THE ROAD NOT TAKEN: MISSING POWERS TO COMPEL DECRYPTION IN BILL C-59, TICKING BOMBS, AND THE FUTURE OF THE ENCRYPTION DEBATE

ROBERT DIAB[*]

In the fall of 2016, Canada's Liberal government published a Green Paper canvassing public opinion on changes to national security law. The Paper explored the possibility of new powers to compel third parties to assist with decryption, framing the discussion around a terrorism plot analogous to a ticking bomb hypothetical. The public did not support new decryption powers, and Bill C-59, now before Parliament, does not include them. This article revisits the Green Paper to shed light on deeper fault lines in debates about whether police should have a power to compel decryption. The Green Paper points to illuminating parallels between arguments for compelled decryption and for torture. The strongest arguments for each make use of ticking bomb scenarios. While the arguments have attracted much criticism, they remain plausible and undermine key assumptions of those opposed to compelled decryption.

Part II of this article traces two common arguments for why state agents seek powers to compel a third party to decrypt: for justice (to secure convictions) and public safety (to prevent terrorism and other serious offences). Opponents cast doubt on the first claim by pointing to many alternative sources of evidence. They tend to dismiss the second claim, that police need decryption powers for public safety, as merely theoretical, but fail to engage its merits. Part III takes a closer look at the public safety claim in light of the torture debate and the ticking bomb scenario. Despite criticism, arguments in favour of compelled decryption based on the scenario remain theoretically plausible on consequentialist grounds, and rhetorically persuasive by aligning the need for compelled decryption with the value of life (over dignity or privacy). The public safety claim also challenges a common view among opponents of compelled decryption that such powers do not involve a trade-off between privacy and security but between two forms of security. The article concludes by considering the possible impact on the debate of a terrorist act implicating encryption.

TABLE OF CONTENTS

[*] Faculty of Law, Thompson Rivers University. Thank you to Lex Gill and Michael Nesbitt for comments on an earlier draft, to the anonymous reviewer, and to the editors of the *Alberta Law Review*.

I. INTRODUCTION

An important part of Bill C-59 — Canada's most recent national security bill — consists in what its authors chose not to include: powers to compel assistance with decryption.[1] In light of events leading up to the Bill, the omission stands out. In 2016, the government published a Green Paper canvassing public opinion on whether, in certain cases, the state should have the power to compel individuals or bodies to unlock a device or decrypt a communication.[2] As more of our phones and messages have come to be encrypted in recent years, police have often faced significant obstacles in carrying out lawful searches.[3] In calling for powers to compel decryption, the Green Paper made a similar case to one that prominent figures in American law enforcement had made. Police need powers to compel decryption not only to investigate crime and obtain convictions, but also to save lives.[4]

Yet, in ways to be explored, prominent voices among United States law enforcement tended to be nuanced or understated in asserting the need to compel decryption to save lives. The authors of the Green Paper were more overt. At some point soon, the Paper suggested, Canadian police may need the power to compel a third party to decrypt a communication to thwart a terrorism plot — one close in nature to a ticking bomb scenario.[5] Often used in the debate about torture and other extreme measures after 9/11, ticking bomb scenarios portray a measure as the only means, in certain cases, of averting catastrophe — to ground the claim that, in those cases, authorities need to use a certain measure not as a matter of convenience but of practical and moral necessity. The majority of respondents to the government's national security consultations in 2016 did not find the Green Paper's case for compelled

[1] Bill C-59, *An Act respecting national security matters*, 1st Sess, 42nd Parl, 2018 (as amended by committee 3 May 2018). Encryption in this article means "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 is "the process of using a key to transform ciphertext back into plaintext, a readable form" (Lex Gill, Tamir Israel & Christopher Parsons, *Shining a Light on the Encryption Debate: A Canadian Field Guide* (Ottawa: Citizen Lab and the Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic, 2018) at 1).

[2] Government of Canada, *Our Security, Our Rights: National Security Green Paper, 2016: Background Document* (Ottawa: Her Majesty the Queen in Right of Canada, 2016) at 7, 55 [*Green Paper*].

[3] See the discussion of the "strength of a cryptographic system" in Gill, Israel & Parsons, *supra* note 1 at 3. See also Devlin Barrett, "FBI Repeatedly Overstated Encryption Threat Figures to Congress, Public," *The Washington Post* (22 May 2018), online: <www.washingtonpost.com/world/national-security/fbi-repeatedly-overstated-encryption-threat-figures-to-congress-public/2018/05/22/5b68ae90-5dce-11e8-a4a4-c070ef53f315_story.html> [Barrett, "Overstated Threat"], noting that annual estimates of the number of devices the Bureau could not access in the course of investigations in previous years (close to 8,000) had been incorrect and the number is closer to 1,000 to 2,000.

[4] From herein, "compelled decryption" refers primarily to compelling a third party to assist with decryption. A third party might include a communication service provider or a company such as Apple or Google that makes devices or operating systems. A power to compel a third party to unlock a device or decrypt a communication raises distinct issues from a power to compel an individual to provide a password or plaintext files. See e.g. Steven Penney & Dylan Gibbs, "Law Enforcement Access to Encrypted Data: Legislative Responses and the *Charter*" (2017) 63:2 McGill LJ 201 at 216–44.

[5] *Green Paper*, *supra* note 2, includes a narrative illustrating the potential use of the various powers it considers, with the segment on encryption (*ibid* at 61) forming only a part of the longer story. The narrative is explored further in Part II below.

decryption persuasive.[6] When it finally tabled Bill C-59, the government chose not to include such powers in the bill.[7]

Some commentators have taken issue with the Green Paper's discussion of decryption, or of digital privacy generally, as misguided and "somewhat aggressive."[8] I approach the Green Paper's case for decryption from a different perspective. The Paper points to illuminating parallels between arguments for compelling third parties to assist with decryption and arguments for torture, shedding light on the deeper fault lines of the debate about encryption. The strongest arguments for both decryption and torture involve national security and ticking bomb scenarios — and despite powerful criticisms of them, the arguments remain plausible and undermine key assumptions of those who oppose powers to compel decryption.

To support these claims, this article distinguishes two forms of argument on which law enforcement officials assert a need to compel third parties to decrypt: for justice or the rule of law (to obtain evidence to secure convictions) and for public safety (to obtain information to prevent terrorism and other serious offences). In ways to be explored, advocates and opponents of compelled decryption have debated the need for such powers without distinguishing forms of the argument at issue.[9] Yet the distinction matters because each claim engages different values and considerations. We perceive and respond differently to the prospect of failing to obtain a conviction, even in serious cases, from the way we respond to the prospect of preventing a mass casualty attack.

The difference also affects approaches to the wider debate on compelled decryption, on both of its two main fronts. On one front, parties question whether the state needs the power to compel decryption, while those on another front grapple with whether we can create such powers without losing the security benefits of strong encryption. The national security argument poses a challenge to opponents of compelled decryption on both fronts.

On the first front, opponents say that powers to compel decryption are not necessary, but merely convenient. As we produce ever more data, including metadata that is often not

[6] See Part II of discussion in Hill & Knowlton Strategies, *National Security Consultations: What We Learned Report* (Ottawa: Public Safety Canada, 2017) [*What We Learned*].

[7] Bill C-59, *supra* note 1, includes the *Communications Security Establishment Act*, which would expand, in section 20, the Communication Security Establishment's (CSE) mandate to the carrying-out of "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" (*ibid*, cl 76). This might include decryption, but the CSE (Canada's foreign signals intelligence agency) may not direct its activities at persons in Canada or infrastructure in Canada.

[8] Micheal Vonn, "A Different Shade of Green Paper: What the Government Forgot to Mention" (28 November 2016), online (blog): *British Columbia Civil Liberties Association* <bccla.org/2016/11/ a-different-shade-of-green-paper-what-the-government-forgot-to-mention/> ("in the main, it reads like it was drafted by a public relations firm tasked with selling the current state of extraordinary, unaccountable powers"); Craig Forcese & Kent Roach, "Righting Security: A Contextual and Critical Analysis and Response to Canada's 2016 National Security Green Paper" (2016) University of Ottawa Faculty of Law, Working Paper No 2016-39 at 32 (the authors refer to the "somewhat aggressive tone of the Green Paper both on privacy and related information-sharing issues"). See also Gill, Israel & Parsons, *supra* note 1 at 37 (noting the *Green Paper*'s recognition of personal and commercial privacy and security interests but arguing the report "did not explain how consideration of these various interests should be weighed, balanced, or understood in relation to each other").

[9] Part II below canvasses advocacy on the part of law enforcement in Canada and the US, and a range of commentary in opposition to compelled decryption.

encrypted, we create ample alternative sources of evidence.[10] But opponents of compelled decryption are less persuasive in response to the claim that police need these powers for public safety. State agents assert that in some cases, encrypted data could serve as a *unique* source of information they need to thwart a terrorist attack. Opponents dismiss this claim as hypothetical and unlikely. But while it may be unlikely, it remains a tenable and forceful claim (in ways to be explored), even if only in theory.

On the second front of the debate, opponents of state powers to compel decryption emphasize the potential detriment to all digital security that such powers would entail. Data security experts generally agree that we cannot technically facilitate ways to decrypt on demand, through "backdoors" or otherwise, without compromising the security of the system at issue — or at least, the contrary has yet to be demonstrated.[11] All backdoor, escrow, or other systems thus far proposed give rise to vulnerabilities that undermine the security that encryption offers to a wide range of stakeholders, public and private.[12] As a consequence, prominent members of the data security community argue that the debate about encryption does not involve an attempt to balance privacy and security so much as it involves a choice between two kinds of security.[13] However, the argument for decryption based on national security and ticking bomb hypotheticals challenges this claim. It suggests that, at least in theory, the trade-off to be made with decryption powers *in some cases* is not one between privacy over personal data and law enforcement in a general sense, but one between data protection and life itself. The former framing of the issue (a trade-off between two forms of security) will continue to play a prominent role in the debate about encryption so long as privacy concerns remain more salient than concerns about public safety. But in the wake of a large-scale terrorist attack, this can readily change. The primary aim of this article is not to advocate the merits of the public safety argument, but to understand how it works and why it persists in many quarters.

Part II of this article briefly outlines the recent history of the encryption debate and the context in which law enforcement has begun to argue that powers to compel third parties to assist with decryption are necessary. It examines the Green Paper's case for decryption powers and situates the claim within the broader debate about encryption. Part III of the article draws on the debate about torture to examine the argument for decryption grounded on national security and a form of the ticking bomb hypothetical. Scholars in both the torture

[10] Examples are found in Charles Duan et al, *Policy Approaches to the Encryption Debate* (Washington, DC: R Street Institute, 2018) [*R Street Policy Study*]; Matt Olsen, Bruce Schneier & Jonathan Zittrain, *Don't Panic: Making Progress on the 'Going Dark' Debate* (Cambridge, Mass: Berkman Center for Internet & Society at Harvard University, 2016) [*Don't Panic*]; Gill, Israel & Parsons, *supra* note 1; all discussed further in Part II, below.

[11] A widely cited document reflecting this position is Harold Abelson et al, "Keys Under Doormats: Mandating Insecurity By Requiring Government Access to All Data and Communications" (2015) 1:1 J Cybersecurity 69. See also Riana Pfefferkorn, *The Risks of "Responsible Encryption"* (Stanford: Center for Internet and Society, 2018); Susan Landau, "Building on Sand Isn't Stable: Correcting a Misunderstanding of the National Academies Report on Encryption" (25 April 2018), online (blog): <www.lawfareblog.com/building-sand-isnt-stable-correcting-misunderstanding-national-academies-report-encryption>; Amie Stepanovich & Michael Karanicolas, "Why an Encryption Backdoor for Just the 'Good Guys' Won't Work" (2 March 2018), online: *Just Security* <www.justsecurity.org/53316/criminalize-security-criminals-secure/>.

