In 2006, the Supreme Court of Canada established a stringent set of safeguards for their use in *Celanese*.[456]

Such orders must be distinguished from the context of criminal law search and seizure. A draft model Anton Piller order (provided as a template from the Ontario Courts) includes mandatory key disclosure and decryption obligations:

---

[452] United States Department of Justice (2018), "Chief Executive and Four Associates Indicted for Conspiring with Global Drug Traffickers by Providing Encryption Services to Evade Law Enforcement and Obstruct Justice", Press Release (15 March 2018) <https://www.justice.gov/opa/pr/chief-executive-and-four-associates-indicted-conspiring-global-drug-traffickers-providing>; The Canadian Press (2018), "Canadian CEO charged with conspiring to sell unhackable phones to criminals", *The Globe and Mail* (16 March 2018) <https://www.theglobeandmail.com/report-on-business/canadian-ceo-charged-with-conspiring-to-sell-unhackable-phones-to-criminals/article38295061/?click=sf_globefb>; United States Federal Bureau of Investigation (2018), "International Criminal Communication Service Dismantled", (16 March 2018) <https://www.fbi.gov/news/stories/phantom-secure-takedown-031618>.

[453] Note however that the issue of *intent* is (at least in theory) critical in the Phantom Secure case:

> "The indictment that dropped on March 15 does not claim that it is a crime simply to provide encrypted communication services or the like, even where those services may result in communications being immune as a practical matter from government access pursuant to warrants or other process. But it is a crime, the Justice Department asserts, to use such services knowingly and intentionally to enable and facilitate the commission of other crimes (like narcotics trafficking). Simply put, the Justice Department takes the position that a secure-communications provider can become part of a criminal conspiracy or racketeering enterprise, if the requisite intent is there."

See Robert Chesney (2018), "Illegal Secrecy? The Prosecution of Phantom Secure and Its Implications for the Going Dark Debate", *Lawfare* (20 March 2018) <https://www.lawfareblog.com/illegal-secrecy-prosecution-phantom-secure-and-its-implications-going-dark-debate>.

[454] *R v Bools*, 2015 ONSC 2869 at para 55 ("Condition 12").

[455] *Bank Mellat v Nikpour,* [1985] FSR 87.

[456] *Canadian Bearings Ltd. et al. v Celanese Canada Inc. et al.*, 2006 SCC 36.

> "... shall forthwith render any necessary assistance to the Authorized Persons to locate, decode, access, and decrypt the Evidence and any and all information or electronic data to which the Authorized Persons may not have ready and immediate access, including the provision of all keys, identification codes, passwords, passphrases, or any other such information or knowledge necessary to achieve access thereto."[457]

Individuals do not have the same rights in private litigation as they do where their liberty or other *Charter*-protected interests are at stake in the criminal law context. However, even in the absence of criminal jeopardy there may still be important *Charter*-values and other important interests at play in civil litigation.[458] The possibility that using this "nuclear option" to secure evidence in a civil proceeding could reveal information relevant to a later criminal investigation raises complex issues about the use of evidence obtained in civil proceedings and the protection of *Charter* rights in a private law context. Though a detailed discussion of this issue is beyond the scope of this report, the Supreme Court of Canada has recognized that pre-trial discovery records are generally protected from disclosure to law enforcement,[459] and that the use of prior discovery evidence which is incriminating triggers the application of s. 13 of the *Charter*.[460]

D. CONCLUSION

As outlined in this section, state agencies have proposed dozens of measures to address the perceived investigative or intelligence challenges attributed to encryption. All of these proposed measures entail substantial negative tradeoffs for human rights, public safety, national security, the economy and consumer safety. Some proposals attempt to undermine encryption at its technical core, at a time when security of information systems has never been more important. Other measures result in substantial negative implications for privacy, free expression and other fundamental rights and freedoms. While most of these measures are inherently undesirable, the following section questions whether solutions to the encryption "problem" are necessary in the first place. The state already has access to many tools that permit it to access encrypted data, and there has been no suggestion that it will abandon these investigative techniques if new measures are adopted. Moreover, the breadth of data available to the state in its various investigative and intelligence-gathering functions today is already profound. It is simply not clear that the drastic costs associated with the anti-encryption measures outlined in this section can be justified in a free and democratic society.

---

[457] Commercial List Users' Committee of the Ontario Superior Court of Justice (2017), "Model Anton Piller Form", <www.ontariocourts.ca/scj/files/forms/com/anton-piller-order-EN.doc> at para 16 (footnote 27); see also British Columbia Courts Anton Piller Working Group (2017), "Draft Model Order for the Seizure and Safekeeping of Evidence", <http://www.courts.gov.bc.ca/supreme_court/practice_and_procedure/practice_directions/civil/PD%20-%2031%20Model%20Order%20-%20Seizure%20%20Safekeeping%20of%20Evidence%20(explanatory%20notes).pdf> at 11.

[458] The potential for abuse and overreach is precisely why the Supreme Court has set out clear safeguards for such orders in *Canadian Bearings Ltd. et al. v. Celanese Canada Inc. et al.*, 2006 SCC 36.

[459] *Juman v. Doucette*, 2008 SCC 8.

[460] *R. v. Nedelcu*, 2012 SCC 59.

PART 5: ENCRYPTION IS NOT AN INSURMOUNTABLE BARRIER

There are alternative responses to the encryption "problem" that do not involve the same kinds of system-wide costs to security, privacy, or constitutionally-protected rights as those discussed at length in Part 4. In this section, we make two core arguments to support this claim.

The first is that while strong encryption works, all security systems are imperfect in practice. Vulnerabilities in networks, devices, and human behaviour can all be exploited to circumvent the otherwise strong protection provided by encryption technology. Generally, this can be done in a targeted manner that does not cause unreasonable interference with the constitutionally protected rights of individuals and that does not create new vulnerabilities or complexities that are exploitable by all. Encryption may increase the expertise, cost, or ingenuity required in the course of a successful investigation but it is rarely a source of investigative impossibility. Instead, encryption is better understood as a source of investigative *friction.*

The second is that the state is not running out of data. The "going dark" narrative advanced by law enforcement and intelligence agencies may represent a real fear, but it does not appear to represent an empirical reality. The types of evidence and intelligence leveraged by state agencies are greater in kind, scope, scale, and availability than ever before in history, and only a small fraction of that data is protected by encryption. The vast majority can be collected and exploited without systematically undermining the technological infrastructure upon which the general public relies. Canadian state agencies already have extraordinary powers that allow them to collect, analyze, and exploit this new information.

INFORMATION BOX 7: LAW ENFORCEMENT AND INTELLIGENCE: DIFFERENT CAPABILITIES AND DIFFERENT OBJECTIVES

While law enforcement agencies and intelligence bodies have many overlapping concerns and objectives, the issues they face are not identical. Law enforcement generally tend to be more concerned with the ability to access evidence on devices stored at rest (such as on a seized laptop or phone), whereas intelligence agencies are more preoccupied with the issue of encrypted data in transit. This is because in the course of gathering intelligence, signals intelligence agencies like the NSA and the CSE systematically engage in the bulk collection of communications-related data as it travels across networks, whereas the privacy-invasive search and seizure powers of law enforcement are generally limited to specific investigations and justified on the basis of specific grounds. Unlike intelligence agencies, law enforcement agencies are constrained by the fact that in order for the information they gather to be useful (and contribute to a conviction), it must be legally admissible in a court of law, and will be subject to stringent disclosure obligations in that context.[i]

In the course of an electronic investigation, it is also important to understand that law enforcement will rarely have access to the kind of technological sophistication, expertise, or resources available to a signals intelligence agency like the CSE. Given these constraints, while certain kinds of searches, interceptions, attacks or intrusions may be technically *possible*, they may not always be realistic or practical to pursue. Intelligence agencies—both because they are not limited by these kinds of evidentiary concerns, and because they have greater access to technical expertise—are able to engage in much more intrusive activities, and are more readily able to overcome the protections afforded by encryption. In some cases however, law enforcement may seek the support of the CSE under the "technical assistance" aspect of the Establishment's mandate.[ii]

[i] To understand the complex issues that arise where information "crosses over" between these two sets of actors, see: Craig Forcese (2018), "Intelligence Swords and Shields in Canadian Law", Speaking Notes (February 2018) <http://craigforcese.squarespace.com/national-security-law-blog/> [on the *evidentiary-intelligence* problem]; see also Human Rights Watch (2018), "Dark Side: Secret Origins of Evidence in US Criminal Cases" (9 January 2018) <https://www.hrw.org/report/2018/01/09/dark-side/secret-origins-evidence-us-criminal-cases> [on parallel construction in the U.S. context].

