IP, Encryption, and the Threat to Public Safety

MATT MALONE

I. INTRODUCTION

Law enforcement agencies in liberal democracies increasingly assert the proliferation of end-to-end encryption is a major threat to public safety.[1] In the criminal justice context, such assertions — and related assertions about the need to embed vulnerabilities in end-to-end encryption for investigative and evidentiary purposes — overlook the necessity of encryption for the protection of intellectual property (IP). This paper makes a doctrinal critique of these calls by law enforcement. Although hardly new,[2] these calls require reconsidered attention as end-to-end encryption becomes an increasing mainstay of the infrastructure of digital communications.[3] End-to-end encryption renders communications "unreadable except to a person who has the key to decrypt it into readable form… all the way from sender to receiver."[4] While government and law enforcement have long utilized end-to-end encryption for their own purposes, this technology is now being disseminated pervasively, such that it has become a fact of life for average

---

1 For example, following the Charlie Hebdo attacks in Paris in January 2015, the UK Prime Minister David Cameron called for a ban on end-to-end encryption. See Jonathan L. Zittrain et al, "Don't Panic: Making Progress on the 'Going Dark' Debate" (2016) at 8, online (pdf): *Berkman Center Research Publication* <dash.harvard.edu/bitstream/handle/1/28552576/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf?sequence=1&isAllowed=y> [perma.cc/B3QG-6TE6].

2 See Solomon Friedman, "PGP & Encrypted Communication" (Paper delivered at the 29th Annual Criminal Law Conference, 14 October 2017), online: <canlii.ca/t/srhp> [perma.cc/8AJW-MZRB].

3 For example, following the bombing of the Alfred P. Murrah Federal Building in 1995, the Clinton Administration called for the creation of backdoors to encrypted telecommunications. See Michael A. Froomkin, "It Came from Planet Clipper: The Battle Over Cryptographic Key 'Escrow'" (1996) U Chicago Leg Forum 15. For an overview of historical efforts see Friedman, *supra* note 2.

4 "What Should I Know About Encryption?" (last modified 24 November 2018), online: *Electronic Frontier Foundation* <ssd.eff.org/en/module/what-should-i-know-about-encryption> [perma.cc/7LMQ-3DPD].

users and an important default in many communication systems,[5] from iMessage[6] to FaceTime[7] to WhatsApp.[8] In response to this state of affairs, law enforcement bodies have identified challenges to criminal investigation and prosecution and have called for access to such communications "in limited circumstances where necessary and proportionate" by embedding vulnerabilities that allow for circumvention of the technology.[9] Some legislative actors have even proposed statutory interventions aimed at dismantling and forestalling the spread of end-to-end encryption in such technologies.[10]

These calls from law enforcement have been the subject of vociferous critique, largely centered on concerns of data insecurity, privacy, and threats to human rights, due process, and fundamental principles of law.[11] They

---

5 Stephanie K. Pell & Christopher Soghoian, "Your Secret Stingray's No Secret Anymore: The Vanishing Government Monopoly over Cell Phone Surveillance and Its Impact on National Security and Consumer Privacy" (2014) 28:1 Harvard JL & Technology 1.

6 "Apple Privacy Policy" (last modified 27 October 2021), online: *Apple* <www.apple.com/legal/privacy/en-ww/> [perma.cc/WEZ9-APQ4].

7 *Ibid.*

8 "About end-to-end encryption", online: *Whatsapp* <faq.whatsapp.com/general/security-and-privacy/end-to-end-encryption/?lang=en> [perma.cc/22JU-YB4B].

9 Office of Public Affairs, "End-to-End Encryption and Public Safety" (11 October 2020), online: *The United States Department of Justice* <www.justice.gov> [perma.cc/82PT-EY29] ["International Statement"]. The nomenclature of embedded vulnerabilities is complex, with the notion variously being referred to as "backdoors." For consistency, this paper simply refers to embedded vulnerabilities.