[12] Abelson et al, *ibid* at 73–74, noting at 73 that "[a]s exceptional access puts the security of Internet infrastructure at risk, the effects will be felt every bit as much by government agencies as by the private sector." See also Susan Landau, *Listening In: Cybersecurity in an Insecure Age* (New Haven: Yale University Press, 2017) at x [Landau, *Listening In*].

[13] See e.g. Landau, *Listening In*, *ibid* at xiii; the issue is canvassed further in Part III, below.

and decryption debates have offered forceful critiques of the argument based largely on the scenario being unlikely or unrealistic. Yet the argument remains coherent in theory, on consequentialist grounds, holding compelled decryption to be necessary where there are no reasonable alternatives and a greater harm is otherwise certain to follow. The argument also remains compelling by aligning decryption, as it did torture, with the value of multiple lives or life itself, over privacy or individual dignity. The article concludes by suggesting that if events were to unfold that lent greater salience to the use of encrypted data as a tool for terrorism, the national security claim for decryption based on a ticking bomb case could readily gain greater purchase.

II. THE "GOING DARK" PROBLEM AND DEBATE OVER THE NEED FOR COMPELLED DECRYPTION

A. CONTEXT

People with something to conceal have relied upon cryptography at least as far back as ancient Greece, including key figures in the American Revolution and the Second World War.[14] Through much of the twentieth century, as cryptographers in the US made strides along with computer scientists, the US military carefully guarded the use of encryption.[15] As much of industry and the public came to embrace digital networks in the 1980s and early 1990s, encryption became more common, escaping close military oversight.[16]

During this period, the American public began debating proposals for mandating backdoors to encryption — most notoriously, the Clipper Chip.[17] This plan would have permitted industry to create tools with strong encryption on the condition that every device would dispatch to a state agency a key to be held in escrow.[18] Security experts raised doubts about the scheme's viability,[19] along with those set out in similar proposals.[20] But as global demand and competition for products with strong encryption grew, lawmakers became less concerned with encryption and public safety and more concerned with economics.[21] Canada's "Cryptography Policy" of 1998 reflected this view, limiting the export of encryption devices to certain countries and imposing a modest set of licencing requirements.[22]

[14] Timothy A Wiseman, "Encryption, Forced Decryption, and the Constitution" (2015) 11:2 I/S 525 at 527–30.

[15] *Ibid* at 530–34; Gill, Israel & Parsons, *supra* note 1 at 21.

[16] Gill, Israel & Parsons, *ibid* at 22.

[17] *Ibid* at 23; also noted is that Canadian law enforcement at that time had supported efforts by the US government to create restrictions on the use of encryption, citing Brad Evenson, "Going Cryptic on the Net," *The Ottawa Citizen* (23 August 1996) B6 ("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").

[18] Gill, Israel & Parsons, *ibid* at 23.

[19] *Ibid*, citing Matt Blaze, "Protocol Failure in the Escrowed Encryption Standard" (Paper delivered at the 2nd ACM Conference on Computer and Communications Security, Fairfax, Va, November 1994), online: <www.mattblaze.org/papers/eesproto.pdf>.

[20] Gill, Israel & Parsons, *ibid* at 24.

[21] *Ibid* at 24. As the authors also note, this consensus was captured in policy recommendations set out by the annex "Guidelines for Cryptography Policy" in OECD, *Cryptography Policy: The Guidelines and the Issues* (Paris: OECD, 1998) 11.

[22] Gill, Israel & Parsons, *ibid* at 28; Industry Canada, *A Cryptography Policy Framework for Electronic Commerce – Building Canada's Information Economy and Society* (Ottawa: Industry Canada, 1998).

For much of the first decade of this century, public debate about law and security seldom involved mention of encryption. But in the present decade, as encryption has become more pervasive, the issue has resurfaced. In 2010, Google began encrypting all messages sent through Gmail, and in 2012, Apple added end-to-end encryption to its iMessage and FaceTime apps.[23] Apple also began to employ full disk encryption by default on its mobile devices, with a key initially accessible to Apple but from 2014, unlocked only with the user's passcode.[24] Other large platforms, including WhatsApp, have adopted end-to-end encryption, and software for encrypting communications is now readily accessible.[25]

At the outset of this period, prominent figures in US law enforcement began to wage a high-profile campaign against the unfettered use of encryption. In submissions to Congress in 2011, Valerie Caproni, General Counsel for the FBI, outlined the contours of the debate.[26] "In order to enforce the law and protect our citizens from threats to public safety, it is critically important that we have the ability to intercept electronic communications with court approval."[27] Agencies were confronting "a potentially widening gap" between the "authority" to intercept communications and the "practical ability" to do so; "[w]e call this capabilities gap the 'Going Dark' problem."[28] Law enforcement's inability to "collect" data in "real or near-real time" would leave agents "several steps behind," and "unable to act quickly to disrupt threats to public safety or gather key evidence that will allow us to dismantle criminal networks."[29]

Caproni's claim can be parsed into three parts: (1) state agents need the power to decrypt to gather evidence, (2) the evidence is necessary to obtain convictions (or maintain the rule of law), and (3) the evidence is necessary to prevent crime (or protect public safety). State powers to compel decryption may indeed be necessary to fulfil either or both goals, but notably, in asserting these claims, Caproni treated them as one, or invoked them indiscriminately. Yet, as noted, the question of whether state agents need the power to compel decryption to achieve either purpose engages different values and considerations. We

[23] Stephanie K Pell, "You Can't Always Get What You Want: How Will Law Enforcement Get What It Needs in a Post-CALEA, Cybersecurity-Centric Encryption Era?" (2016) 17:4 North Carolina JL & Technology 599 at 622–23, citing Ryan Singel, "Google Turns on Gmail Encryption to Protect Wi-Fi Users" (13 January 2010), online: <www.wired.com/2010/01/google-turns-on-gmail-encryption-to-protect-wi-fi-users/>. For an explanation of end-to-end encryption, see Matthew Green, "How Do We Build Encryption Backdoors" (16 April 2015), online (blog): *A Few Thoughts on Cryptographic Engineering* <blog.cryptographyengineering.com/2015/04/16/how-do-we-build-encrypt ion-backdors/>. In 2018, Apple was said to address recent efforts to circumvent encryption when a phone or iPad is plugged into USB by revising its mobile operating system to require a code to be input in this case (Lorenzo Franceschi-Bicchierai, "Apple Is Testing a Feature That Could Kill Police iPhone Unlockers" (4 June 2018), online: <www.vice.com/en_us/article/zm8ya4/apple-iphone-usb-restricted-mode-celle brite-grayshift>).

[24] Pell, *ibid* at 623, citing Matthew Green, "Why Can't Apple Decrypt Your iPhone?" (4 October 2014), online (blog): *A Few Thoughts on Cryptographic Engineering* <blog.cryptographyengineering.com/2014/10/04/why-cant-apple-decrypt-your-iphone/>.

[25] Andy Greenberg, "Whatsapp Just Switched On End-to-End Encryption for Hundreds of Millions of Users" (18 November 2014), online: <www.wired.com/2014/11/whatsapp-encrypted-messaging/>; Seth Rosenblatt, "Want End-to-End Encryption? Use These Apps" (12 January 2016), online: <the-parallax.com/2016/01/12/want-end-to-end-encryption-use-these-apps/>.

[26] US, *Going Dark: Lawful Electronic Surveillance in the Face of New Technologies: Hearing Before the Subcommittee on Crime, Terrorism, and Homeland Security of the House Committee on the Judiciary*, 112th Cong (2011) (Washington, DC: Federal Bureau of Investigation, 2011) (Valerie Caproni, General Counsel, Federal Bureau of Investigation), online: <archives.fbi.gov/archives/news/testimony/going-dark-lawful-electronic-surveillance-in-the-face-of-new-technologies>.

[27] *Ibid.*

[28] *Ibid.*

[29] *Ibid.*

value both the rule of law and human life. But the prospect of saving lives, of averting a mass casualty attack, presents us as a more pressing goal — triggers a more visceral response — than that of convicting a serious offender. Whether decryption powers are *in fact* indispensable to achieving either purpose is a crucial question, but distinct from the nature of the claim itself. Suffice it to note here that at the outset of recent US debates on the issue, officials offered two distinct grounds in support of powers to compel decryption, but did so without distinction.

Following Caproni, former FBI Director James Comey became the primary public advocate of state powers to compel decryption. He too would argue for these powers without discriminating between justice and public safety as bases for the claim. Speaking at the Brookings Institute in 2014, he asserted: "Those charged with protecting our people aren't always able to access the evidence we need to prosecute crime and prevent terrorism even with lawful authority."[30] Yet Comey was alive to the greater force of the public safety claim, especially the link between encryption and terror. Speaking before the Senate in 2016, Comey asserted:

> When changes in technology hinder law enforcement's ability to exercise investigative tools and follow critical leads, we may not be able to root out the child predators hiding in the shadows of the Internet, or find and arrest violent criminals who are targeting our neighborhoods. We may not be able to identify and stop terrorists who are using social media to recruit, plan, and execute an attack in our country.[31]

In statements of this tenor, he framed encryption not only as a potentially absolute hurdle to preventing a number of serious crimes, but he also repeatedly invoked the image of a terror plot that authorities fail to prevent. Comey did not overtly invoke the ticking bomb hypothetical. Yet his concerns about decryption being a material factor in our "ability to identify [and] stop"[32] an attack from taking place implied the possibility that without the power to decrypt, something approximating a ticking bomb scenario could unfold.

[30] James Comey, "Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?" (Remarks delivered at the Brookings Institution, Washington, DC, 16 October 2014), online: <www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course>. For a further example of both lines of argument being blurred, see Rod J Rosenstein, Address (delivered at the United States Naval Academy, 10 October 2017), online: *US Department of Justice* <www.justice.gov/opa/speech/deputy-attorney-general-rod-j-rosenstein-delivers-remarks-encryption-united-states-naval> ("[e]ncrypted communications that cannot be intercepted and locked devices that cannot be opened are law-free zones that permit criminals and terrorists to operate without detection by police and without accountability by judges and juries"). Christopher Wray, succeeding Comey as Director of the FBI, sought to place the scale of the problem in context by asserting in early 2018 that the Bureau was "unable to access the content of 7,775 devices — using appropriate and available technical tools — even though we had the legal authority to do so," noting that "[e]ach one of those nearly 7,800 devices is tied to a specific subject, a specific defendant, a specific victim, a specific threat" (Christopher Wray, "Raising Our Game: Cyber Security in an Age of Digital Transformation" (Remarks delivered at the FBI International Conference on Cyber Security, Fordham University, New York, 9 January 2018), online: <www.fbi.gov/news/speeches/raising-our-game-cyber-security-in-an-age-of-digital-transformation> [footnotes omitted]). Wray repeated these figures on numerous occasions throughout late 2017 and early 2018, until a *Washington Post* report suggested the figure to be closer to 1,000 to 2,000, with confirmation from the FBI itself (Barrett, "Overstated Threat," *supra* note 3).

[31] US, *Encryption Tightrope: Balancing Americans' Security and Privacy: Hearing Before the Committee on the Judiciary of the US House of Representatives*, 114th Cong (2016) at 2 (James B Comey, Director, Federal Bureau of Investigation) (Comey tied the danger of encryption to the threat of ISIS members recruiting agents and planning attacks in the US).

[32] *Ibid* at 3.

In December of 2015, a terrorist shooting occurred in San Bernardino, California. In the wake of the event, the public grappled with a case that overtly tied encryption to terrorism. Syed Rizwan Farook and his wife shot 14 people at a Health Department building, and were then shot by police.[33] The FBI recovered Farook's iPhone, obtained a warrant to search it, but could not access its data.[34] The Bureau sought an order compelling Apple to assist with decrypting it, giving rise to litigation and questions about the legality of compelling a commercial provider to assist with decryption.[35] The work-issued phone was eventually decrypted by a third party, yielding no significant new information.[36] But in the critical hours and days after the attack, a host of important issues arose: "Was anyone else involved or aware of [the attack]? Who had supplied the weapons to Farook and Malik? Had they been aided or abetted by anyone else? Were they part of a larger conspiracy?"[37] In short, another attack might have been imminent, and police might have found data on the phone to prevent it.