[ii] s. 273.64 (1)(c), National Defence Act, RSC 1985, c N-5 or the proposed s. 21 of the *Communications Security Establishment Act* in Bill C-59 (*An Act respecting national security matters*), First Reading; Christopher Parsons, Lex Gill, Tamir Israel, Bill Robinson, and Ronald Deibert (2017), "Analysis of the Communications Security Establishment Act and Related Provisions in Bill C-59 (An Act respecting national security matters), First Reading", The Citizen Lab and the Canadian Internet Policy and Public Interest Clinic (18 December 2017) <https://citizenlab.ca/wp-content/uploads/2018/01/C-59-Analysis-1.0.pdf> at 32 et seq.

A. REFRAMING ENCRYPTION AS INVESTIGATIVE FRICTION

Encryption is not a foolproof solution for individuals seeking to protect the security or confidentiality of data. Even where encryption poses a technical barrier, vulnerabilities in networks, physical devices, and flawed human behaviour all create opportunities for state actors to circumvent protective measures and acquire information. As a result, encryption is better understood as a technology which creates investigative friction rather than impossibility. It forces government agencies (whether engaged in law enforcement or intelligence collection activities) to exercise more targeted attention, use better analytical tools, and deploy resources more strategically to acquire data. In some cases, encryption will undoubtedly increase the cost and difficulty of lawful efforts to gather evidence and intelligence. However, it may also provide an incentive for state agents to ensure that intrusive activities are tailored, targeted, and directed towards the most pressing and serious government objectives.

Accessing otherwise encrypted data may sometimes require using sophisticated technical tools or resource-intensive operations, the likes of which are usually only available to state-level actors. Such was the case for Ahmed Mansoor, an internationally recognized human rights defender targeted using a chain of iPhone zero-day exploits and dubbed "the million dollar dissident" in a series of Citizen Lab reports.[461] In other cases, rudimentary technical tools for endpoint hacking, the use of covert human intelligence, and commonplace social engineering techniques are sufficient to undermine protections offered by encryption and to reveal the contents of encrypted communications to adversaries.[462] As described in a joint statement issued by ENISA and Europol:

> "The focus should be on getting access to the communication or information; not on breaking the protection mechanism. The good news is that the information needs to be unencrypted at some point to be useful to the criminals. This creates opportunities for alternatives such as undercover operations, infiltration into criminal groups, and getting access to the communication devices beyond the point of encryption, for instance by means of live forensics on seized devices or by lawful interception on those devices while still used by suspects."[463]

Beyond compelled key disclosure (discussed at length in Part 4), Orin Kerr and Bruce Schneier identify five additional categories of "encryption workaround," which they describe as "find the key, guess the key … exploit a flaw in the encryption software, access plaintext while the device is in use, [or] locate another plaintext copy.[464] For example, a password may be revealed through closed-circuit television (CCTV) camera surveillance of a targeted individual, volunteered by a target to an undercover agent, acquired through a phishing attack, or captured by surreptitiously installed keylogging software. The use of social engineering techniques, covert human intelligence sources, and careful observation may often be more effective than a complex or costly technical solution. In a 2016 Canadian case, law enforcement circumvented the presence of full disk encryption by using a password found on a sticky note.[465] Of course, even highly secure tools will invariably have vulnerabilities—for example, it is possible that weaknesses in group chat protocols in tools like Signal, Whatsapp, and Threema could be exploited to undermine communications integrity.[466] Law enforcement are also finding novel ways to circumvent fingerprint-based security mechanisms on mobile devices, from unlocking devices with the fingers of deceased individuals to reconstructing a suspect's

---

[461] Bill Marczak and John Scott-Railton (2016), "The Million Dollar Dissident: NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender", (24 August 2016) The Citizen Lab <https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae>.

[462] There are many case studies exploring the ways such attacks are used to target and undermine civil society.

See e.g., Masashi Crete-Nishihata, Jakub Dalek, Etienne Maynier, and John Scott-Railton (2018), "Spying on a Budget: Inside a Phishing Operation with Targets in the Tibetan Community," The Citizen Lab (30 January 2018) <https://citizenlab.ca/2018/01/spying-on-a-budget-inside-a-phishing-operation-with-targets-in-the-tibetan-community/>; Citizen Lab, "Communities @ Risk: Targeted Digital Threats Against Civil Society," (2014) The Citizen Lab, Munk School of Global Affairs <https://targetedthreats.net/>; Seth Hardy, Masashi Crete-Nishihata, Katharine Kleemola, Adam Senft, Byron Sonne, Greg Wiseman, Phillipa Gill, Ronald J. Deibert (2014), "Targeted Threat Index: Characterizing and Quantifying Politically-Motivated Targeted Malware," 23rd USENIX Security Symposium (August 20–22, 2014), San Diego, CA <https://www.usenix.org/system/files/conference/usenixsecurity14/sec14-paper-hardy.pdf>.

[463] Europol and ENISA (2016), "Joint Statement on lawful criminal investigation that respects 21st century data protection," (20 May 2016) <https://www.europol.europa.eu/publications-documents/lawful-criminal-investigation-respects-21st-century-data-protection-europol-and-enisa-joint-statement-0> at 1.

[464] Orin S. Kerr and Bruce Schneier (2018), "Encryption Workarounds," 106 Georgetown LJ 989 on SSRN (first posted 22 March 2017) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2938033> at 991.

[465] *R v Nero*, 2016 ONCA 160 at para 153.

[466] Paul Rösler, Christian Mainka, Jörg Schwenk (2017), "More is Less: How Group Chats Weaken the Security of Instant Messengers Signal, WhatsApp, and Threema," Cryptology ePrint Archive, International Association for Cryptologic Research (July 2017) <https://eprint.iacr.org/2017/713.pdf>.

prints from photographs.[467] There have also been cases where laptops and mobile devices have simply been grabbed (often in public places) by law enforcement in capture-the-flag style operations, with agents seizing the target's device before he or she could re-encrypt its contents.[468] Many of these techniques raise independent *Charter* and human rights concerns.

Figure 5: Little Bobby on End Point Security[469]

Targeted endpoint hacking is a tool that is employed by law enforcement and intelligence agencies alike. As of 2018, some law enforcement agencies are developing and formalizing programs for employing these types of exploits as a means of ensuring ongoing access to encrypted communications, data, and devices. For example, the FBI's "Cryptographic and Electronic Analysis Unit" and "Remote Operations Unit" have developed extensive experience in exploiting devices to bypass encryption and maintain ongoing contacts with external exploit vendors.[470] Numerous other policing agencies in the United States have also reportedly acquired low-cost capabilities and portable capabilities allowing them to bypass encryption on many iPhone devices.[471] Hacking Team, a third party exploit vendor based in Milan, has reportedly sold exploits to intelligence and law enforcement agencies in dozens of countries around the world, including those with problematic human rights records.[472] Such measures are inherently intrusive and are likely to be particularly problematic whenever deployed remotely, including for reasons

---

[467] Thomas Fox-Brwster (2018), "Yes, Cops Are Now Opening iPhones With Dead People's Fingerprints", *Forbes* (22 March 2018) <https://www.forbes.com/sites/thomasbrewster/2018/03/22/yes-cops-are-now-opening-iphones-with-dead-peoples-fingerprints/#20038ea9393e>; See Marc Rogers (2013), "Why I Hacked Apple's TouchID, And Still Think It Is Awesome", *Lookout Security* (23 September 2013) <https://blog.lookout.com/why-i-hacked-apples-touchid-and-still-think-it-is-awesome>.

[468] The most famous case using this tactic is likely that of Ross Ulbricht, creator of the online marketplace Silk Road.

See Natasha Bertrand (2015), "The FBI staged a lovers' fight to catch the kingpin of the web's biggest illegal drug marketplace", *Business Insider* (29 May 2015) <http://www.businessinsider.com/ross-ulbricht-will-be-sentenced-soon--heres-how-he-was-arrested-2015-5>; Andy Greenberg (2015), "Undercover Agent Reveals How He Helped the FBI Trap Silk Road's Ross Ulbricht," *Wired* (14 January 2015) <https://www.wired.com/2015/01/silk-road-trial-undercover-dhs-fbi-trap-ross-ulbricht/>:

> "As part of a coordinated law enforcement effort designed to prove that Ulbricht was the Dread Pirate Roberts and to seize his laptop before he could encrypt its hard drive. ….. The plan for the arrest...was to get him into a position where we could have him in a public setting, and I could initiate a chat with him," Deryeghiayan said in response to questions from prosecutor Serrin Turner. "The purpose was that if indeed [the Dread Pirate Roberts] was Ross Ulbricht, we could get his computer in an open, unencrypted state."