10 See US, Bill S 4501, *Lawful Access to Encrypted Data* Act, 116th Congress, 2019–2020.

11 For example, in the Canadian context, Steven M. Penney and Dylan Gibbs have argued that calls for "exceptional access" create too great a risk of data insecurity to justify the benefits. See Steven Penney & Dylan Gibbs, "Law Enforcement Access to Encrypted Data: Legislative Responses and the *Charter*" (2017) 63:2 McGill LJ 201. Christopher Parsons and Tamir Israel support a similar argument. See Tamir Israel & Christopher Parsons, "Government's encryption proposal will undermine public safety", *Toronto Star* (28 August 2019), online: *Toronto Star* <www.thestar.com/opinion/contributors/2019/08/28/governments-encryption-proposal-will-undermine-public-safety.html> [perma.cc/8PHP-3EU6] [Israel & Parsons, "Encryption Proposal"]. See also Christopher Parsons, "Canada's New and Irresponsible Encryption Policy: How the Government of Canada's New Policy Threatens Charter Rights, Cybersecurity, Economic Growth, and Foreign Policy" (2019), online: *Citizen Lab* <citizenlab.ca> [perma.cc/KH3H-8ZCR]; Tamir Israel & Christopher Parsons, "Shining a Light on the Encryption Debate: A Canadian Field Guide" (2018), online: *Citizen Lab* <citizenlab.ca/2018/05/shining-light-on-encryption-debate-canadian-field-guide/> [perma.cc/PWC7-UANE].

rarely invoke explicitly the protection of IP. This comment supplements these critiques by offering a perspective centered on the connection between the proliferation of end-to-end encryption and its importance in protecting IP (in particular, trade secrets and confidential information, which are highly reliant on encryption). This paper argues embedded vulnerabilities pose a fatal threat to IP and, by extension, to public safety. It takes as a starting point the growing understanding by law enforcement that the protection of IP is a national security issue. It then points to a confusion in law enforcement's recognition of encryption as vital to protecting these assets — while many law enforcement bodies call for its circumvention. Ultimately, the paper argues such calls undermine the maintenance of public safety by endangering these assets.

The argument is grounded in a reading of the joint statement "End-To-End Encryption and Public Safety" (the "International Statement") released on 11 October 2020, which exhorted private actors in the technology industry to provide law enforcement with access to such communications "in limited circumstances where necessary and proportionate."[12] The International Statement was signed by top-ranking law enforcement officials in seven countries, including Canadian Public Safety Minister Bill Blair.[13] At the outset, it is important to note this comment does not tackle the merits of any technical proposition that it is (or is not) possible to create embedded vulnerabilities. The essay effectively treats encryption as a "static" concept in the same manner as the International Statement, delving into neither scenarios where it is invoked for marketing or advertisement purposes nor those where it is presented as an evolving litmus in the evolution of decryption. It also does not cast doubt on the sincerity of law enforcement bodies to effectuate their responsibilities to protect public safety and does not explore the efforts that have been conducted to examine how advertising-reliant business models, which are common throughout social media, might serve as natural guardrails on the use of default end-to-

---

12 "International Statement", *supra* note 9. Embedded vulnerabilities nomenclature is complex, with the notion variously being referred to as "backdoors." For consistency, this paper simply refers to embedded vulnerabilities.

13 Signatories included top-ranking law enforcement officials from the "Five Eyes" (i.e., the United States, the United Kingdom, Australia, Canada, and New Zealand) as well as India and Japan. The change in Canadian policy was initially announced by then-Public Safety Minister Ralph Goodale, who previously supported the widespread use of end-to-end encryption. See Israel & Parsons, "Encryption Proposal", *supra* note 11; "International Statement", *supra* note 9 [signed by Public Safety Minister Bill Blair].

end encryption.[14] Instead this paper focuses solely on the arguments propounded in the International Statement to support law enforcement bodies' call for access, drawing out the assumptions about IP, secrecy, and public safety upon which they stand, and the connections between them. In doing so, it is does not confront objections based on an indiscriminate entitlement from the state through its law enforcement bodies to "access any information at any time."[15] Under such a view, whether the justifications proffered to support the calls for access are accurate, persuasive, or grounded in any real connection with public safety is irrelevant.[16] This paper presumes the justifications propounded by law enforcement are sincere, affecting and shaping citizen behavior; public, legislative, and lawful discourse; and the decision-making processes of affected stakeholders.