The San Bernardino case thus presented the public with a situation analogous to a ticking bomb scenario. For advocates of compelled decryption, the case offered a concrete example to support the claim that without a power to decrypt, law enforcement could not only fail to obtain a conviction but also to avert a mass casualty attack. Comey was consistently careful to avoid asserting this overtly.[38] Doing so may have seemed imprudent, given the climate of heightened concern over privacy in the wake of the Snowden revelations and data breaches by a host of commercial providers. Since 2014, three bills have been introduced in Congress dealing with encryption — two contemplating decryption powers and one seeking to resist them — but none has passed.[39] As a former Justice Department official noted, "There is zero

[33] Landau, *Listening In*, *supra* note 12 at x.

[34] *Ibid.*

[35] District Attorney, New York County, *Report of the Manhattan District Attorney's Office on Smartphone Encryption and Public Safety: An Update to the November 2015 Report* (New York: 2016) at 19–22 [*District Attorney New York 2016 Report*].

[36] Devlin Barrett, "FBI Paid More Than $1 Million to Hack San Bernardino iPhone," *The Wall Street Journal* (21 April 2016), online: <www.wsj.com/articles/comey-fbi-paid-more-than-1-million-to-hack-san-bernardino-iphone-1461266641>.

[37] *District Attorney New York 2016 Report*, *supra* note 35 at 6.

[38] In February of 2016, during a Senate hearing on national security threats, Senator Dianne Feinstein (DCA) was more direct in tying encryption to terrorism when she asserted: "While the coalition's air campaign is helping to deny ISIL some territorial safe havens and financial resources, how do we degrade it and destroy it if all they need to carry out an attack in the West is an internet connection and an encrypted message application?" (Lorenzo Franceschi-Bicchierai, "Sen. Feinstein Says Terrorists Only Need the Internet and Encryption to Attack" (9 February 2016), online: <www.vice.com/en_us/article/qkjbpw/sen-feinstein-says-terrorists-only-need-the-internet-and-encryption-chat-app-to-attack>).

[39] In April 2016, Senators Feinstein and Richard Burr introduced draft legislation in the Senate, *Compliance with Court Orders Act of 2016*, which would require companies to "provide in a timely manner responsive, intelligible information or data, or appropriate technical assistance to obtain such information" (US, Bill S_, *Compliance with Court Orders Act of 2016*, 114th Cong, 2016 (discussion draft), online: <www.burr.senate.gov/imo/media/doc/BAG16460.pdf>). See Dianne Feinstein, Press Release, "Intelligence Committee Leaders Release Discussion Draft of Encryption Bill" (13 April 2016), online: *United States Senator for California: Dianne Feinstein* <www.feinstein.senate.gov/public/index.cfm/2016/4/intelligence-committee-leaders-release-discussion-draft-of-encryption-legislation>. See also Russell Brandom, "New Bill Would Require Companies to Decrypt Data on Demand" (8 April 2016), online: <www.theverge.com/2016/4/8/11203928/feinstein-burr-encryption-bill-required-to-unlock-data> ("a similar anti-encryption measure failed to pass congress in 2014 after the president withdrew his support"). In 2017, Feinstein continued to advocate for the passage of a decryption bill (Natasha Lomas, "FBI Director Comey Backs New Feinstein Push for Decrypt Bill" (3 May 2017), online: <techcrunch.com/2017/05/03/fbi-director-comey-backs-new-feinstein-push-for-decrypt-bill/>). By contrast, in early 2016, a bipartisan bill was introduced in the House titled, *Ensuring National Constitutional Rights for Your Private Telecommunications Act of 2016*: see Brian Barrett, "New Bill Aims to Stop State-Level Decryption Before It Starts" (10 February 2016), online: <www.

chance of any domestic restrictions on encryption absent a catastrophic event which clearly could have been stopped if the government had been able to break some encryption."[40]

Law enforcement has, however, continued to assert a need to be able to compel decryption, and the claim gives rise to a host of broader questions. To what extent does encryption pose an obstacle to law enforcement in *practice*? What evidence supports the claim that it does? If the state does need decryption powers, can systems be developed for this that maintain the security that strong encryption offers? These questions are explored further below. Notably, the law enforcement community in North America is divided on the question of necessity. Former RCMP Commissioner Bob Paulson and other prominent officials have expressed the view that the state can maintain law and order without decryption powers.[41] General Michael Hayden, former director of both the CIA and NSA, has voiced opposition to back doors to encryption on the view that they would compromise cyber-security more broadly.[42] Michael Chertoff, former Secretary of Homeland Security, and Jonathan Evans, former Director General of the British Security Service MI5, concur.[43] Some European governments agree.[44] The argument also has strong support among members of the cryptography and data security community.[45]

B. ARGUMENTS FOR DECRYPTION IN THE CANADIAN CONTEXT

Before turning to the 2016 Green Paper and the current government's discussion of decryption powers, it may help to first look briefly at the law and policy context in which the Green Paper's proposal was made.[46]

wired.com/2016/02/encrypt-act-2016/> (the bill would "preempt states from attempting to implement their own anti-encryption policies at a state level").

[40] Ellen Nakashima & Barton Gellman, "As Encryption Spreads, U.S. Grapples with Clash Between Privacy, Security," *The Washington Post* (10 April 2015), online: <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>.

[41] Bob Paulson, Address (delivered at the Securetech 2015 Conference, Ottawa, 25 November 2015), cited in Gill, Israel & Parsons, *supra* note 1 at 36.

[42] Lorenzo Franceschi-Bicchierai, "Former NSA Chief: I 'Would Not Support' Encryption Backdoors" (6 October 2015), online: <www.vice.com/en_us/article/8qxwda/former-nsa-chief-strongly-disagrees-with-current-nsa-chief-on-encryption>.

[43] Paul Szoldra, "Ex-NSA Chief Thinks the Government Is Dead Wrong in Asking Apple for a Backdoor" (26 February 2016), online: <www.businessinsider.com/michael-hayden-encryption-apple-2016-2>; Conor Friedersdorf, "Former National-Security Officials Now See the Peril of Weakening Encryption," *The Atlantic* (30 July 2015), online: <www.theatlantic.com/politics/ archive/2015/07/former-national-security-officials-see-the-peril-of-weakening-encryption/399848/>; John Leyden, "Former GCHQ Boss Backs End-to-End Encryption," *The Register* (10 July 2017), online: <www.theregister.co.uk/2017/07/10/former_gchq_wades_into_encryption_debate/>; Jamie Grierson, "Ex-MI5 Chief Warns Against Crackdown on Encrypted Messaging Apps," *The Guardian* (11 August 2017), online: <www.theguardian.com/technology/2017/aug/11/ex-mi5-chief-warns-against-crackdown-encrypted-messaging-apps>; sources cited in Gill, Israel & Parsons, *supra* note 1 at 17.

[44] See the discussion of positions of the German and Dutch governments and the EU Parliament's Committee on Civil Liberties, Justice and Home Affairs in Gill, Israel & Parsons, *supra* note 1 at 18. By contrast, France, the United Kingdom, the Netherlands, and Hungary have adopted laws allowing for assistance with access to encrypted data (Daniel Severson, "The Encryption Debate in Europe" (Stanford: Hoover Institution, 2017), online: <www.hoover.org/sites/default/files/research/docs/severson_webreadypdf.pdf>).

[45] Abelson et al, *supra* note 11; Landau, *Listening In*, *supra* note 12.

[46] For the overview in the next three paragraphs, I am indebted to the discussion in Part 4 of Gill, Israel & Parsons, *supra* note 1.

Presently, Canadian law contains no authority for the state to compel a person or an entity to assist with decryption.[47] There are, however, a host of related powers. The *Criminal Code* authorizes "production orders" that compel third parties to assist with accessing data in their possession or control, but does not require that services or facilities be equipped to provide access to encrypted data.[48] The *Criminal Code* also allows for "assistance orders" to compel any person to assist with lawful surveillance, but the orders do not require parties to facilitate or assist with decryption.[49] In a recent case, the Ontario Court of Justice declined a Crown application for an assistance order to compel an accused to unlock an encrypted phone as contrary to the right against self-incrimination and the right to silence.[50] Scholars debate whether the *Canadian Charter of Rights and Freedoms*[51] would permit a power to compel passwords — with strong arguments for and against.[52] Bill C-59 will allow Canada's Communications Security Establishment (CSE, its foreign signals intelligence agency) to engage in lawful hacking that may include decryption, but the CSE may not direct its activities at persons in Canada, or infrastructure in Canada, using these powers.[53]

Other commonwealth nations do provide for compelled decryption.[54] The UK's *Investigatory Powers Act (2016)* allows the Secretary of State to issue a "technical capability notice" against a person or body compelling them to assist in removing "electronic protection" from "any communications or data" — though when deciding whether to issue the order, the Secretary must consider cost and "technical feasibility."[55] Australia's *Crimes Act 1914*, amended after 11 September 2001, provides for orders compelling the assistance of persons with passwords or other means of accessing encrypted data.[56] South African law

[47] The government acknowledges this gap in the law in the *Green Paper*, *supra* note 2 at 61.

[48] *Criminal Code*, RSC 1985, c C-46, s 487.014.

[49] *Ibid*, s 487.02.

[50] *R v Shergill*, 2019 ONCJ 54.

[51] Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (UK), 1982, c 11 [*Charter*].

[52] For an argument that password compulsion could be *Charter* compliant, see Penney & Gibbs, *supra* note 4 at 226–44; Steven Penney, "'Mere Evidence'? Why Customs Searches of Digital Devices Violate Section 8 of the *Charter*" (2016) 49:1 UBC L Rev 485 at 502–504. For a contrary view, see N Dalla Guarda, "Digital Encryption and the Freedom from Self-Incrimination: Implications for the Future of Canadian Criminal Investigations and Prosecutions" (2014) 61:1 Crim LQ 119; see also Gill, Israel & Parsons, *supra* note 1 at 65–69, and Robert J Currie, "Electronic Devices at the Border: The Next Frontier of Canadian Search and Seizure Law?" (2016) 14:2 CJLT 289 at 317–19.

[53] See note 7 above on section 20 of the *Communications Security Establishment Act* in Bill C-59, *supra* note 1; Christopher Parsons et al, *Analysis of the* Communications Security Establishment Act *and Related Provisions in Bill C-59 (*An Act respecting national security matters*), First Reading (December 18 2017)* (Toronto: The Citizen Lab & Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic, 2017) at 28, 46.

[54] For a broader survey of nations with law providing for compelled decryption, including the European Union, see US, Law Library of Congress, *Government Access to Encrypted Communications* (Washington DC: Library of Congress, 2016).

[55] *Investigatory Powers Act 2016* (UK), ss 253(1), 253(5)(c), 255(3)(c). Gill, Israel & Parsons, *supra* note 1 at 33, note that 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.