[469] Robert M Lee and Jeff Haas, "A Sunday Morning Web Comic on Technology and Security", *Little Bobby,* Week 128 (9 July 2017) <http://www.littlebobbycomic.com/projects/week-128/>.

[470] United States Department of Justice (2018), Office of the Inspector General, "A Special Inquiry Regarding the Accuracy of FBI Statements Concerning its Capabilities to Exploit an iPhone Seized During the San Bernardino Terror Attack Investigation", Office of the Inspector General (March 2018) <https://oig.justice.gov/reports/2018/o1803.pdf> at 2-3.

[471] Joseph Cox (2018), "Cops Around the Country Can Now Unlock iPhones, Records Show", *Motherboard* (12 April 2018) <https://motherboard.vice.com/en_us/article/vbxxxd/unlock-iphone-ios11-graykey-grayshift-police>.

[472] Mattathias Schwartz (2017), "Cyberwar for Sale", *New York Times* (4 January 2017) <https://www.nytimes.com/2017/01/04/magazine/cyberwar-for-sale.html?smi=%20d=3Dtw-share&_r=1&mtrref=undefined>; See also: Bill Marczak, Claudio Guarnieri, Morgan Marquis-Boire, and John Scott-Railton (2014), "Hacking Team and the Targeting of Ethiopian Journalists", The Citizen Lab (12 February 2014) <https://citizenlab.ca/2014/02/hacking-team-targeting-ethiopian-journalists/>; *Ibid* (2014), "Mapping Hacking Team's "Untraceable" Spyware", The Citizen Lab (17 February 2014) <https://citizenlab.ca/2014/02/mapping-hacking-teams-untraceable-spyware/>; Bill Marczak, Claudio Guarnieri, Morgan Marquis-Boire, John Scott-Railton, and Sarah McKune (2014), "Hacking Team's US Nexus", The Citizen Lab (28 February 2014) <https://citizenlab.ca/2014/02/hacking-teams-us-nexus/>.

of jurisdictional overreach.[473] Depending on the technical measure adopted, hacking activities may result in collateral harm to the security and privacy interests of non-targeted individuals. Certain kinds of techniques may also have a deleterious impact on public trust in consumer technologies and have potentially far-reaching and difficult to anticipate implications for the global security ecosystem.[474] There also are critical issues of proportionality at play, especially when law enforcement activities are conducted with the assistance of sophisticated actors like the CSE or private companies specializing in the sale and use of exploit technology.[475] Recent developments in foreign jurisdictions, perhaps most notably in Germany, have favoured creating legal frameworks for targeted hacking in lieu of measures that would weaken encryption for the public at large.[476] Yet the German example demonstrates that reliance on such powers remains controversial even when measures like prior judicial authorization, skilled technical oversight, transparency reporting, and a coherent framework for ensuring that such activities operate as a "last resort" are in place.[477] Finally, individualized end-point hacking must be carefully and explicitly differentiated from larger scale attacks on communications networks, which will inherently involve collateral harm to non-targeted users, data, and networks. The "cyber operation" powers proposed in Bill C-59 (*National Security Act 2017*) for the CSE (and similar activities leveraged in the course of the CSE's foreign intelligence mandate) raise precisely these types of concerns.[478]

At the time of publication, it remains unclear how often Canadian law enforcement use endpoint hacking techniques in the course of investigations because there are no legislated transparency or reporting requirements of the type employed for other privacy-intrusive measures (such as wiretapping) for these activities.[479] However, court records do indicate that the RCMP and other Canadian police forces engage in forensic analysis and targeted attacks on both devices and accounts in order to

---

[473] See Amie Stepanovich (2016), Testimony Re Matter of Proposed Amendments to the Federal Rules of Criminal Procedure, Rule 41, Advisory Committee on Criminal Rules, Access Now & Electronic Frontier Foundation (28 April 2016) <https://www.accessnow.org/cms/assets/uploads/archive/docs/Rule41botnettestimony.pdf>; Rainey Reitman (2016), "With Rule 41, Little-Known Committee Proposes to Grant New Hacking Powers to the Government", Electronic Frontiers Foundation (30 April 2016) <https://www.eff.org/deeplinks/2016/04/rule-41-little-known-committee-proposes-grant-new-hacking-powers-government>; Center for Democracy & Technology (2014), Written Statement In Re Matter of Proposed Amendments to the Federal Rules of Criminal Procedure, Rule 41, Advisory Committee on Criminal Rules, Center for Democracy & Technology (24 October 2014) <https://cdt.org/files/2014/10/CDT-Rule41-Written-Statement-final-20141024.pdf>.

[474] Measures that require service providers to engineer or sign malicious software updates designed to compromise user security is one such example—a request at issue in the *Apple v FBI* dispute.

See e.g., Tom Simonite (2016), "How Apple Could Fed-Proof Its Software Update System", *MIT Technology Review* (11 March 2016) <https://www.technologyreview.com/s/601007/how-apple-could-fed-proof-its-software-update-system/>; Christopher Soghoian (2016), "The technology at the heart of the Apple-FBI debate, explained", *The Washington Post* (29 February 2016) <https://www.washingtonpost.com/news/the-switch/wp/2016/02/29/the-technology-at-the-heart-of-the-apple-fbi-debate-explained/>.

> "If consumers fear that the software updates they receive from technology companies might secretly contain surveillance software from the FBI, many of them are likely to disable those automatic updates. And even if you aren't worried about the FBI spying on you, if enough other people are, you will still face increased threats from hackers, identity thieves and foreign governments.
>
> There are a lot of parallels between computer security and public health, and in many ways, software updates are like immunizations for our computers. Just as we want parents to get their children immunized, we want computers to receive regular software updates. Indeed, just as the decision by some parents to not vaccinate their children puts their entire community at risk, so too the decision to turn off automatic updates not only impacts the individual, but other users and organizations, as those vulnerable, infected users' computers will be used by hackers to target others."

[475] See Christopher Parsons, Lex Gill, Tamir Israel, Bill Robinson, and Ronald Deibert (2017), "Analysis of the Communications Security Establishment Act and Related Provisions in Bill C-59 (An Act respecting national security matters), First Reading", The Citizen Lab and the Canadian Internet Policy and Public Interest Clinic (18 December 2017) <https://citizenlab.ca/wp-content/uploads/2018/01/C-59-Analysis-1.0.pdf> at 32 et seq.; s. 273.64 (1)(c), *National Defence Act*, RSC 1985, c N-5; Proposed s. 21 of the *Communications Security Establishment Act* in Bill C-59 (*An Act respecting national security matters*), First Reading.

There are many private companies in the business of providing hacking services to governments and other actors. In the *FBI v Apple* dispute, the FBI ultimately paid a firm to find and exploit a previously unknown security flaw in the device.

See Ellen Nakashima (2016), "FBI paid professional hackers one-time fee to crack San Bernardino iPhone", *The Washington Post* (12 April 2016) <https://www.washingtonpost.com/world/national-security/fbi-paid-professional-hackers-one-time-fee-to-crack-san-bernardino-iphone/2016/04/12/5397814a-00de-11e6-9d36-33d198ea26c5_story.html>.

[476] Sven Herpig, Stefan Heumann (2017), "Germany's Crypto Past and Hacking Future", *Lawfare* (13 April 2017) <https://www.lawfareblog.com/germanys-crypto-past-and-hacking-future>; Matthew Hughes (2017), "Germany's police don't need backdoors because they can hack your phone anyway", *The Next Web* (28 July 2017) <https://thenextweb.com/insider/2017/07/28/germanys-police-dont-need-backdoors-because-they-can-hack-your-phone-anyway/>.

[477] See also: Access Now (2018), "Encryption in the US: Crypto Colloquium Outcomes Report", *Access Now* (January 2018) <https://www.accessnow.org/cms/assets/uploads/2018/02/Encryption-in-the-United-States-Crypto-Colloquium-Outcomes-Report.pdf>; Privacy International (2018), "Hacking Safeguards and Legal Commentary" (11 January 2018) <https://www.privacyinternational.org/advocacy-briefing/1057/hacking-safeguards-and-legal-commentary>.

[478] Christopher Parsons, Lex Gill, Tamir Israel, Bill Robinson, and Ronald Deibert (2017), "Analysis of the Communications Security Establishment Act and Related Provisions in Bill C-59 (An Act respecting national security matters), First Reading", The Citizen Lab and the Canadian Internet Policy and Public Interest Clinic (18 December 2017) <https://citizenlab.ca/wp-content/uploads/2018/01/C-59-Analysis-1.0.pdf> at 27 et. seq. [For Canadian context]; Privacy International (2017), "Government Hacking and Surveillance: 10 Necessary Safeguards", (15 December 2017) <https://privacyinternational.org/node/957> [for international context].