II. The International Statement

Raising concern about challenges to public safety posed by the proliferation of end-to-end encryption as a default in communication technologies, the International Statement called for the creation of "mutually agreeable solutions" with companies in the technology industry to facilitate "[t]he ability of law-enforcement agencies to protect victims in the public at large."[17] Released during the U.S. government's Cybersecurity & Infrastructure Security Agency's "National Cybersecurity Awareness Month,"[18] the International Statement was seen as a call to Big Tech to adopt more cooperative approaches with national security entities in the

---

14 By this argument, the business model of many companies necessitates that a lot of data remain unencrypted, since targeted advertising — the lynchpin of the model for many social network companies — requires certain data to facilitate reaching narrow audiences. For more on this point, see Zittrain et al, *supra* note 1 at 3, 10.

15 "International Statement", *supra* note 9.

16 James B. Comey, "Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?", *FBI News* (16 October 2014), online: <www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course> [perma.cc/LUH8-4HG9].

17 "International Statement", *supra* note 9.

18 See "National Cybersecurity Awareness Month" (last visited 13 February 2022), online: *Cybersecurity & Infrastructure Security Agency* <www.cisa.gov/cybersecurity-awareness-month> [perma.cc/VR4W-3H36].

interception of communications.[19] In the International Statement, the signatories noted that they "challenge the assertion that public safety cannot be protected without compromising privacy or cyber security" – albeit without providing any blueprint for the sought-after compromise.[20] The International Statement highlighted the investigatory and prosecutorial challenges associated with certain types of crimes, such as the sexual exploitation of children, organized crime, and terrorism.[21] However, few agree on the scope of the problem posed by encryption to law enforcement in the execution of its duties.[22]

As indicated at the outset, this paper is focused on the International Statement's import for IP. In particular, this paper focuses on trade secrets and confidential information – information-based assets that are not widely known, that have value from not being widely known, and that have been the subject of reasonable steps to maintain and continue their secrecy. Law enforcement understands the importance of these forms of IP, and in particular their relationship with encryption, as is made clear in the International Statement's opening salvo: "[w]e, the undersigned, support strong encryption, which plays a crucial role in protecting personal data, privacy, intellectual property, trade secrets and cyber security."[23] Despite this preamble, a true belief in the importance of these assets has been wanting in Canada for some time. This is partly because the country's economy has historically hinged on commodity security based on physical

---

19 Hirsh Chitkara, "A transnational coalition of intelligence agencies seeks to abolish end-to-end encryption" (13 October 2020), online: *Business Insider* <www.businessinsider.com/intelligence-agencies-seek-to-abolish-end-to-end-encryption-2020-10> [perma.cc/7BST-ZHV2].

20 "International Statement", *supra* note 9.

21 These threats are essentially tantamount to the Four Horsemen of the Infocalypse that were enumerated by Timothy May, quoting Sandy Sanfort, in his *Cyberphunk FAQ* in 1994 when he described the "[s]cenario for a ban on encryption" as likely to be motivated by law enforcement's concern about the use of the technology by terrorists, drug dealers, pedophiles, and organized crime. See Timothy C. May, "Scenario for a Ban on Encryption" (10 September 1994), online: *Cyberpunk FAQ* <koeln.ccc.de/archiv/cyphernomicon/chapter10/10.4.html> [perma.cc/Q55T-8422]. Also, in 2019, then-Public Safety Minister Ralph Goodale highlighted both issues in calling for the need to embed vulnerabilities in encrypted communications systems. See Israel & Parsons, "Encryption Proposal", *supra* note 11

22 Zittrain et al, *supra* note 1 at 2.

23 "International Statement", *supra* note 9 [emphasis added].

assets.[24] Originally a staples economy based on fish, fur, timber, and wheat, today only 9.2% of Canada's GDP remains linked to natural resources, with most value now existing in goods that are intangible.[25] Canada is still developing a defence and security mindset that takes seriously the protection of intangible assets. For example, the Canadian Centre for Cyber Security's reporting system for reporting cybercrime advises "[i]f you believe a cyber incident is an imminent threat to life or of a criminal nature, please contact your local police services."[26] However, the RCMP National Cybercrime Coordination Unit's maze-like reporting system (still in pilot-testing) does not enable such reporting and will only "reach full operating capability in 2024."[27] The Ontario Provincial Police online crime reporting tool, which is limited to reporting certain crimes, does not mention cybercrime or criminal theft of IP.[28] Canada's counterparts in the United States,[29] the United Kingdom,[30] and Australia[31] all have robust reporting mechanisms for theft, including theft of intangibles. Although a seemingly discrete point, these mechanisms for protecting IP matter greatly since IP is the key form of protection of many intangible assets.