[56] *Crimes Act 1914* (Austl), 1914/12, s 3LA. In December 2018, Australia passed the *Assistance and Access Bill* based in part on the UK legislation noted above, allowing for a "technical capability notice" that would compel providers of encrypted devices or services to do "acts or things" to assist with providing access to the encrypted data of targeted individuals. But the bill precludes orders that would create a "systematic vulnerability" which the bill defines as anything that would affect a "whole class of technology" rather than devices or communications of a particular person (*Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Austl), 2018/148, ss 317B, 317L). See

allows for a "decryption direction" compelling assistance through passwords or otherwise.[57] Recent governments in Canada have tabled bills containing decryption powers of a more limited scope (relating to "telecommunication services providers"), but none have passed.[58]

Calls among Canadian law enforcement for state powers to compel decryption date back to at least the late 1990s.[59] Police across Canada have maintained an interest in acquiring decryption powers, with the Canadian Association of Chiefs of Police passing a resolution to this effect in 2016.[60] Canadian police fall in line, in this regard, with counterparts abroad.[61] Public Safety Canada, the federal ministry responsible for national security, called for decryption powers in its 2016 Green Paper discussed below. In 2017, in its annual "Public Report on the Terrorist Threat to Canada," the Ministry expressed a continuing concern with the possible use of encryption to facilitate terrorism but did not call for decryption powers explicitly.[62]

1. THE 2016 GREEN PAPER

In the fall of 2016, soon after the Liberal government took power, the Ministry of Public Safety held a nationwide public consultation on amendments to national security law.[63] To lend context, the Ministry published a pair of documents titled "Our Security, Our Rights: National Security Green Paper."[64] The longer "background document"[65] set out primary threats to national security, including the prospective return of "many Canadians" who travelled to Syria and Iraq to partake in ISIS, and the possible "presence of trained and connected terrorist actors within Canada."[66] The Ministry was also concerned about

also Austl, Commonwealth, Parliament of Australia, *Bills Digest No 49, 2018-19*, by Cat Barker, Helen Portillo-Castro & Monica Biddington (Canberra: Parliament of Australia, 2018).

[57] *Regulation of Interception of Communications and Provision of Communication-Related Information Act* (S Afr), No 70 of 2002, s 21.

[58] See the discussion in Gill, Israel & Parsons, *supra* note 1 at 61 of bills C-47 (2009), C-52 (2010), and C-30 (2012), including clause 2 of the latter bill stating: "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" (Bill C-30, *An Act to enact the Investigating and Preventing Criminal Electronic Communications Act and to amend the Criminal Code and other Acts*, 1st Sess, 41st Parl, 2012, cl 2 (first reading 14 February 2012)). See also Bill C-47, *An Act regulating telecommunications facilities to support investigations*, 2nd Sess, 40th Parl, 2009 (first reading 18 June 2009); Bill C-52, *An Act regulating telecommunications facilities to support investigations*, 3rd Sess, 40th Parl, 2010 (first reading 1 November 2010).

[59] Gill, Israel & Parsons, *ibid* at 27.

[60] Canadian Association of Chiefs of Police, *Resolutions Adopted at the 111th Annual Conference* (Ottawa: CACP, 2016) at 19–26, online: <cacp.ca/resolution.html?asst_id=1197>.

[61] International Association of Chiefs of Police, *Data, Privacy and Public Safety: A Law Enforcement Perspective on the Challenges of Gathering Electronic Evidence* (Alexandria, Va: IACP, 2015), online: <www.theiacp.org/sites/default/files/all/i-j/IACPSummitReportGoingDark.pdf>.

[62] Public Safety Canada, *2017 Public Report on the Terrorist Threat to Canada: Building A Safe and Resilient Canada*, (Ottawa: Her Majesty the Queen in Right of Canada, 2017) at 9 ("increasing prevalence of encrypted technologies allows terrorists to conceal their communications and evade detection by police and intelligence agencies").

[63] *What We Learned*, *supra* note 6 at 1.

[64] In addition to a longer background document (*Green Paper, supra* note 2), Public Safety Canada also published a shorter summary document: Government of Canada, *Our Security, Our Rights: National Security Green Paper* (Ottawa: Her Majesty the Queen in Right of Canada, 2016) [*Shorter Green Paper*].

[65] *Shorter Green Paper*, *ibid* at 5

[66] *Green Paper*, *supra* note 2 at 5.

"[e]xtremist narratives" that have "inspired some Canadians to plot and pursue attacks."[67] The Paper focuses largely on facets of the *Anti-Terrorism Act 2015* (Bill C-51),[68] such as the new "threat reduction" powers of the Canadian Security Intelligence Service, information sharing, no-fly lists, and *Criminal Code* terrorism provisions. The Paper also included a topic not addressed in Bill C-51, headed "Investigative Capabilities in a Digital World," dealing with decryption and powers to compel passwords.[69]

In their discussion of decryption, the authors of the Green Paper made a similar indiscriminate use of arguments based on the rule of law and public safety to the approach found in the US context. The authors noted at the outset that "[t]o protect Canadians from crime or threats to safety and security, Canada's law enforcement and national security investigators must be able to work as effectively in the digital world as they do in the physical."[70] Whether or not information comes primarily or exclusively from "the increasingly complex digital landscape, investigators need access to that information to investigate threats to national security and criminal activity, and to cooperate with foreign partners in a timely manner."[71] But the implications for terror investigations were key: "Digital communications are now a fundamental tool for terrorism-related activities, including radicalization to violence, facilitation of travel for terrorist purposes, acquisition of funding and equipment, and even training for terrorist actions."[72]

Existing law "may not be adequate to deal with the complexity."[73] The Ministry was keen to address obstacles to obtaining "basic subscriber information" held by an Internet service provider,[74] the lack of "consistent and reliable technical intercept capability on domestic telecommunication networks," and access to encrypted data.[75] Investigators and prosecutors face impediments on all three fronts. The Paper contemplated a law that would "require a person or organization to decrypt their communications," though the document was silent on the particulars.[76]

[67] *Ibid.* The document also cites Public Safety Canada, *2016 Public Report on the Terrorist Threat to Canada: Building a Safe and Resilient Canada*, (Ottawa: Her Majesty the Queen in Right of Canada, 2016) as further support for the view that "the principal terrorist threat to Canada remains that posed by violent extremists who could be inspired to carry out an attack within Canada. Violent extremist ideologies espoused by terrorist groups like Daesh and al-Qaida continue to appeal to certain individuals in Canada" (*Green Paper*, *ibid* at 3).

[68] Bill C-51, *An Act to enact the Security of Canada Information Sharing Act and the Secure Air Travel Act, to amend the Criminal Code, the Canadian Security Intelligence Service Act and the Immigration and Refugee Protection Act and to make related and consequential amendments to other Acts*, 2nd Sess, 41st Parl, 2015 (assented to 18 June 2015), SC 2015, c 20.

[69] *Green Paper*, *supra* note 2 at 55.

[70] *Ibid.*

[71] *Ibid.*

[72] *Ibid.*

[73] *Ibid* at 56.

[74] *Ibid.* The *Green Paper* notes the Supreme Court of Canada's decision in *R v Spencer*, 2014 SCC 43, finding a reasonable expectation of privacy in basic subscriber information (BSI) and thus the prima facie requirement for a warrant — in the absence of a reasonable law authorizing a search without one. The *Green Paper*'s discussion (at 57–58) implies that a reasonable law would be one requiring only reasonable suspicion for a valid warrantless search of BSI.

[75] *Green Paper*, *ibid* at 56–57. In what follows, I treat what is described as "Interception Capability for Communications Services" (at 59) together with password compulsion and compelled decryption as belonging to a related set of potential powers that involve access to encrypted data. The *Green Paper* is not specific as to what form these powers might take, or what they might entail technically. The *Green Paper* instead considers the possibility of including them in a general sense, though it offers a concrete scenario for each to give an idea of how the power at issue might be used.

[76] *Ibid* at 61.

To illustrate how all the powers at issue in the Paper might be useful, the Paper contains a set of interconnected "hypothetical scenarios."[77] The story begins with "Mr. A," "a charismatic speaker who holds weekly meetings in a local community centre," expressing "strong views on social and political issues."[78] The young men he addresses become "devoted followers."[79] As Mr. A becomes more radical, his calls for change "start taking on a more violent tone."[80] At a later stage, agents acquire a "suspicion that Mr. A. has inspired Mr. M to begin planning a terrorist attack in Canada with an unidentified person."[81] Yet "[m]uch of Mr. M's collaboration" with this person "happens through exchanges over the Internet, such as through online forums."[82] Police obtain a warrant to intercept messages from Mr. M but discover that Mr. M's service provider lacks the capacity to facilitate interception, and cannot provide for it within the time period set out in the warrant.[83] The focus then shifts to decryption:

> [P]olice 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.[84]

The text says nothing more about the threat at issue. But Mr. M is working with the unknown collaborator on a terrorist plot at an unknown stage. The clock is ticking. Law enforcement are in the dark. Lives are on the line. The thrust is clear: without powers to compel decryption, police may not only fail to get evidence but also to thwart a large-scale attack from unfolding at any moment.

Yet the Green Paper did not assert this explicitly. Nor did the Paper frame its case for compelled decryption powers with a story about a failed prosecution or a murder investigation that runs cold. Its authors made a notable choice in offering a scenario about a terrorism plot *currently unfolding* that compelled decryption might be essential to foiling. The choice was not accidental. For reasons to be explored in Part III, making the case for powers to compel decryption based on justice (to obtain convictions) suggests a measure of added efficiency or convenience, but not a strong case for their *necessity*. For this, something approximating a ticking bomb encryption scenario is key.

[77] *Ibid* at 7.
[78] *Ibid* at 8.
[79] *Ibid*.
[80] *Ibid*.
[81] *Ibid* at 57.
[82] *Ibid*.
[83] *Ibid* at 59.
[84] *Ibid* at 61.

C. THE STATE OF THE DEBATE ON WHETHER THE STATE NEEDS POWERS TO COMPEL DECRYPTION

Before taking a closer look at the national security argument, I turn first to the wider debate on whether the state needs powers to compel decryption — to lend context. Those in the opposing camp argue that: (1) law enforcement often asserts a need for these powers on the basis of an inaccurate picture of how criminals and terrorists use encryption, (2) state agents have failed to make clear the nature of the obstacle that encryption poses, and (3) police have ample sources of other data on which the state can rely to gather evidence and protect public safety. Each of the arguments casts doubt on whether the state needs a power to compel decryption, but they give rise to two issues.

First, critics of compelled decryption often fail to distinguish the form of the necessity argument they seek to target. As Comey, the authors of the Green Paper, and other advocates of compelled decryption have done, opponents of these powers fail to discriminate between justice and public safety as bases for the necessity claim. Opponents arguing against the need for new powers make a more effective case in the context of prosecutions than of public safety — due in part to the lack of urgency and the nature of the risk the former entails in distinction to the latter.

A second issue: opponents stand on solid ground in their criticisms so long as we agree to embrace a shift in perspective from theory to practice — or we agree that the best way to assess the need for new powers is to consider how encryption has thus far been used in practice. While these are plausible assumptions on the part of opponents to new powers, they leave the case for new powers based in theory untouched.

This section concludes by noting that figures from the law enforcement camp offer forceful responses to the common arguments canvassed here, but they too entail a shift in focus from the theoretical to the practical, and thus speak more to the problem of encryption for prosecution than for public safety.

1. PROPONENTS CLAIM NECESSITY BASED ON AN UNREALISTIC VIEW OF HOW PEOPLE USE ENCRYPTION

Opponents make two points here. They contend that when advocates claim a need to compel decryption for public safety or law enforcement, they rely on unrealistic or implausible scenarios. As a recent overview asserts, "encryption policy is treated as a thought experiment, often with over-simplified facts coupled with a great deal of certainty."[85] The report notes the common use of ticking bomb hypotheticals to illustrate how the government's ability to prevent a terror attack might depend exclusively on access to an encrypted text or communication.[86] As opponents of torture had argued, the best response is to "reject the hypothetical's frame."[87] Doing so entails a recognition that ticking bomb scenarios involve "simplified assumptions … not consistent with reality."[88] Opponents of

[85] *R Street Policy Study*, *supra* note 10 at 1.