[479] See Part VI, *Criminal Code,* RSC 1985, c C-46.

circumvent encryption,[480] and courts have acknowledged that "the use of encryption … makes it hard, but not impossible" for police to intercept encrypted messages.[481] Depending on the nature of the exploit, such activities are presumably authorized pursuant to the general warrant provisions in section 487.01(1), the assistance order provisions in section 487.02 of the *Criminal Code,* the interception of private communications powers in section 183, or, potentially, as corollaries to regular search warrants.[482] Some cases could involve the assistance of the CSE under the technical and operational assistance aspect of its mandate,[483] or may involve the purchase of offensive technical tools and services from private companies. Indeed, leaked documents from such a private vendor (Italian-based Hacking Team) confirm that several Canadian police agencies expressed interest in acquiring such services, although it has not been confirmed whether any ultimately acquired them.[484] It is also possible that intelligence agencies secure access to otherwise encrypted data by finding account and device credentials through more questionable means—whether because they have been revealed through a data breach conducted by a malicious actor and published online, through strategic targeting of system administrators, or acquired through an illicit third party.[485] Following the Supreme Court's decision in *R. v. Marakah*, the possibility of acquiring otherwise protected data through a co-accused person, witness, or other communications partner without a warrant appears to have been foreclosed.[486]

It is important to recognize that a number of the activities we have described in this section are considered *prima facie* illegal in Canada. While in some investigative contexts it is possible that they may constitute an appropriate limit on an individual's *Charter* rights this will not always be the case, and they may nonetheless have the potential to deeply invade individuals' privacy, security, safety and dignity. However, the reality is that such techniques remain available to law enforcement and intelligence agencies alike, and constitute components of their respective toolkits. The result is that even where data is encrypted in ways that are generally secure there will often be a way for a motivated actor to access it.

B. THE STATE IS NOT RUNNING OUT OF DATA

The fact that encryption might render some data inaccessible to state agencies in some contexts does not, in and of itself, establish an insurmountable investigative or evidentiary barrier. Far from "going dark," more information is available about individuals' private lives today than in any other moment in human history—a trend that has led some academics to argue that even alongside the emergence of strong commercial encryption, we now live in a "golden age of surveillance."[487] Law enforcement and intelligence agencies enjoy access to vast amounts of personal information. They are also likely to maintain or increase that access for the foreseeable future, for at least three reasons.

First, the sheer volume of data generated and recorded as a byproduct of our digital lives continues to grow, which means that the overall volume of data available to the state is unlikely to diminish. Second, there are often practical upper limits to how much data can or is likely to be obscured by encryption, largely because there are business incentives for some companies to design communications tools in a manner that maintains plaintext access. For example, by having greater access to users' private

---

[480] See e.g., *R v Tsekouras*, 2015 ONSC 1470 at paras 10-11 [discussion of BlackBerry encryption].

[481] *R v Williams*, 2015 NBBR 17 at 15.

[482] *Criminal Code,* RSC 1985, c C-46.

Law enforcement might be of the view, for example, that hacking a computer or device is analogous to breaking down someone's front door in order to carry out a search warrant or authorized interception: *Lyons v The Queen*, [1984] 2 SCR 633.

[483] s. 273.64 (1)(c), *National Defence Act*, RSC 1985, c N-5.

[484] Justin Ling (2015), "Canadian Police, Spies Eyed Hacking Team Tech – and the Law Now Makes it Easier to Acquire", *VICE News* (13 July 2015) <https://news.vice.com/article/canadian-police-spies-eyed-hacking-team-tech-and-the-law-now-makes-it-easier-to-acquire>.

[485] While the Communications Security Establishment (and in some cases the Canadian Security Intelligence Service) are potentially able to engage in all of these activities in at least some situations, law enforcement are likely to be far more limited in their ability to secure evidence in this manner—even with assistance from the CSE subject to s. 273.64 (1)(c), National Defence Act, RSC 1985, c N-5 or the proposed s. 21 of the *Communications Security Establishment Act* in Bill C-59 (*An Act respecting national security matters*), First Reading.

[486] *R v Marakah*, 2017 SCC 59.

Note however than many closely connected legal questions remain yet unresolved. See e.g., *Mills v R,* 2017 NLCA 12 [leave to appeal to Supreme Court of Canada granted]; *Vice Media Canada Inc. v R*, 2017 ONCA 231 [leave to appeal to Supreme Court of Canada granted]; *R v Reeves*, 2017 ONCA 365 [leave to appeal to Supreme Court of Canada granted].

[487] Peter Swire & Kenesa Ahmad (2011), "'Going Dark' Versus a 'Golden age for Surveillance", Center for Democracy and Technology (8 November 2011) <https://cdt.org/blog/'going-dark'-versus-a-'golden-age-for-surveillance'/> at 2.

communications data, companies can create more detailed profiles for the purpose of targeted advertising.[488] These types of providers collect disparate information that was once locked away in decentralized file cabinets, safety deposit boxes, and other physical media, and aggregate it in new forms through email, messaging, and file storage services. Google, Microsoft, and other intermediaries routinely provide these services at little or no cost to the user and, as a result, operate under powerful incentives to retain their ability to mine user data for analysis, commercialization, and resale. Widely adopted end-to-end encryption, alongside techniques to encrypt certain forms of metadata, undermine such business models and are consequently unlikely to be chosen as a design defaults by all providers.[489]

Finally, even for companies that are commercially motivated to protect user privacy, it may not be technically feasible to extend end-to-end encryption across all services, and certain forms of metadata may need to remain available as plaintext for technical reasons. Companies are also motivated to avoid fully encrypting all of their customers' communications and data because of concerns regarding usability, speed, and efficacy. For example, in 2014 Facebook's former Chief Security Officer admitted the company "has been able to deploy end-to-end encryption for a long time" but avoided doing so citing of concerns about usability and complexity.[490] These variables, taken together, mean that we are unlikely to see a digital ecosystem where all (or even most) data held by intermediaries is both encrypted and unavailable to those intermediaries by default, at least for the foreseeable future.

In Canada, law enforcement already possess the necessary legal tools to access this kind of stored information, and in the past decade have gained greater ease of access through legal reform. In all cases where an intermediary maintains plaintext access to data, that service provider can be served with a production order under existing *Criminal Code* powers.[491] Even where data is retained only for short periods of time, preservation orders allow investigators to place a hold on information until a production order can be secured, as long as the storage is not truly ephemeral in nature.[492] A range of lawful access powers have also made it easier for Canadian law enforcement to gain access to other kinds of electronic evidence. *Criminal Code* provisions introduced in the 2015 *Protecting Canadians from Online Crime Act* gave law enforcement the ability to secure various kinds of metadata and location records with ease, in some cases even based on a lower threshold than access to other forms of private communications data (i.e., on the basis of "reasonable suspicion" rather than "reasonable belief"). As discussed in Part 1, metadata and other seemingly innocuous digital records can reveal highly sensitive information about an individual's biographical core, their behaviour and preferences, their personal relationships and private communications.[493] Indeed, metadata analysis is sufficiently advanced that governments use this information to help to justify lethal military and covert actions.[494] In the words of an RCMP metadata analyst:

> "In this digital age, we're leaving crumbs of digital data behind everywhere we go and in everything that we do. … The frequent usage of these devices really turns them into a tracker in the hand of the

---

[488] For example, see Google's long term collection and analysis of e-mail message content for the purpose of targeted advertising.

Brian Fung (2017), "Gmail will no longer snoop on your emails for advertising purposes", *The Washington Post* (26 June 2017) <https://www.washingtonpost.com/news/the-switch/wp/2017/06/26/gmail-will-no-longer-snoop-on-your-emails-for-advertising-purposes/>.

[489] See Scott Schober (2016), "Google's Big Encryption Gamble", (21 May 2016) <https://scottschober.com/googles-big-encryption-gamble/>.

[490] These concerns (which cite usability issues in the e-mail encryption context) are likely to be somewhat overstated when applied to instant messaging applications, particularly in light of the success of tools like Signal and WhatsApp. As of 2016, Facebook allowed opt-in end-to-end encrypted chats on a per-conversation basis.