[86] *Ibid.*

[87] *Ibid.*

[88] *Ibid.*

decryption powers suggest focusing instead on the more complicated factual scenarios in which encryption has posed an obstacle to law enforcement and how it did so.[89]

Opponents also frame the necessity claim as implausible by suggesting that it fails to take into account how people and companies have come to use encryption. As the authors of a 2016 report from Harvard's Berkman Klein Centre for Internet and Society contend, communications among actors involved in serious crimes "will neither be eclipsed into darkness nor illuminated without shadow."[90] Commercial pressures on large platforms and providers such as Google and Apple are leading them to "limit the circumstances in which [they] will offer encryption that obscures user data from the companies themselves."[91] Sources of unencrypted data will continue to expand and that will help law enforcement "fill gaps" left by concealed communications.[92] Moreover, law enforcement will continue to have access to much encrypted communication since "an overwhelming percentage of Internet users communicate through web-based services, such as webmail, instant messages, and social networking websites that are not end-to-end encrypted."[93] State agents can still obtain much of this data by warrant or subpoena.[94]

Opponents of compelled decryption thus contend that advocates for new powers make implausible assumptions. Their ticking bomb hypotheticals are improbable or unrealistic. Their assessments of alternative sources of evidence seem too pessimistic and out of touch with how we now create and transmit data. Yet in both cases, opponents shift the focus of discussion from the plane of theory to practice. Both claims are tantamount to asserting that while a case for necessity *might* be made in theory, alternatives can and are being found in practice. Law enforcement does not therefore *appear* to face an insurmountable obstacle with encryption. The argument is persuasive, but it fails to address the claim for necessity based in theory.

2. EVIDENCE OF A LACK OF ACCESS IS NOT EVIDENCE OF NECESSITY

Law enforcement officials in the US have noted that each year they encounter hundreds of devices they cannot access, pointing to many cases where encryption impedes them from preventing or prosecuting crime.[95] But what the numbers do not indicate is "how many such devices were the linchpin of investigations, as opposed to merely being devices that were seized routinely but were ultimately unnecessary in view of other evidence."[96] Commentators

[89] *Ibid.*

[90] *Don't Panic*, *supra* note 10 at 2.

[91] *Ibid.* Elaborating on this point: "End-to-end encryption and other technological architectures for obscuring user data are unlikely to be adopted ubiquitously by companies, because the majority of businesses that provide communications services rely on access to user data for revenue streams and product functionality, including user data recovery should a password be forgotten" (*ibid* at 3).

[92] *Ibid* at 2.

[93] *Ibid* at 4.

[94] *Ibid.*

[95] Barrett, "Overstated Threat," *supra* note 3, reports on FBI Director Wray's repeated (though erroneous) estimates. See also District Attorney, New York County, *Third Report of the Manhattan District Attorney's Office on Smartphone Encryption and Public Safety* (New York: 2017) [*District Attorney New York Third Report*] at 5 (the District Attorney recovered 1,200 devices in 2017, of which "700 were locked using full-disc encryption").

[96] *R Street Policy Study*, *supra* note 10 at 5.

note the "lack of specific data about what kinds of investigations are being impeded and the extent to which investigations were successful by pursuing other routes."[97] We have evidence that police frequently confront encryption, but not that it hinders them from preventing or prosecuting serious crimes.[98]

This line of argument also entails a shift from theory to practice. Opponents of compelled decryption are asking here whether there *have* been cases in which encrypted information forms the "linchpin" of a plot that police failed to stop, or a conviction that prosecutors failed to obtain — but not whether there *could* be such a case. This argument is also plausible only if we agree to focus on past practice. Once we do, we must concede that powers to compel decryption do not appear to be necessary for prosecution. Opponents of decryption powers might go further and assert that *even if* prosecutors were to present a case in which encryption hindered them from obtaining a conviction, one could argue that the true cause of their failure was a lack of diligence or ingenuity on the part of investigators or prosecutors. One might say the case was hindered due not to a failure to decrypt but to a failure to find other evidence still out there to be found.

Can the same not be said in the case of public safety or national security — even in the case of a ticking bomb hypothetical? A case in which encrypted information was said to be the linchpin of a terror attack police failed to prevent might simply be — for opponents of compelled decryption — a case of police not being quick enough to find other avenues of investigation. Are there not *always* other avenues? In practice, there may well be. In theory, however, we can still posit a situation in which there are no reasonable alternatives as the clock ticks down to imminent and serious harm (more on this below).

Put otherwise, any case in which encrypted data appears to impede prosecutors is one that opponents of compelled decryption can always say is open to being solved if state agents looked more diligently for other evidence. Whether in practice or in theory, in a case where encryption poses an obstacle to prosecution, time is always on the side of opponents of compelled decryption. The same inference cannot be drawn as readily about public safety. Here, urgency and the risk of a loss of life make the argument for decryption more compelling.

3. THE STATE CAN FIND AMPLE AND SUFFICIENT DATA FROM OTHER SOURCES

Proponents of this argument commonly cite Peter Swire and Kenesa Ahmad's 2012 article on encryption, describing the present as a "golden age of surveillance," given the ever-

[97] National Academies of Sciences, Engineering, and Medicine, *Decrypting the Encryption Debate: A Framework for Decision Makers* (Washington, DC: The National Academies Press, 2018) at 42.

[98] *Ibid*. See also Pell, *supra* note 23 at 627 ("What we do not know is how many of these 'failed search' cases, nevertheless, resulted in successful prosecutions. In other words, how often was encryption the dispositive issue?"). See also Marshall Erwin, "The High Standard of Proof in the Encryption Debate" (5 February 2016), online: <www.justsecurity.org/29177/high-standard-proof-encryption-debate/> [emphasis in original]:

> Of course, a Manhattan DA is going to want all the available information that can be helpful to his case. But *helpful* isn't the standard we should be looking to apply as a matter of public policy. What we want to know is whether the information was *necessary* for a successful prosecution or whether alternative sources of information would have been sufficient for that prosecution.

increasing abundance of tracking data within the reach of law enforcement.[99] Much of this information takes the form of unencrypted metadata, which can provide a wealth of detail about location, movement, identity of parties — even family, sexual, or political associations.[100] A further ample source of data is found in the "[n]etworked sensors" that make up the "Internet of Things" which is "projected to grow substantially" in coming years.[101]

Opponents of compelled decryption offer other strands of this argument. One points to lawful hacking, or the various means of overcoming encryption through technical processes,[102] such as those employed by a private company that helped the FBI decrypt the iPhone in the San Bernardino case. Police can also gain access when criminals err in implementing encryption or through other "intrusions at the end points" of communications.[103] And finally, "traditional sources" remain important, such as "witness interviews, physical surveillance, or biological evidence."[104] On this view, people acting upon encrypted data, rather than data itself, pose the real danger — and those actions tend to give rise to discoverable evidence.

This third line of argument is also only effective against the necessity claim if one embraces a shift from theory to practice. Opponents claim here that although in theory encrypted data can form the linchpin of an investigation, in practice investigators will be inundated with data and other evidence, and absolute impediments to prosecution or public safety will be rare and probably non-existent. This may be true. But these facts do not refute the argument for necessity based on situations, in theory, involving imminent risk of serious harm and no reasonable alternative to decryption.

4. RESPONSES IN SUPPORT OF STATE POWERS TO COMPEL DECRYPTION

Advocates of powers to compel decryption have often followed opponents in shifting focus from theory to practice — conceding important ground — but forcefully rebut the arguments canvassed here.

A key concern for law enforcement is the ability to respond in a timely fashion.[105] In some cases, encrypted data may offer the most effective or possibly the only means of quickly identifying co-conspirators or principal suspects about to commit serious offenses.[106] But

[99] Peter Swire & Kenesa Ahmad, "Encryption and Globalization" (2012) 13:2 Colum Sci & Tech L Rev at 420.

[100] *R Street Policy Study*, *supra* note 10 at 5–7. *Don't Panic*, *supra* note 10 at 3:

> Metadata is not encrypted, and the vast majority is likely to remain so. This is data that needs to stay unencrypted in order for the systems to operate: location data from cell phones and other devices, telephone calling records, header information in e-mail, and so on. This information provides an enormous amount of surveillance data that was unavailable before these systems became widespread.

See also National Academies of Sciences, Engineering, and Medicine, *supra* note 97 at 46.

[101] *Don't Panic*, *ibid* at 3.

[102] *R Street Policy Study*, *supra* note 10 at 6–7.

[103] *Don't Panic*, *supra* note 10 at 9.

[104] National Academies of Sciences, Engineering, and Medicine, *supra* note 97 at 45.

[105] *Ibid* at 44.

[106] *Ibid.*

state agents cannot always easily find substitutes for encrypted data.[107] For example, metadata may indeed be a rich source of information; in some cases, details concealed by encryption are crucial, such as what a package contains or a particular party's identity.[108] As one commentator has noted, "the information gained from going bright doesn't necessarily correspond to that lost from going dark."[109]

A further line of argument concerns resources. Law enforcement in Canada and the US have circumvented encryption with the help of third parties, as in the San Bernardino case, but this can be expensive and, therefore, as an option, it does not scale.[110] Whatever help police or prosecutors receive in hacking into devices can also easily be rendered obsolete with each update cycle or new device.[111] Resorting to technical means to overcome encryption on a case-by-case basis is also time-consuming and resource intensive, and thus beyond the means of many smaller police agencies.[112]

In summary, both camps offer strong arguments about the need for decryption powers. However, given the uncertainty over the precise impediment that encryption poses and whether other data can serve as an adequate substitute, the debate has reached a deadlock. Are powers to compel decryption necessary or merely convenient? On closer examination, opponents of compelled decryption make a stronger case against the need for such powers in relation to prosecution than they do in relation to public safety. In the case of prosecutions, the impact of encryption is unclear, rendering the need for decryption at best debatable. But the same inference cannot be drawn about the need for decryption powers grounded in a *theoretical* case involving public safety. Here, it *is* possible to posit a case in which encrypted data forms the linchpin of a terror plot — thus calling for a closer examination of the merits of this case on its own terms.

III. National Security and the Future of the Encryption Debate

Having surveyed the contours of the debate about compelled decryption, this part of the article turns to the public safety case for new powers and shifts the focus of discussion from practice to theory. It looks at terrorism in particular (rather than law enforcement generally) and arguments premised on the ticking bomb hypothetical. Proponents of torture and other invasive measures have gravitated to arguments of this kind for at least two centuries.[113] Despite powerful critiques of the ticking bomb scenario, arguments premised upon it retain

[107] *Ibid.*

[108] *Ibid.*

[109] Justin (Gus) Hurwitz, "Encryption$^{\text{Congress}}$ mod (Apple + CALEA)" (2017) 30:2 Harv JL & Tech 355 at 401.

[110] *District Attorney New York Third Report*, *supra* note 95 at 4; see also *District Attorney New York 2016 Report*, *supra* note 35 at 7 ("[r]eports estimate that third-party data extraction on the single iPhone in the San Bernardino case cost close to one million dollars. Such an expenditure is simply not an option for the thousands of state and local law enforcement agencies throughout the United States" [footnotes omitted]).

[111] *District Attorney New York Third Report*, *ibid* at 7–9.

[112] *District Attorney New York 2016 Report*, *supra* note 35 at 7.

[113] Richard Matthews, *The Absolute Violation: Why Torture Must be Prohibited* (Montreal: McGill-Queen's University Press, 2008) at 7, notes that the scenario forms the "centerpiece" of much protorture advocacy; for examples of its use in defences of torture, including Jeremy Bentham's discussion, see Matthews, *ibid* at 68–99 and Fritz Allhoff, *Terrorism, Ticking Time-Bombs, and Torture: A Philosophical Analysis* (Chicago: University of Chicago Press, 2012) at 87–112 [Allhoff, *Terrorism*].

a basic plausibility that is difficult to refute. Thus, regardless of the abstract and practically improbable nature of these arguments, they continue to support a line of reasoning to the effect that in a situation where torture or compelled decryption are the only means of averting significant harm, they ought to be used because they advance a greater good. Arguments of this kind also retain a degree of emotional force by aligning the use of the measure at issue with the value or importance of saving many lives as opposed to protecting other sources of value, such as dignity or privacy.

This Part seeks to make four points in relation to the argument: (1) it is best understood when expressed overtly; (2) it invites powerful criticisms, but as with the argument for torture based on ticking bomb hypotheticals, it remains logically tenable and emotionally compelling; (3) it challenges claims about decryption involving a trade-off between two broad forms of security; and (4) it could readily regain purchase in the wake of an attack implicating encryption.

A. THE NATIONAL SECURITY CLAIM MADE OVERTLY

The 2016 Green Paper discussed in Part II offered an equivocal or veiled form of the argument for compelled decryption based on national security. The Paper hinted at the prospect of an imminent attack and suggested that the only means of preventing it was to access data that was encrypted. The argument is best tested when set out overtly.

Law enforcement needs a power to compel decryption because in certain cases it may be the only way to save multiple lives. For example, we might imagine a case in which a small group of actors plans a terror attack of a significant scale using communications that are encrypted end-to-end. For reasons relating to human frailty, police are tipped off. They gain knowledge of an attack that will take place shortly but are told that details can only be found on an encrypted device or line of communication. Despite their best efforts to access the information in time, police fail to do so. The attack unfolds, and several people die. Police later discover that, in the short space of time available to them, the vital information (about parties and means) was to be found in the encrypted data — and in the time available, there were no reasonable alternatives to obtaining it other than through tools by which decryption could be compelled. Had they accessed the information in time, the attack would have been averted.

At this point, I wish to highlight one simple point about the scenario: however implausible it may be, it supports the claim that law enforcement needs a power to compel decryption by showing one sense in which that power might be the only way to save lives. Below, I argue that even if the scenario does no more than establish a *possibility* that decryption powers are necessary in a case of this kind, it does something important.

B. THE CRITIQUE AND PERSISTENCE OF THE NECESSITY CLAIM BASED ON TICKING BOMB HYPOTHETICALS

Before turning to that argument, I briefly consider notable limitations and qualifications to claims based on the scenario — in relation to both torture and compelled decryption.

1. COUNTER-ARGUMENTS

a. Practical Implausibility

Opponents of torture commonly argue that the ticking bomb hypothetical involves a set of conditions that are unlikely to be found in practice.[114] They readily apply to ticking bomb encryption scenarios. As Jonathan Allen writes:

> [F]or the "ticking bomb" scenario to constitute a truly compelling case for torture, we would have to know: (a) that we are holding the right person; (b) that the person being tortured really does possess the information we need; (c) that acquiring the information the captured terrorist possesses would be very likely to put us in a position to avert a disaster, and that his accomplices haven't already adopted a contingency plan he knows nothing about; (d) that the information we obtain through torture is reliable.[115]

In practice, authorities are likely to possess "uncertainty and imperfect knowledge,"[116] and short of possessing it, they cannot be sure that torture is necessary. Conversely, as Elaine Scarry suggests, if authorities possessed certainty on the relevant points, they likely would not need to torture.[117]

Some opponents of torture go further by asserting that the ticking bomb hypothetical is not only practically implausible, but *impossible*. Richard Matthews contends "there is no possible empirical correlate to the imagined situation"[118] because when considered in any depth, its constituent elements are exposed as hopelessly vague, indeterminate, and contradictory. For example, how soon does the attack have to be to count as "imminent"? An hour, a day, a week? Where do we draw the line? Also, torture itself takes time to be effective. The sooner the attack, the less time one has to carry out effective torture.[119] These issues render the scenario "just a fantasy."[120] One might argue in response, however, that while vague or in tension, none of the elements entails a clear contradiction. Impossible here really means "exceedingly improbable."

[114] Henry Shue, "Torture" (1978) 7:2 Philosophy & Public Affairs 124 at 142–43; Michael Davis, "The Moral Justifiability of Torture and Other Cruel, Inhuman, or Degrading Treatment" (2005) 19:2 Intl J Applied Philosophy 161 at 171; Ronald Dworkin, *Is Democracy Possible Here? Principles for a New Political Debate* (Princeton: Princeton University Press, 2006) at 49–50; David Luban, "Liberalism, Torture, and the Ticking Bomb" (2005) 91:6 Va L Rev 1425 at 1442–45.

[115] Jonathan Allen, *Warrant to Torture? A Critique of Dershowitz and Levinson* (Champaign: University of Illinois at Urbana-Champaign, 2005) at 9, online: <hdl.handle.net/2142/40>, cited in Bob Brecher, *Torture and the Ticking Bomb* (Malden, Mass: Blackwell Publishing, 2007) at 31.

[116] Luban, *supra* note 114 at 1444.

[117] Elaine Scarry, "Five errors in the Reasoning of Alan Dershowitz" in Sanford Levinson, ed, *Torture: A Collection* (Oxford: Oxford University Press, 2004) 281 at 284, cited in Brecher, *supra* note 115 at 33–34.

[118] Matthews, *supra* note 113 at 98.

[119] *Ibid* at 74.

[120] Brecher, *supra* note 115 at 16:

> When we look closely at the scenario on which it is based, it turns out that it really is just a fantasy — and not merely in the sense simply of being unrealistic or far-fetched. It is a fantasy because its conditions run counter to each other.… The time and effectiveness conditions run against each other; the likelihood of accurate information is very far from certain; and the necessity which the circumstances press upon the authorities can only ever be retrospective: we cannot know in advance that we are faced with such a case.

See also Alfred W McCoy, *A Question of Torture: CIA Interrogation, from the Cold War to the War on Terror* (New York: Henry Holt and Company, 2006) at 192, describing the scenario involving "improbable, even impossible, cluster of variables," cited in Matthews, *supra* note 113 at 72.

As noted earlier, opponents of compelled decryption also embrace the implausibility argument. The hypothetical's assumptions are too simple to be "consistent with reality."[121] Real world plots are messier, knowledge is likely to be more limited, crucial issues to be unclear, such as the availability of alternatives or the certainty of success in preventing an attack by decrypting a device. Critics also cast the hypothetical as unrealistic for reasons relating to broader trends in technology, including the abundance of unencrypted data and more opportunities to gain access to encrypted data by probing the end points of communications.[122] On this view, a key premise of the hypothetical — that compelled decryption is the *only* means of obtaining information that could thwart an imminent attack — is increasingly unlikely or implausible. The ticking bomb scenario might support a moral claim, but the claim is not important or helpful to what law enforcement should focus on in the present to be effective.

b. The Hypothetical Proves Nothing about the Need for Decryption Power in Law

Marshall Erwin has been critical of law enforcement claims about the extent of the impediment that encryption poses, noting a "paradox at the heart of this debate: Because the data in question is encrypted, we will never know what necessary information has been lost to analysts and investigators.… [If the] problem is real, the FBI will never be able to furnish evidence of that fact. It will not be able to say what information it is lacking."[123] The argument readily extends to the ticking bomb hypothetical. The scenario proves nothing about the need for decryption powers because it fails to grasp the nature of the problem of proof in this instance. If the data at issue were effectively encrypted, law enforcement would not be able to access it in time to prevent the attack; if they were to access it, then encryption was not the issue. Put otherwise, the hypothetical in which police gain access to encrypted information through one tool or another *at the last minute* proves only that they were too slow (or slow but fortunately not too slow). It does not prove that they *needed* decryption powers to prevent the attack. The need for or utility of data that was effectively encrypted would not be susceptible as proof in a ticking bomb or other scenario precisely because *it would remain inaccessible*.[124]

One possible response to this argument is that the scenario is not meant to demonstrate how one might *prove* that decryption could enable law enforcement to prevent an attack they learn about shortly before it occurs. Rather, it is meant to demonstrate the logical plausibility of the assertion that, in some cases, the only way to prevent an attack is to gain access to otherwise inaccessible data. On this view, the hypothetical remains valid even if we amend the scenario to assume that the encryption was too strong for authorities to overcome in time. The mere fact that encrypted data held *the only key* to thwarting the attack is the point.

[121] *R Street Policy Study*, *supra* note 10 at 1.

[122] *Don't Panic*, *supra* note 10 at 9.

[123] Erwin, *supra* note 98.

[124] *Ibid*:

> Here is the paradox at the heart of this debate: Because the data in question is encrypted, we will never know what necessary information has been lost to analysts and investigators. Critics often press the FBI to more clearly specify the problem it is trying to solve. Indeed, I've done this myself in conversations with law enforcement colleagues. The Bureau has done a horrible job articulating what that problem is. But I've also come to realize that, if that problem is real, the FBI will never be able to furnish evidence of that fact. It will not be able to say what information it is lacking.

However, Erwin's argument points out the difficulty of *proving* the necessity for decryption *in fact*. If we were to come across a case in which an attack could not be thwarted in time, and the encrypted device did in fact contain crucial information, the case would still not support law enforcement's claim that decryption powers were *necessary*. It would prove only that law enforcement was too slow (to hack the device) or lacked ingenuity.[125]

c. The Necessity Claim Is a Red Herring; Decryption Powers Would No Longer Make a Difference

Encryption tools are now so pervasive as to be beyond the effective control of any law-making authority. Strictly speaking, this is not an argument against the hypothetical as a ground for arguing the state's *need* for decryption powers but a claim against the inference it is meant to support: that is, that states should pass laws to facilitate decryption in order to save lives. In the torture debate, the analogous argument was one contending that torture is ineffective. It produces poor, unreliable intelligence. Even if it may be necessary to torture in some theoretical or moral sense, experience suggests it will not likely be effective.[126]

In the context of encryption, commentators argue analogously that regardless of whether a moral case can be made for compelled decryption, it is practically irrelevant. States cannot enforce a power to compel decryption on a broad enough scale to be effective. As Robert Graham argues, "the 'source code' itself behind end-to-end encryption is now widely available online, which means that short of shutting down the internet, there is nothing that can be done to stop individuals, including terrorists, from creating and customizing their own encryption software."[127] Laws that the FBI and other North American police agencies call for would be "futile," since they would "not apply to software or phones created in other countries … [or] to jihadist programmers who create their own apps based on open-source software."[128] This does not render the problem of encryption insurmountable for law enforcement. It means that laws mandating decryption powers — premised on the view that the state *needs* access to decrypted information to be effective — are misguided and pointless. In Graham's view, law enforcement should instead focus on attempting to "out-smart the software" and focus on the end points rather than on the middle of communications.[129] Human error will also leave law enforcement with frequent opportunities

[125] Dworkin, *supra* note 114, makes a similar case about the ticking bomb scenario in relation to torture at 50–51.

[126] See e.g. Brecher, *supra* note 115 at 24, discussing the US Army's *Field Manual* prohibition on the "use of force" in interrogations on the basis that it is a "poor technique [that] yields unreliable results, may damage subsequent collection efforts, and can induce the source to say whatever he … thinks the interrogator wants to hear."

[127] Robert Graham, "How Terrorists Use Encryption," *CTC Sentinel* 9:6 (June 2016) 20 at 20. See also Jean-Louis Gassée, "Let's Outlaw Math" (14 December 2015), online (blog): *Monday Note* <mondaynote. com/let-s-outlaw-math-3cdcdb7d3e56> ("Try googling 'open source encryption': You'll get thousands of results, from academic papers to fully formed encryption tools. Anyone with a command of Linux can use or customize these unbreakable encryption tools").

[128] Graham, *ibid* at 25. See also Stepanovich & Karanicolas, *supra* note 11, noting

> [i]t is nearly impossible to keep people from accessing certain tools or technologies online. In 2017, Russia passed a law which banned the use of Tor, a program for facilitating anonymous, encrypted communication, but as of early 2018 there were still over 250,000 daily users of the service in Russia.… The mostly likely result of a move to introduce backdoors into tech products would be a migration by criminals and terrorists to smaller, less regulated products which could offer strong encryption without consequence.

[129] Graham, *ibid* at 25.

to exploit failures in execution, which can range from imperfect implementation of security protocols around encryption to leaving clues about physical movements or actions.[130]

2. WHY THE NECESSITY CLAIM BASED ON THE TICKING BOMB REMAINS COMPELLING

The criticisms canvassed above might be summarized by saying that the national security argument based on the ticking bomb hypothetical tells us nothing about whether law enforcement *needs* to torture or possess powers to compel decryption in either a practical or a moral sense. In practical terms, the argument does not establish that "but for" torture or decryption, harm would result since the scenario is exceedingly implausible. It permits or requires torture or compelled decryption only under "exacting conditions," namely, where law enforcement is certain that the person or encrypted data will provide the necessary information *and* the information will prevent the attack.[131] But insofar as these are unlikely to arise in practice, torture or compelled decryption are not necessary.[132] Moreover, since no national or regional law can now prevent the use of encrypted forms of communication or data created abroad, the argument does not establish that we need powers to decrypt to save lives — because they will not. Therefore, we lack a clear basis to make a moral claim for necessity.