Zach Miners (2014), "Facebook holds back on end-to-end encryption", *Computer World* (19 March 2014) <https://www.computerworld.com/article/2488773/cybercrime-hacking/facebook-holds-back-on-end-to-end-encryption.html>. David Lumb (2016), "Facebook Messenger now lets you toggle end-to-end encryption", *EnGadget* (4 October 2016) <https://www.engadget.com/2016/10/04/facebook-messenger-now-lets-you-toggle-end-to-end-encryption/>; Facebook, "Secret Conversations" (accessed 5 February 2018) <https://www.facebook.com/help/messenger-app/1084673321594605/?helpref=hc_fnav>.

[491] See ss. 487.013 to 487.018, *Criminal Code,* RSC 1985, c C-46.

[492] See s. 487.019, *Criminal Code,* RSC 1985, c C-46.

[493] See e.g., *R v Spencer*, 2014 SCC 43; *R v Vu*, 2013 SCC 60; *In the matter of an application by XXXXX XXXX for warrants pursuant to Sections 12 and 21 of the Canadian Security Intelligence Act, RSC 1985, C. C-23 and in the presence of the Attorney General and Amici and in the matter of XXXX XXXXXXX XXXXX XXXXX XXX threat related activities,* 2016 FC 1105.

[494] David Cole (2014), "'We Kill People Based on Metadata'", *New York Review of Books* (10 May 2014) <http://www.nybooks.com/daily/2014/05/10/we-kill-people-based-metadata/>.

> "As NSA General Counsel Stewart Baker has said, "metadata absolutely tells you everything about somebody's life. If you have enough metadata, you don't really need content." When I quoted Baker at a recent debate at Johns Hopkins University, my opponent, General Michael Hayden, former director of the NSA and the CIA, called Baker's comment "absolutely correct," and raised him one, asserting, "We kill people based on metadata."

> user. And if you know how to leverage that information and make sense of it, there's so much you can do with it. If investigators aren't leveraging this to their advantage, they're missing out."[495]

Academics have argued that information losses caused by encryption have been "more than offset" by the proliferation of metadata records, new capabilities to capture and analyze location data, the ability to engage in social graph analysis of networks, and the availability of "big data" analysis to facilitate investigations.[496] In many instances, the offset is direct. Data encrypted in transit or on a mobile device is frequently backed up to—and readily accessible from—a cloud service provider.[497] Even where interception of an interaction with a particular website, peer-to-peer file-sharing service or online commentary site yields nothing but data encrypted in transit, subscriber data and "source or destination" metadata can provide an avenue to precisely the same anonymous online activity.[498]

In other instances the offset is less direct, as technological change continues to create new data that simply never existed historically. Such data, in turn, opens new and readily accessible investigative avenues.[499] The use of open source intelligence (or OSINT)[500] techniques allows investigators to harvest information from publicly available sources such as social media, and has been described by law enforcement as especially helpful in identifying "prolific and serious offenders in cyberspace and … major cybercrime targets."[501] For example, the RCMP's Firearms Internet Investigation Support Unit leverages publicly available online open source intelligence to assist in the screening of specific firearm license applicants, assess ongoing eligibility, proactively identify public safety risks from firearms-related criminal activity, and assist in investigations of firearm-related crimes.[502] However, it should be noted that the RCMP have also relied on open sources to engage in more problematic activities, including political profiling and surveillance of social movements. During the Group of 8 (G8) and Group of 20 (G20) meetings that were hosted in Ontario in 2010, Toronto Police Services conducted 24-hour monitoring of social media sites such as Facebook and Twitter to identify mass transit disruption, track demonstrator movements, monitor individuals posting negative comments about

---

[495] Royal Canadian Mounted Police (2017), "Crumbs of digital data: Data analyst makes sense of phone calls", *Gazette Magazine* 78:3 (4 July 2017) <http://www.rcmp-grc.gc.ca/en/gazette/crumbs-digital-data?re>.

[496] Peter Swire & Kenesa Ahmad (2011), "'Going Dark' Versus a 'Golden age for Surveillance", Center for Democracy and Technology (8 November 2011) <https://cdt.org/blog/'going-dark'-versus-a-'golden-age-for-surveillance'/> at 8-10.

[497] Access Now (2018), "Encryption in the US: Crypto Colloquium Outcomes Report", *Access Now* (January 2018) <https://www.accessnow.org/cms/assets/uploads/2018/02/Encryption-in-the-United-States-Crypto-Colloquium-Outcomes-Report.pdf> at 15.

[498] See e.g., Communications Security Establishment, "Levitation and the FFU Hypothesis", released by Edward Snowden, < https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASH013f/ed0da817.dir/doc.pdf>; *R v Spencer*, 2014 SCC 43.

[499] Then-RCMP Commissioner Bob Paulson has suggested that the best solution to the "going dark" encryption challenge is to devise new and creative ways to conduct investigations.

See RCMP Commissioner Bob Paulson (2015), "Keynote Address at the Securetech 2016 Conference", *Royal Canadian Mounted Police* (25 November 2015) <http://www.rcmp-grc.gc.ca/en/news/2015/27/commissioner-bob-paulson-presents-keynote-address-securetech-2015-conference>; archived at <https://cippic.ca/uploads/RCMP_Paulson-KeynoteatSecuretech2015-2015.pdf>.

[500] *Professional Institute of the Public Service of Canada v Canada (Attorney General)*, 2015 FC 1101 at para 19:

> "An open source inquiry involves accessing publicly available information, such as various internet sources, including social media."

See also Public Safety Canada (2011), "Social Media Sites: New For a for Criminal, Communication and Investigative Opportunities", *Public Safety Canada* (August 2011) <http://publications.gc.ca/collections/collection_2012/sp-ps/PS14-5-2011-eng.pdf> at 12:

> "OSINT is about searching for information accessible to the public, but finding the information that the public does not know how to obtain, and analyzing it in a fashion the public doesn't know how to analyze."

[501] The RCMP states that open source intelligence units are "critical to criminal investigations with cyber elements, and will increase in complexity and volume as criminals continue to exploit new and emerging technologies."

See Royal Canadian Mounted Police (2015), "Cybercrime Strategy" <http://www.rcmp-grc.gc.ca/wam/media/1088/original/30534bf0b95ec362a454c35f154da496.pdf> at 8-9.

[502] Royal Canadian Mounted Police (2017), obtained under Access to Information request by Mr Dennis R Young, Request File No: A-2014-01540 (18 January 2017) <https://calibremag.ca/wp-content/uploads/2017/08/Info-Commissioner-Reports-FIISU-has-No-Criteria-or-List-of-Public-Safety-Risks-Jan-18-2017.pdf> archived atL <https://cippic.ca/uploads/2017-ATI-Dennis_Young-RCMP-FISSU.pdf>:

> "The unit gathers information from a variety of online sites that are accessible to the public. The Internet unit has two service components: in its primary role, the unit provides … any information uncovered during an internet (sic) search of firearm licence applicants and licenced clients under continuous eligibility to support their regulatory/public safety investigations. The secondary role consists of open source searches of internet sites identifying public safety risk from firearms and criminal activities relating to firearms. The information gleaned from this area of the internet (sic) is forwarded to the police of jurisdiction for further investigation."

the police,[503] gather advance information about individuals and groups intending to participate in protests,[504] and investigate the anonymous online activity of individuals identified as suspects.[505] Similarly, the RCMP's Project SITKA relied extensively on open source information (such as Facebook activity) to monitor and profile individuals and groups participating in political protest on Indigenous issues. An RCMP report on the project notes, in particular, the utility of social media and blogging activity as a means of obtaining real-time intelligence regarding the location of ongoing protests, as a means of identifying actual attendees, and as a means of conducting risk assessments of individuals for the RCMP's suspect categorization scheme.[506]

Law enforcement has also made use of the digital environment to facilitate covert surveillance investigations and to infiltrate groups of interest. At one time, these activities would have required substantial human resources, logistical complexity, and considerable risk, but can now be conducted remotely with reduced logistical and operational costs.[507] Encryption can be integral to maintaining the security of these types of covert law enforcement activities,[508] and Canadian law enforcement agencies are increasingly leveraging these new information sources.[509] Emerging developments in networked sensors and the "Internet of Things"—technology which is rapidly being integrated into every imaginable form of home appliance, vehicle, and personal assistant device—are also likely to provide new and readily exploitable avenues for law enforcement.[510] At the same time, state

---

[503] Jason A Bakas, "Open Source Intelligence: Social Media for Use in Investigations and Policing", <http://www.academia.edu/7205751/Open_Source_Intelligence_Social_Media_For_Use_In_Investigations_And_Policing>:

> "Toronto Police began expanded its analysis of OSNIT specify into social media during the 2010 G8 and G20 Summits. TPS had two officers on 12-hour round the clock shifts analyzing public opinion and communications by protesters. A review of keywords and hash-tags showed that the citizens more frequently used Twitter as they sought information about road closures, mass transit disruptions, and police and demonstrator movements then other media. Those posting negative comments about the police used Facebook more frequently than other social media platforms."

[504] CP24.com (2010), "Police Monitoring Social Media in Anticipation of G20 Protests", *CP24* (26 April 2010) <https://www.cp24.com/police-monitoring-social-media-in-anticipation-of-g20-protests-1.506283>.

Some advocacy groups may also decide to post information law enforcement would not be able to compel in advance, such as protest itineraries. See *Villeneuve c Ville de Montréal,* 2018 QCCA 321.

[505] *R v Sonne*, 2011 ONSC 6734, para 64; *R v Sonne*, 2012 ONSC 140, para 11.

[506] Royal Canadian Mounted Police (2015), "Project SITKA: Serious Criminality Associated to Large Public Order Events with National Implications", *Her Majesty the Queen in Right of Canada as represented by the Royal Canadian Mounted Police* (16 March 2015) at 11-12 and Appendix A at vii-x (obtained by access to information request) <https://warriorpublications.files.wordpress.com/2016/11/project-sitka-report.pdf> archived at: <https://cippic.ca/uploads/2015-ATI-RCMP-project_sitka.pdf>.

Aboriginal Affairs and Northern Development Canada (AANDC) also extensively monitored the social media conduct and activities of Dr. Cindy Blackstock, a public advocate engaged in human rights litigation against AANDC on behalf of the First Nations Child and Family Caring Society. See: Office of the Privacy Commissioner of Canada (2013), "Aboriginal Affairs and Northern Development Canada Wrongly Collects Information from First Nations Activist's Personal Facebook Page", *Office of the Privacy Commissioner of Canada* (29 October 2013) <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-federal-institutions/2012-13/pa_201213_01/>.

[507] See e.g., Government of Canada (2018) "Advanced Open Source Intelligence Course (AOSINT)", *Canadian Police College* (last modified 13 February 2018) <http://www.cpc-ccp.gc.ca/en/aosint>:

> "Have a toolkit to track individuals and organizations internationally using public record databases and effective people searching tools; Conduct advanced social media investigations using commercially available tools. Conduct investigations involving peer-to-peer and file sharing networks."

See also: Public Safety Canada (2011), "Social Media Sites: New For a for Criminal, Communication and Investigative Opportunities", *Public Safety Canada* (August 2011) <http://publications.gc.ca/collections/collection_2012/sp-ps/PS14-5-2011-eng.pdf> at 12-13:

> "Police officers and private investigators can attempt to befriend such individuals using fake accounts in order to try to infiltrate the network of the suspect. Fake accounts can be long-term efforts, with the goal of gaining enough connections with the suspect to earn their trust."

[508] See e.g., *R v Mills*, 2017 NLCA 12; The Tor Project, "Users of Tor", (2018) <https://www.torproject.org/about/torusers.html.en>; Roger Dingledine (2010), "Anti-Censorship & Transparency", *IIS* (26 October 2010) Från Internetdagarna. Folkets Hus, Stockholm <https://youtu.be/35l56KjTCb8?t=1h25m20s>; Public Safety Canada (2011), "Social Media Sites: New For a for Criminal, Communication and Investigative Opportunities", *Public Safety Canada* (August 2011) <http://publications.gc.ca/collections/collection_2012/sp-ps/PS14-5-2011-eng.pdf> at 14 [identifying "awareness of the amount of personal detail [law enforcement] leave behind during a digital investigation" as a central early challenge to open source intelligence gathering].

[509] Generally, research demonstrates that as early as 2011 various public safety bodies such as the RCMP, Ontario policing services, and the CBSA were seeking to remove historical filters on agency network access to social media sites and other open sources in order to fully harvest their investigative potential.

See Tamir Israel (2011), "The Evolving Role of Cyber Surveillance in Public Sector Decision-Making", *CIPPIC* (2 June 2011) <https://www.cippic.ca/sites/default/files/AgentsoftheState-Roundtable_Presentation.pdf>; Kenrick Bagnall (2016), Computer Cyber Crime (C3) Section, Intelligence Services, Toronto Police Service, "Cybercrime State of the Union: A Law Enforcement Perspective", presentation (30 March 2016) <https://www.focusonseries.ca/images/stories/Presentations/Cyber2016/Focus_on_Cybercrime_Presentation_March_30_2016.pdf> [noting that the Toronto Police Service's (TPS) cyber investigation unit assisted TPS in 1,387 cases in 2015].

[510] Matt Olsen, Bruce Schneier, Jonathan Zittrain et. al. (2016), "Don't Panic! Making Progress on the "Going Dark" Debate," Berkman Klein Center for Internet and Society <https://cyber.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf> at 12-15. See also: Deanna Paul, "Your Own Pacemaker Can Noow Testify Against You in Court" *Wired* (29 July 2017) <https://www.wired.com/story/your-own-pacemaker-can-now-testify-against-you-in-court/>.

agencies continue to exploit historical digital datasets. For example, the fact that mobile devices maintain connectivity by continuously "checking in" with nearby cell phone towers can create a rich tapestry of individuals' movements across space and time.[511]

Empirically, measuring the impact of encryption on the state's investigative capacity is challenging. To a large degree, these difficulties arise from a lack of public accountability regarding both the scope and nature of modern surveillance practices on the one hand, and regarding the presence and extent of investigative barriers on the other. It is clear that in some contexts, the presence of encryption will prevent law enforcement agencies from accessing some data. For example, over the course of the last decade technology companies have increasingly deployed encryption both to better protect website data in transit and data stored on mobile devices at rest. However—and while Canadian law enforcement officials have frequently stated that encryption impedes their work in the abstract—challenges posed by the technology have never been mentioned in the annual electronic surveillance reports produced by the federal and provincial governments of Canada, nor has public data ever demonstrated that such hurdles otherwise exist.[512] The RCMP itself has also acknowledged that in many cases alternative investigative techniques are available when encryption poses an initial obstacle. In a 2016 briefing document, it noted that it was in the process of undertaking:

> "...the early stages of its own quantitative and qualitative study in relation to intercept challenges and encryption and their operational impact (e.g. delays, increased costs, or fewer or lesser charges). However, it is difficult to capture cases where police did not seek judicial authorization for digital evidence due to certain barriers, and instead pursued an alternative investigative strategy (e.g. undercover work)."[513]

However, the RCMP has not, as of this report's release, publicized the results or any data related to that effort. While it has privately shared select examples of investigations hampered by encryption to certain journalists, the raw facts underlying these case studies have never been subject to publication, expert scrutiny or independent review.[514] Where law enforcement agencies face barriers to accessing data that is encrypted in transit, but stored in an accessible format abroad, improving the efficiency of cross-border data access is clearly a more minimally rights-impairing solution than any large-scale effort undermine encryption tools.[515] The UN Special Rapporteur on freedom of expression has also recognized that a wide range of alternate measures remain available to law enforcement that do not require any systemic attempt to compromise encryption.[516]

Equally difficult to quantify is the overall impact of encryption on investigations conducted by state agencies. To the extent that statistics are available, they suggest that law enforcement wiretapping authorizations were reduced in 2015-2016.[517] However, there is no evidence that this decrease is because encryption has become a barrier to effective wiretapping. Instead, it is more likely that law enforcement are able to obtain the data they need from other sources that do not require Part VI authorization, or due to another entirely unrelated variable. Additionally, while law enforcement agencies in Canada are legally obligated to track and report statistics regarding their use of traditional electronic surveillance tools such as wiretaps, no comparable obligations exist for modern data

---

511 Christopher Parsons (2018), "Law Enforcement and Security Agency Surveillance in Canada: The Growth of Digitally-Enabled Surveillance and Atrophy of Accountability", Social Science Research Network (SSRN) (7 March 2018) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3130240> at 6-10.

512 See generally Public Safety Canada, Annual Reports on the Use of Electronic Surveillance <https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/index-en.aspx>; s. 195, *Criminal Code,* RSC 1985, c C-46; see also Christopher Parsons and Adam Molnar (2018), "Government Surveillance Accountability: The Failures of Contemporary Canadian Interception Reports", forthcoming in Can J of L and Tech.

513 Royal Canadian Mounted Police, "Encryption and Law Enforcement", Brief obtained in 2017 under the *Access to Information Act* by Christopher Parsons at 3.