To be clear, these are valid and persuasive arguments. They will remain vital counter-arguments in the ongoing debate about compelled decryption. The point of what follows is not to demonstrate that they are wrong or that the national security argument refutes them. The point is to demonstrate that the counter-arguments *do not refute the national security claim*. And for this reason, the national security claim will continue to spur debate.

Both counter-arguments are premised on realism. Consider the criticism of decryption being necessary in a "but for" sense. Are there cases in which compelled decryption is the only way to avoid serious harm? Critics suggest that if there are such cases, they are highly unlikely — so unlikely as not to count as proof of anything. Yet this criticism does more than simply favour a practical over a theoretical perspective. It treats the ticking bomb scenario as a premise in the argument for necessity — one that can only be valid if the scenario is likely or realistic. However, as Fritz Allhoff has suggested, the ticking bomb scenario is not the premise of an argument, but a supposition.[133] It asks us to suppose a set of facts. It becomes a premise, and the foundation for an argument, in the form of a condition: *if* a situation like this *were* to arise, torture or compelled decryption would be the only means of avoiding a grave harm; therefore, it should be used. As Allhoff notes, "the fact that [the scenario] is counterfactual cannot serve as evidence against it"; or, as he asserts:

[130] *Ibid.*

[131] Michael L Gross, "Doctors in the Decent Society: Torture, Ill-Treatment and Civic Duty" (2004) 18:2 Bioethics 181 at 191.

[132] *Ibid.*

[133] Allhoff, *Terrorism*, *supra* note 113 at 93.

"actualization is morally irrelevant."[134] The question is not whether the scenario is likely to occur, but whether it *could* occur.[135]

If there are conditions (however unlikely) in which compelled decryption or torture could be necessary to avoiding harm — in a "but for" sense — does this mean that the measures *should* be used? In other words, they may be necessary to thwarting an attack in a practical sense, but are they necessary in a moral sense? Moral theorists from at least Jeremy Bentham onward have contended that where we are certain that if we were to use a given measure — and only that measure — we could avoid serious, imminent, and otherwise inevitable harm to many people, we should do so.[136] The imperative arises from the notion that using the tool renders a greater benefit than the cost incurred in not using it.[137] The logic of the argument for torture or compelled decryption on the basis of the ticking bomb hypothetical is thus consequentialist, premised on the view that the harms entailed in using torture or compelled decryption are outweighed by the benefit of saving one or more lives.[138] In the case of torture, moral theorists have defended this line of reasoning by drawing on a range of perspectives, from utilitarianism to virtue theory.[139]

The national security claim can also be defended on consequentialist grounds against the concern that compelled decryption entails a conflict between one set of rights and another: an interest in digital privacy or security and the right to life. Put bluntly, one might wonder whether the digital security of billions should be compromised (through compelled decryption) to save a small number of lives if some real world ticking bomb scenario were to occur.[140] But here too we might imagine a scenario in which the number of lives at stake

[134] Fritz Allhoff, "A Defense of Torture: Separation of Cases, Ticking Time-Bombs, and Moral Justification" (2005) 19:2 Intl J Applied Philosophy 243 at 247.

[135] *Ibid*; Allhoff's position is premised on the view that a purely theoretical consideration is a viable or preferable context in which to consider the moral merits of torture. Matthews, *supra* note 113 at 97, argues to the contrary that to establish "a valid argument" for torture, "you have to deal with the practice, and that involves empirical reference, knowledge of history, knowledge of practical ethics, and all of the other messy details."

[136] Allhoff, *Terrorism*, *supra* note 113 at 90. Once again, opponents of torture question whether we ever could have this kind of certainty. For Brecher, *supra* note 115 at 35, because we could not be certain in any given case that torture will result in an attack being thwarted, "what we are actually being invited to accept is that interrogational torture is morally justifiable because it *might* — and … *only just might* — avoid the catastrophe." But Brecher's criticism assumes that torture is only morally justified where there is a certainly that torture will result in catastrophe being avoided. But a measure might still be morally justified (necessary) if its use in an urgent situation seems the only reasonable course of action (in the hope of sparing many lives), even it proves futile.

[137] Allhoff, *Terrorism*, *ibid*. A distinction can be drawn between torture being morally necessary or justified and it being legal. See e.g. Brecher, *supra* note 115 at 45, discussing differences between Posner and Dershowitz's positions on the morality and legality of torture. Relevant here is the moral sense, as in Michael Levin's assertion that "[t]here are situations in which torture is not merely permissible but morally mandatory" (Michael Levin, "The Case for Torture," *Newsweek* 99:23 (7 June 1982) 13).

[138] This is a contested claim: see e.g. Matthews, *supra* note 113 at 73 for the argument that the consequentialist justification for torture is premised on a "sanitization of a practice that is filthy by its nature" — by which he refers to historical and empirical evidence supporting the view that torture is never practiced in isolation from religious, political, or racial animus, or other motives distinct from considerations about saving lives.

[139] See e.g. Allhoff, *Terrorism*, *supra* note 113 at 113–38. For contrary views on the consistency of torture with various forms of consequentialism, see Matthews, *supra* note 113 at 100–37.

[140] The next section, below, canvasses opinions on why compelled decryption would compromise data security. I am indebted to Lex Gill for cautioning against drawing a simple opposition here between digital security and human lives; in some parts of the world, compromising people's digital security can directly endanger their lives. See e.g. the discussion in Gill, Israel & Parsons, *supra* note 1 at 15–16.

rises to a number high enough to make the trade-off seem worthwhile.[141] Put differently, a principled and absolute opposition to a measure such as torture or compelled decryption can only be based on a fundamental value the measure can never be justified in transgressing.[142] There may be such a value, but stacked against the value of a large number of lives, it is difficult to imagine what this would be.

The question of whether we should use a given measure in an argument based on the ticking bomb hypothetical thus engages at least two sets of values: the cost of using a given measure (torture, decryption) against the cost of the harm we seek to avoid (or the benefit we seek to gain). The assessment engages "our deepest moral commitments."[143] As Michael Gross notes, "it is important to see that any position that absolutely bans torture does so, primarily, because it weighs human dignity over human life."[144] In the torture debate, liberal jurists and bioethicists favour dignity.[145] In the encryption debate, most commentators appear to favour privacy and data security.[146] But a priority placed on different values — collective security rather than individual rights — leads to a different position on the use of torture and may do so in the case of decryption.[147] As Gross argues, "decent" societies (rather than liberal societies, pointing to Israel and to some Muslim states) place greater weight on collective over individual values. In the case of Israel: "This attitude is rooted in a religious, communitarian tradition that stems from a genuine disrespect for liberal individualism inherent in a founding ideology anchored in a national and socialist state. The deep reverence

[141] Allhoff, *Terrorism*, *supra* note 113 at 121, makes a similar point in relation to the right to be free from torture:

> We can acknowledge that not all rights violations are of equal moral significance and even, for the sake of argument, suppose that the right against torture counts more than the right to life. While I suspect that this latter supposition is false, the rights of a substantial number of people who would otherwise die militate in favor of torture. To put it another way, even if the right against torture is five times more morally valuable than the right to life, the rights of the thousands that the terrorist threatens swamp his right against torture.

[142] *Ibid* at 132.

[143] *Ibid* at 93. See also Gross, *supra* note 131 at 191–92.

[144] Gross, *ibid* at 191. See also Michael Ignatieff, *The Lesser Evil: Political Ethics in an Age of Terror* (Princeton: Princeton University Press, 2004) at 143: "For torture, when committed by a state, expresses the state's ultimate view that human beings are expendable. This view is antithetical to the spirit of any constitutional society whose raison d'être is the control of violence and coercion in the name of human dignity and freedom." *Cf* Matthews, *supra* note 113 at 27, though he argues against torture on consequentialist grounds (the certainty of the harms that flow from torture outweigh the uncertain benefits). He does not defend an *absolute* prohibition.

[145] Gross, *ibid* at 192.

[146] See e.g. Gill, Israel & Parsons, *supra* note 1 at 11–12 [footnotes omitted]:

> The right to privacy, protected by Article 12 of the Universal Declaration of Human Rights (UDHR) and Article 17 of the International Covenant on Civil and Political Rights (ICCPR), 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 ... [and] also critical to a range of other human rights, including freedom of association, and is an increasingly important precondition for many core democratic functions, from protecting the integrity of democratic elections and judicial proceedings to effective political advocacy.

See also *Universal Declaration of Human Rights*, GA Res 217A (III), UNGAOR, 3rd Sess, Supp No 13, UN Doc A/810 (1948) 71; *International Covenant on Civil and Political Rights*, 19 December 1966, 999 UNTS 171 (entered into force 23 March 1976); National Academies of Sciences, Engineering, and Medicine, *supra* note 97 at 32–35.

[147] As Michael Levin, *supra* note 137 argues:

> The most powerful argument against using torture as a punishment or to secure confessions is that such practices disregard the rights of the individual. Well, if the individual is all that important — and he is — it is correspondingly important to protect the rights of individuals threatened by terrorists. If life is so valuable that it must never be taken, the lives of the innocents must be saved even at the price of hurting the one who endangers them.

for life is perpetuated by a historic fear of national extermination and entails stubborn concern for collective well-being."[148]

The value placed on life "undermines" the thrust of the absolute prohibition on torture in the UN *Convention on Torture*,[149] even in times of war or emergency, premised as it is upon "an atomistic concern for individual well-being" that is meant to prevail over threats to the collective.[150]

Gross offers a view of why the national security argument for torture based on the ticking bomb hypothetical bears a strong resonance in Israel, given its communitarian leanings. But one need not be a communitarian, or part of a society with communitarian leanings, to agree that the ticking bomb case offers a plausible basis for the moral necessity for compelled decryption. One need only accept that since, in certain cases, compelled decryption powers *could* enable police to save lives, the state should adopt them because life is more valuable than data. Once again, opponents of compelled decryption would take issue with this. The balancing is inaccurate, they would assert; it is not a matter of life over data, but rather, the *possible* utility or benefit of decryption powers to save lives (which is so remote as to be worthless) versus the *certain* harm that compelled decryption would entail for data protection (more on this below). While the criticism is fair, attitudes to torture in the years after 9/11 suggest that for many people, the mere possibility that a certain measure might saves lives will serve as a compelling argument despite evidence that such a measure is less likely to save lives than to cause serious and unnecessary harm to specific individuals. High profile Congressional reports on the use of torture at Guantanamo Bay made clear that it was ineffective in producing actionable intelligence — along with ample other evidence calling into question the utility of torture.[151] Yet sizable portions of the US population still support it.[152] There is no reason to assume that a similar logic would not apply in the case of encryption, especially in an environment in which concerns about security are more salient than concerns are at present about privacy.

In summary, there are many persuasive arguments against the claim that law enforcement needs a power to compel decryption for national security as demonstrated by a ticking bomb hypothetical. The scenario is implausible. In practice, even if encrypted data were to form the linchpin of a terror plot, this would not prove the state needs a power to compel decryption. The whole issue might also be moot, given the wide availability of strong encryption and the likely futility of national law in many cases. One can grant that each of these arguments is valid, yet the national security argument based on the ticking bomb scenario still remains cogent *in theory* and emotionally compelling — with implications for the future of the debate.

[148] Gross, *supra* note 131 at 192.

[149] *Convention Against Torture, and Other Cruel, Inhuman or Degrading Treatment or Punishment*, 10 December 1984, 1465 UNTS 85 (entered into force 26 June 1987).

[150] Gross, *supra* note 131 at 192.