514 David Seglins, Robert Cribb and Chelsea Gomez (2016), "Inside 10 Cases Where the RCMP Hit a Digital Wall", CBC News (15 November 2016), <http://www.cbc.ca/news/investigates/police-power-privacy-rcmp-cases-1.3850783>; see also Christopher Parsons (2016). "Pleading the Case: How the RCMP Fails to Justify Calls for New Investigatory Powers", Technology, Thoughts, and Trinkets (15 November 2016) <https://christopher-parsons.com/pleading-the-case-how-the-rcmp-fails-to-justify-calls-for-new-investigatory-powers/>.

515 See Public Safety Canada (2011), "Social Media Sites: New For a for Criminal, Communication and Investigative Opportunities", *Public Safety Canada* (August 2011) <http://publications.gc.ca/collections/collection_2012/sp-ps/PS14-5-2011-eng.pdf> at 14-15 [identifying cross-border challenges in accessing data from global social media platforms]. See also Canadian Internet Policy and Public Interest Clinic (CIPPIC) (2017), "CIPPIC Joins in Letter to Council of Europe Regarding Proposed Expansion of Cross-Border Law Enforcement Data Access", *CIPPIC* (8 September 2017) <https://cippic.ca/news/coalition_submission_to_CoE_regarding_proposed_2nd_p rotocol_on_cross_border_LEA_data_access>.

516 David Kaye (2015), Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/29/32, 29th session of the Human Rights Council <http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/Pages/ListReports.aspx> at para 11.

517 See Public Safety Canada (2016), "2016 Annual Report on the Use of Electronic Surveillance", Table 1 "Number of Applications" [reports 72 Part VI applications sought for 2015 and 2016, a decrease over recent years].

acquisition tools such as the production orders discussed above,[518] As discussed above, the growing use of encryption has also undoubtedly been offset to some degree by an increase in new forms of unencrypted data. Indeed, many Canadian policing agencies themselves have no clear understanding regarding the scope of, or relationships between, their own surveillance practices. For example, in 2015 the RCMP noted it was unable to provide comprehensive accounts regarding its collection of subscriber data when audited by the Office of the Privacy Commissioner of Canada.[519] Similarly, when presented with freedom of information requests, many policing agencies noted that information regarding metadata access was not historically tracked, while others simply did not respond to requests at all.[520] The end result is that instrumental arguments for the "necessity" of greater access to encrypted datasets are difficult to justify empirically, as state agencies seeking to justify restrictions on encryption can present an incomplete picture of the shift that occurs when historically accessible interactions are occluded by encryption.

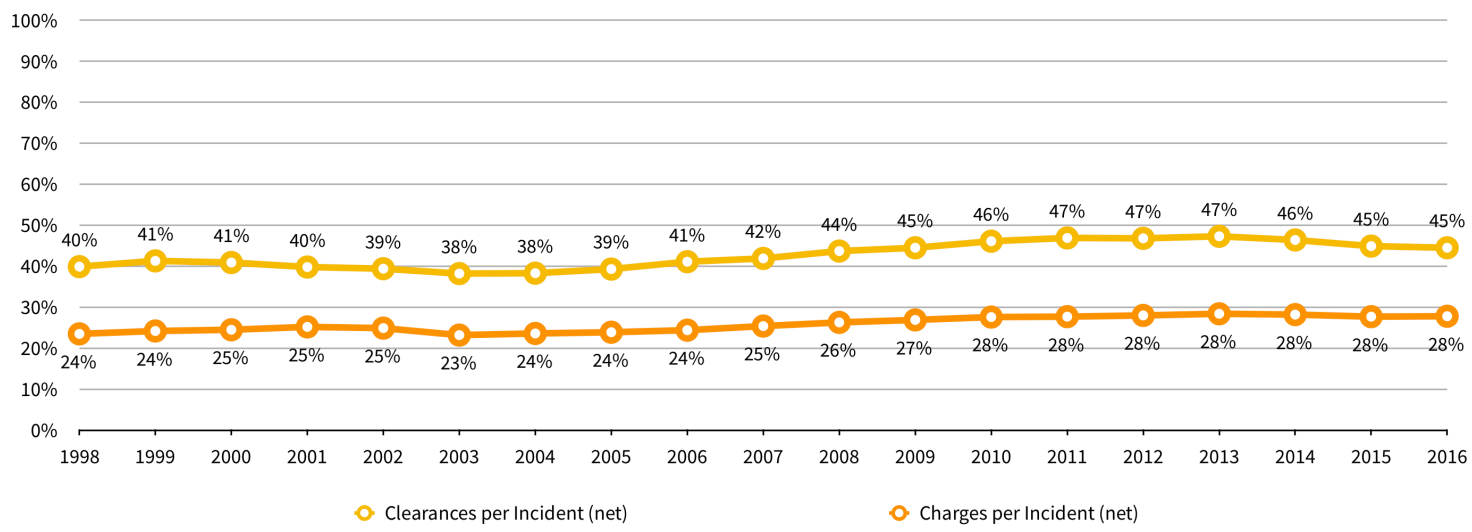


Figure 6: Clearance & Charge Rates per Police-Reported Incident, 1998-2016[521]

What is clear at this stage is that law enforcement clearance and charge rates have remained steady in recent years, and all other things being equal, this trend suggests that the proliferation of encryption is not responsible for any wide-ranging crisis in policing. The onus for demonstrating investigative obstacles of a magnitude sufficient to justify intrusive new powers to access encrypted data has simply not been met; law enforcement and intelligence agencies must bear the burden of demonstrating obstacles such that any such exceptional access is required. Failing to do so, their calls for such access should be set aside by legislators.

---

[518] Christopher Parsons and Adam Molnar (2018), "Government Surveillance Accountability: The Failures of Contemporary Canadian Interception Reports", forthcoming in *Can J of L and Tech.*

[519] Michael Geist (2015), "RCMP Records Called 'Incomplete and Inaccurate' in Memo", *Toronto Star* (27 February 2015) <https://www.thestar.com/business/2015/02/27/rcmp-records-called-incomplete-and-inaccurate-in-memo-geist.html>.

[520] For example, the Vancouver Police Department noted "This information was not tracked by the VPD in the years of the request. We simply do not have this information to provide." However, it did state that it will begin centralizing production orders in a manner that would permit tracking beginning in January 2015. Halifax Regional Police similarly noted that it "does not record or track the number of times individual investigations obtain production orders…[for metadata]."

See Freedom of Information Requests filed by Christopher Parsons, in relation to Vancouver Police Department (https://drive.google.com/open?id=0B3NEKmwodtrOVjg4UGdOVWhJQms) and Halifax Regional Police (https://drive.google.com/open?id=0B3NEKmwodtrOUXRuRmh1TENMd1E).

[521] Compiled from Statistics Canada, "Incident-Based Crime Statistics, Annual", CANSIM Table 252-0051 <http://www5.statcan.gc.ca/cansim/a26?lang=eng&retrLang=eng&id=2520051&tabMode=dataTable&p1=-1&p2=9&srchLan=-1>, Displayed for each year: percentage of overall Clearances per overall reported Actual Incidents; Percentage of overall Clearances by Charge per overall reported Actual Incidents.

CONCLUDING REFLECTIONS

Encryption technologies routinely fail to secure the communications and data they are designed to protect. Even large, global companies with a strong commitment to security at best engaged in a perpetual cat-and-mouse game. The range of adversaries seeking to access their customers' data without authorization include state agencies themselves, as well as third party vendors who develop exploits and sell vulnerabilities. Moreover, the encryption systems that individuals rely on to protect their communications depend on the security of those persons' devices, the applications they choose, and the network infrastructure with which they are communicating. Flaws in these systems all expose users to the potential risk that third parties could subsequently decrypt their communications or stored data. Indeed, third parties, including law enforcement and security agencies, regularly gain access to plaintext data despite the use of encryption. And in many cases, even where data is secured in transit, it lies unencrypted on third party chat, data storage, or data processing servers. While encryption can generate some friction for some investigations, it does not and cannot perfectly protect all data—this has never been the case, and there are no signs that this will change in the near future.

Despite these challenges in securing personal devices and communications, it is imperative that private companies can at least attempt to protect their users' activities. Yet these companies must protect their users from an astounding number of potential third parties. They need to ensure that children cannot easily bypass protections that prevent purchases against their parent or guardian's wishes. They have to protect devices from abusive partners who seek to carry out surveillance or other forms of technology-facilitated abuse. Companies must design their services to inhibit the abilities of thieves and criminals to access data, whether physically stored on devices or communicated through the Internet. Employees need to know that their personal devices cannot be targeted by their employers to monitor their workplace activities. Companies need to know that employees' devices cannot be accessed or exploited for the purpose of economic espionage. And citizens, especially those from minority groups, marginalized communities, and those exploring dissenting views, need to know that their data is protected from both targeted and mass government surveillance that risks chilling *Charter*-protected speech and undermining important security interests.

Demands from law enforcement and security agencies seeking greater access to devices, communications services, and data have been extensively analyzed throughout this report. The concerns expressed by these agencies is deceptively simple: without complete access to all data potentially pertaining to an investigation, agencies may not be able to bring an investigation to a conclusion. In the present context, some threads related to a criminal action or national security issue may simply remain inaccessible.

But while law enforcement and security agencies do have a positive obligation to investigate criminal matters and respond to national security issues, it is crucial not to lose sight of why they have this obligation. At least in theory, these agencies are tasked with maintaining the security necessary to ensure that the basic rights of all persons living in a democratic state can be upheld. Such rights do not begin and end with the right to life or property—instead, the democratic promise also guarantees that individuals have the right to speech, association, privacy, and other liberties to conduct their personal and professional lives without undue interference by the state. These rights are now routinely exercised in digitally-mediated ways. As such, encryption is now vital to protect individuals from undue interference by state actors as well as unauthorized private parties. When law enforcement and security agencies call for irresponsible encryption policies, they threaten the ability of individuals to exercise their fundamental rights and freedoms.

Canadian law enforcement and security agencies undoubtedly face challenges in the digital age. But the challenge they face is in modernizing their methods to adapt to new technologies. These agencies have already acquired a range of new powers following the attacks on the United States on September 11, 2001. These new capabilities were designed so that Canadian agencies could keep pace with the world as memories shifted from personal diaries and filing cabinets to blogs, social media, and cloud hosting providers. Agencies subscribe to services that monitor social media for intelligence, collect bulk location data in so-called 'tower dumps', use fake cellular towers to collect information transmitted from mobile devices, deploy malware to intrude into endpoint devices and networking equipment, and can even retroactively re-create the majority of our digital lives with the assistance of Canada's signals intelligence agency. These are profound changes in government surveillance capacity. Consider that, just a decade and a half ago, each of these kinds of activities would have required dozens or hundreds or thousands of government agents tasked with following people—many of whom might not be subject to any particular suspicion. Such agents

would need to gain entry to individuals' personal safes, install cameras in their homes and offices and motor vehicles, access and copy the contents of filing cabinets at the end of each day, and listen to conversations that would otherwise be held in coffeeshops, diners, university classrooms, and other private environments.

So much of our lives are now lived online that today's investigative powers and technologies bear resemblance to the imaginations of science fiction authors in decades past. It is both easier to access information about individuals today than ever before and—because we generate and leave behind so much information—to retroactively determine what they were doing, with whom, where, and at what times. Such capabilities were unimaginable fifteen years ago, though they are not evenly accessible to all Canadian agencies. Many of these powers raise their own significant democratic and civil rights concerns, and constitute issues in their own right that extend far beyond the scope of this report. Nevertheless, it is undeniable that the potential investigative capacities of Canadian agencies are more extensive than at any time in history.

Calls by law enforcement and security agencies to further extend their powers to access encrypted data have manifested in multiple ways. In some countries, governments have called for bans on, and censorship of, encryption software. In other contexts they have restricted the kinds of encryption that can be sold abroad, attempted to force intermediaries to modify their products to facilitate state access to data, or even sought to compel individuals to decrypt their devices under threat of imprisonment. These policies are irresponsible. They would endanger civil liberties and weaken democratic norms, undermining efforts to advance human rights internationally while emboldening rights-infringing states. They are ineffective at advancing law enforcement and security agencies' overriding objectives to act in a way which secures the basic rights of all persons in Canada.

State measures that attempt to reduce the public availability of secure and uncompromised encryption technology rarely meet their purported objectives of preventing access to encryption products by criminal actors, and often present serious negative and unintended consequences. Banning popular digital tools can prompt public opposition and these tools will typically remain accessible as individuals route around state impediments. While some law abiding citizens may decide to not bypass state-imposed restrictions, motivated criminal actors are likely to adopt the strongest protections possible. As a result,banning encryption products will tend to detrimentally affect law-abiding citizens disproprotionately.

Other proposals are intended to affect the types of products technology companies and intermediaries develop, or to limit the security integrated into their products. The ultimate objective of these policies is to ensure that state agents can gain access to the plaintext of encrypted data or communications in all circumstances. These measures can include establishing regulatory regimes that require private companies to build in "backdoors" to their products or adopt key escrow systems to facilitate state access. In other cases, they may involve compelling companies to modify their otherwise-strongly encrypted services to target specific persons or groups, or simply applying economic or political pressure to 'encourage' companies to exclude secure encryption products and services from their offerings. Section Four outlines, in detail, how such proposals endanger the security of end-users, erode consumer trust intn such digital services, and chill lawful speech and association. Governments committed to the promotion of freedom, equality, and diversity should be to support expression and association—including on challenging topics. This is facilitated, in part, by ensuring that individuals retain the ability to communicate in ways that are genuinely private, and that provide the security to explore difficult and sensitive ideas freely. In a digitally-mediated world, then, governments have an obligation to promote and guarantee the availability of secure communications and storage technology, including encryption.

Any act by one government to inhibit the distribution of a private company's strongly encrypted services will have international ramifications. Private businesses may decline to generally provide strongly encrypted services and, by extension, jeopardize persons around the world as other states access persons' private communications in contravention of their human rights. When countries like Canada consider measures that restrict public access to encryption, they must be aware of the international precedent they set, and the risk that their actions may embolden authoritarian regimes and countries with weak human rights records to do the same. While domestic law enforcement and security agencies may not be concerned with the international ramifications of such access, it is the responsibility of governments to be mindful of how their domestic positions and policies impact their human rights obligations abroad.

Finally, states may attempt to use measures that target individual users of encryption technologies in an effort to obtain plaintext communications or stored data. In the criminal law context, these measures amount to a violation of the individual's rights to silence and against self-incrimination. As argued in this report, attempts to make a legal differentiation between alphanumeric passphrases and biometric identifiers for the purpose of this analysis take unduly narrow and formalistic views of the law. Any effort to conscript an individual in an investigation against their own interests in this manner would amount to a

significant violation of their rights and freedoms and run counter to the core organizing principles of Canadian criminal law. Again, the domestic impacts of these choices cannot be considered without considering Canada's own efforts to support and promote the rule of law, democratic values, and human rights internationally.

Far from adopting an irresponsible encryption policy that enacts or advances any of the aforementioned measures, the Canadian government should be taking steps to advance the development, adoption, accessibility, and integrity of robust encryption. This must begin at home. Canada's over-arching cryptography policy should explicitly acknowledge the unconditional benefits of secure encryption, and the government should not advance projects that would limit or discourage the private sector from developing and adopting uncompromised encryption tools. However, if such measures are contemplated, the perceived empirical and policy case favouring their adoption must be proactively and transparently presented to the public. To this end, Canada's cryptography policy should embed a multi-stakeholder approach that encodes engagement with technologists, academics, civil society, and other relevant stakeholders as a precursor to the adoption of any changes to the state's treatment of encryption. Furthermore, Canada should act to clarify situations where there is any ambiguity regarding the use and reliability of encryption technologies that currently exist. For example, the government's policy on compelled password disclosure at borders should be clarified so that Canadians and other travelers alike can cross our borders without fear that their constitutional rights will be placed in jeopardy. Finally, Canada's commitment to innovation and cybersecurity must foster a domestic atmosphere that encourages and facilitates innovation in cybersecurity and encryption research. This commitment can include arms-length funding of robust encryption technologies, policies that encourage the adoption of robust encryption in private sector technologies, and government procurement that favours secure and uncompromised tools. But the Government of Canada's commitment to secure encryption should not stop at home. Canada should also take a leadership role in global cryptography policy by advocating for the importance of strong and uncompromised encryption in international policy fora and in the international legal community. Canada should also foster and facilitate the wide dissemination and adoption of secure encryption technologies internationally.

Ultimately, the case for irresponsible encryption policies has simply not been made. Canadian government agencies have access to more data, about more individuals, than ever before. Neither the Canadian government nor its agencies have presented a compelling case that encryption functions as a significant hindrance to their investigative or intelligence-gathering objectives. This report has provided ample evidence to demonstrate that measures intended to undermine the availability, reliability, and public use of strong encryption implicate important *Charter* rights, jeopardize human rights, and are simply bad policy. With this in mind, the underlying presumption that state agencies have some sort of unmitigated right to access data regardless of the corresponding costs to society must be met with a critical eye. Measures that compromise encryption in exchange for what are at best marginal gains in investigative or intelligence-gathering capacity are misguided. More than that, they are in profound conflict with Canada's commitment to fostering innovation, security, and respect for human rights.