[151] On the use of torture at Guantanamo Bay, see the US, Senate Select Committee on Intelligence, *Committee Study of the Central Intelligence Agency's Detention and Interrogation Program* (Washington, DC: United States Senate, 2014), online: <fas.org/irp/congress/2014_rpt/ssci-rdi.pdf> [*Committee Study*]. On the history of the use of torture, see Matthews, *supra* note 113 at 100–38.

[152] Recent US poll data on beliefs about torture is cited below at note 166.

C. CHALLENGE TO CLAIMS THAT DECRYPTION IS PRIMARILY CONCERNED WITH SECURITY

The argument for compelled decryption based on the ticking bomb scenario challenges claims made on another front of the encryption debate: the question of what is at stake in creating backdoors or other means of compelled decryption.

A number of authorities in the field share a view on two points. Backdoors to encryption — or other means of providing for state powers to compel decryption — cannot, as a practical matter, be facilitated without compromising the security benefits of strong encryption.[153] Put otherwise, no scheme or suggestion for state decryption powers thus far tabled has overcome concerns about vulnerabilities or weaknesses the scheme would entail.[154] This question is beyond the scope of this article. Yet, as a corollary of their doubt about secure backdoors being viable, scholars and privacy advocates argue that deciding whether to grant the state powers to compel decryption entails a choice not between privacy and security, but between two forms of security.[155] As Susan Landau puts it:

> When the FBI supports exceptional access, and tech companies resist it, the FBI is not weighing the demands of security versus privacy. Rather, it is pitting questions about the efficiency and effectiveness of law enforcement against our personal, business, and national security. Instead of security versus privacy, this is an argument of security versus security. And although the FBI's goals are to improve law enforcement's ability to conduct investigations, the proposed means — weakening encryption and the security of phones — risk a far greater harm.[156]

[153] A notable expression of this view was set out in a report published in 2015 by a group of prominent cryptography and data security experts: Abelson et al, *supra* note 11 at 70 (the authors note that systems allowing for "*exceptional access*" are "unworkable in practice, raise enormous legal and ethical questions, and would undo progress on security at a time when Internet vulnerabilities are causing extreme economic harm"). See also Bruce Schneier, "The Value of Encryption" *The Ripon Forum* 50:2 (April 2016), online: <www.riponsociety.org/article/the-value-of-encryption>:

> The FBI wants the ability to bypass encryption in the course of criminal investigations. This is known as a "backdoor," because it's a way to access the encrypted information that bypasses the normal encryption mechanisms. I am sympathetic to such claims, but as a technologist I can tell you that there is no way to give the FBI that capability without weakening the encryption against all adversaries as well.

For a more recent discussion, see Gill, Israel & Parsons, *supra* note 1 at 51–57.

[154] At the time of writing, the most recent proposal to be debated is one provided by Ray Ozzie, as reported in Steven Levy, "Cracking the Crypto War" (25 April 2018), online: <www.wired.com/story/crypto-war-clear-encryption/>. A number of prominent figures in the cryptography and security community were quick to point out its flaws or to note its lack of novelty. See e.g. Bruce Schneier, "Ray Ozzie's Encryption Backdoor" (7 May 2018), online (blog): *Schneier on Security* <www.schneier.com/blog/archives/2018/05/ray_ozzies_encr.html>:

> I have no idea why anyone is talking as if this were anything new. Several cryptographers have already explained why this key escrow scheme is no better than any other key escrow scheme. The short answer is (1) we won't be able to secure that database of backdoor keys, (2) we don't know how to build the secure coprocessor the scheme requires, and (3) it solves none of the policy problems around the whole system.

See also Matthew Green, "A Few Thoughts on Ray Ozzie's 'Clear' Proposal" (26 April 2018), online (blog): *A Few Thoughts on Cryptographic Engineering* <blog.cryptographyengineering.com/2018/04/26/a-few-thoughts-on-ray-ozzies-clear-proposal/> (setting out concerns with the proposal in some detail).

[155] See e.g. Bruce Schneier, "The Value of Encryption," *supra* note 153:

> Either we build encryption systems to keep everyone secure, or we build them to leave everybody vulnerable. The FBI paints this as a trade-off between security and privacy. It's not. It's a trade-off between more security and less security. Our national security needs strong encryption.

See also Brian Barrett, "The Apple-FBI Fight Isn't about Privacy vs. Security. Don't be Misled" (24 February 2016), online: <www.wired.com/2016/02/apple-fbi-privacy-security/>.

[156] Landau, *Listening In*, *supra* note 12 at xiii.

The risk is far greater because cyber-security threats and concerns have grown exponentially in recent decades.[157] Granting law enforcement powers to compel decryption would entail a trade-off of the highly effective protection that strong encryption generally offers for the uncertain and likely limited benefits that law enforcement would gain.[158]

Although plausible, the argument rests on the state's interest in compelled decryption being defined in abstract or opaque terms. If law enforcement gains nothing more than *a degree* of effectiveness in crime prevention, then the benefits do not clearly outweigh the costs. Landau's own discussion of the issue reflects this reasoning. In the wake of the San Bernardino shootings, she asserted: "Surely the FBI could find other ways to open the phone … without making Apple undo its security protections, thus putting other phones at risk."[159] Compelled decryption here was not the only means of accessing the data, just a more convenient means. Landau makes no concession of the stakes at issue if law enforcement had failed:

> Discussion raged for weeks. Which approach offers more security? Forcing Apple to undo the protections the company had carefully designed for the iPhone? Or leaving these protections in place, potentially not accessing the terrorists' communications, but leaving everyone else's phone secure? Then, after having testified in court and in Congress that only Apple could undo the phone's security protections, the FBI had a surprise announcement. Law enforcement didn't need Apple's help after all; a contractor had found a way to unlock the phone.[160]

In Landau's telling, the FBI was simply crying wolf. The case demonstrated that compelled decryption was not necessary in either a practical or a moral sense. The phone could be hacked. If it could not be hacked, nothing appeared to turn on it.

Yet if the phone had contained data about other parties or other plots and a third party had not manage to access it, much could have turned on it. Setting aside for the moment issues of likelihood or proof, entertaining this counterfactual entails a kind of ticking bomb hypothetical. In this case, the balance to be struck in granting police powers of compelled decryption is not one between law enforcement efficacy in a broad or vague sense and data security, but between data security and several people's lives.

Once again, this does not refute the claim that compelled decryption entails a trade-off between two forms of security. But it challenges its accuracy. We plausibly describe the values we must balance in considering compelled decryption in terms of two forms of security, in a broader sense, so long as we assume such powers will only serve to make police more efficient to some degree. But when we come to associate compelled decryption with the more tangible and pressing value of saving lives — possibly through a future terror attack more directly implicating encryption — we contemplate a different trade-off.

[157] *Ibid*. See also Abelson et al, *supra* note 11 at 70–73.

[158] Gill, Israel & Parsons, *supra* note 1 at 92:

> 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.

[159] Landau, *Listening In*, *supra* note 12 at x–xi.

[160] *Ibid* at xi.

IV. CONCLUSION

This article has sought to use the 2016 Green Paper as a basis for examining the contours of the broader debate about powers to compel third parties to assist with decryption. The debate is unfolding on at least two fronts. One asks whether the state needs to possess powers to compel decryption. The other asks whether it can possess these powers without compromising the benefits of strong encryption. On the first front, law enforcement relies on two distinct grounds to make its case — justice and national security — but often fails to distinguish them. Opponents of compelled decryption argue persuasively against the justice argument. Police and prosecutors do not require a power to compel third parties to decrypt in order to obtain convictions because they have no pressing time constraints and ample other sources of data on which to draw. Opponents are less persuasive in response to the public safety argument. The public safety case for compelled decryption tends to be grounded on one form or another of the ticking bomb scenario, and the scenario is indeed implausible and unrealistic — but this critique fails to grasp why the argument has enduring force. It continues to be invoked due in part to the difficulty of dispelling the *possibility* that in some cases, in theory, compelling a party to decrypt may be the only way to save many lives.

The enduring force of this argument is relevant to the future of the encryption debate in two ways. One is that it undermines the attempt on the part of security experts to frame the debate in terms of a trade-off between data protection and public safety in a broad, abstract sense. It offers a competing and more provocative framing of the issue as one between data protection (privacy, dignity, individual liberty) and life itself. In a political and cultural climate in which privacy concerns are prevalent, this framing has not gained purchase. But in a different climate, it might.

This points to a second implication: the impact a terror attack involving encryption would have on the debate about the need for powers to compel decryption. Writing in 2014, two American jurists, Jamil Jaffer and Daniel Rosenthal, expressed the concern that terrorists are known to be making use of encryption and "continue to plot significant, mass casualty attacks against the United States and our allies."[161] They saw a "significant possibility that a major terrorist attack, planned using encrypted communications and likely more deadly than the recent horrific attacks in Paris and San Bernardino, will take place in the United States or Europe."[162] As with 9/11, the climate of fear in the wake of such an event would leave "little opportunity for any meaningful dialogue between the technology sector, advocacy groups, and the government to work together to find a sensible solution."[163]

In such a climate, it is also likely that the ticking bomb scenario would become a central motif in government rhetoric about encryption. Public and scholarly positions in the debate over compelled decryption would also likely shift — as was the case with torture in the

[161] Jamil N Jaffer & Daniel J Rosenthal, "Decrypting Our Security: A Bipartisan Argument for a Rational Solution to the Encryption Challenge" (2016) 24:2 Catholic UJL & Technology 273 at 278.

[162] *Ibid.*

[163] *Ibid.*

decade after 9/11.[164] The ticking bomb torture scenario became a pervasive motif in popular representations of terrorism,[165] and much of the US electorate continues to support the use of torture.[166] However unrealistic or implausible the ticking bomb encryption scenario may be in practice, it could readily furnish the basic frame in which much of the public perceives the issue of whether to compel decryption. A better understanding of the ticking bomb encryption argument may prove useful in efforts to work out sensible solutions to the problems that encryption poses for the rule of law.

[164] Robert Diab, *The Harbinger Theory: How the Post-9/11 Emergency Became Permanent and the Case for Reform* (Oxford: Oxford University Press, 2015) at 127–88, discussing Ignatieff, *supra* note 144; Dworkin, *supra* note 114; Bruce Ackerman, *Before the Next Attack: Preserving Civil Liberties in an Age of Terrorism* (New Haven: Yale University Press, 2006); Alan M Dershowitz, *Preemption: A Knife That Cuts Both Ways* (New York: WW Norton & Company, 2006); Richard A Posner, *Not a Suicide Pact: The Constitution in a Time of National Emergency* (Oxford: Oxford University Press, 2006); John Yoo, *War by Other Means: An Insider's Account of the War on Terror* (New York: Atlantic Monthly Press, 2006).

[165] Diab, *ibid* at 112–13.

[166] Alec Tyson, "Americans Divided in Views of Use of Torture in U.S. Anti-Terror Efforts" (26 January 2017), online (blog): *Pew Research Center* <www.pewresearch.org/fact-tank/2017/01/26/americans-divided-in-views-of-use-of-torture-in-u-s-anti-terror-efforts/> ("[o]verall, 48% say there are some circumstances under which the use of torture is acceptable in U.S. anti-terrorism efforts"); Chris Kahn, "Exclusive: Most Americans Support Torture Against Terror Suspects - Reuters/Ipsos Poll," *Reuters* (30 March 2016), online: <www.reuters.com/article/us-usa-election-torture-exclusive/idUSKCN0WW0Y3> ("[n]early two-thirds of Americans believe torture can be justified to extract information from suspected terrorists, according to a Reuters/Ipsos poll"); Somini Sengupta, "Torture Can be Useful, Nearly Half of Americans in Poll Say" *The New York Times* (5 December 2016), online: <www.nytimes.com/2016/12/05/world/americas/torture-can-be-useful-nearly-half-of-americans-in-poll-say.html> (a poll conducted by the International Committee of the Red Cross found that "[n]early half of Americans in a global survey said they believed an enemy fighter could be tortured to extract information").