---

24 The seminal trade secrets case in Canada — *Lac Minerals Ltd v International Corona Resources Ltd*, [1989] 2 SCR 574, 61 DLR (4th) 14 [*Lac Minerals*] — involved the mining industry.

25 Statistics Canada, *Natural resource indicators, fourth quarter 2020*, Catalogue No 11-001-X (Ottawa: Statistics Canada, 2021).

26 "Report a cyber incident" (last modified 21 February 2022), online: *Canadian Centre for Cyber Security* <cyber.gc.ca/en/incident-management>.

27 "The National Cybercrime Coordination Unit (NC3)" (last modified 3 December 2021), online: *Royal Canadian Mounted Police* <www.rcmp-grc.gc.ca/en/the-national-cybercrime-coordination-unit-nc3> [perma.cc/835Z-TTXY].

28 "Report a Crime" (last visited 13 February 2022), online: *Ontario Provincial Police* <www.opp.ca/index.php?id=132> [perma.cc/835Z-TTXY].

29 US, Department of Justice, "Report a Crime" (last modified 3 February 2022), online: <www.justice.gov/actioncenter/report-crime> [perma.cc/67E5-S85F].

30 "Reporting Fraud and Cyber Crime" (last visited 13 February 2022), online: *ActionFraud* <www.actionfraud.police.uk/reporting-fraud-and-cyber-crime> [perma.cc/W5AP-LS92].

31 "ReportCyber" (last visited 13 February 2022), online: *Australian Cyber Security Centre* <www.cyber.gov.au/acsc/report>.

III. Trade Secrets and Encryption

It is a constituent element of trade secrecy and confident information protections that the party seeking to invoke those protections undertake reasonable steps to maintain secrecy. In Canada, trade secrets and confidential information are principally covered through the civil instrument of the breach of confidence, which describes this requirement as establishing "the necessary quality of confidence."[32] As well, a recent amendment to the *Criminal Code of Canada* now criminalizes misappropriation of trade secrets, incorporating a similar requirement that the subject matter be the focus of "efforts that are reasonable under the circumstances to maintain its secrecy."[33] The *Security of Information Act*, which penalizes theft of trade secrets by foreign actors, likewise stipulates that a trade secret is only a trade secret where it "is the subject of efforts that are reasonable under the circumstances to maintain its secrecy."[34]

But what is reasonable under the circumstances? Although there is no particular action guaranteeing a given subject matter such status, the Canadian Intellectual Property Office, in its guidance for the public on how to acquire such status, advises several best practices: use of non-disclosure agreements, confidentiality clauses, password protection, lock and key, and

---

[32] See *Lac Minerals Ltd*, *supra* note 24. This case imported the test for the breach of confidence from *Coco v AN Clark (Engineers) Ltd*, [1969] RPC 41 (Ch) at 47, where Justice Megarry (as he then was) put it as follows: "[i]n my judgment, three elements are normally required if, apart from contract, a case of breach of confidence is to succeed. First, the information itself, in the words of Lord Greene, M.R. in the Saltman case on page 215, must 'have the necessary quality of confidence about it.' Secondly, that information must have been imparted in circumstances importing an obligation of confidence. Thirdly, there must be an unauthorized use of that information to the detriment of the party communicating it." See also WTO, *Agreement on Trade-Related Aspects of Intellectual Property Rights*, art 39, 2(c), online (pdf): WTO <www.wto.org/english/docs_e/legal_e/27-trips.pdf> [perma.cc/HW8N-MXVB]: "so long as such information… has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret." See *United States-Mexico-Canada Agreement*, art 20.72(b) states that "trade secret" "means information that … has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret."

[33] *Criminal Code*, RSC 1985, c C-46, s 391(5)(c).

[34] *Security of Information Act*, RSC 1985, c O-5, s 19(4)(d). The act was amended through the *Anti-terrorism Act*, SC 2001, c 41.

significantly, encryption.[35] The United States Patent and Trademark Office has issued similar guidance, emphasizing the importance of encryption for trade secrets.[36] The US Department of Justice manual for district attorneys providing instruction on prosecuting IP crimes specifically includes encryption on a checklist for determining whether subject matter are trade secrets,[37] as does the Department's victim-focused manual for *Reporting Intellectual Property Crime*.[38] Also, the US Cybersecurity & Infrastructure Security Agency advocates, in its public-facing "tips" series, "to add an additional layer of security to sensitive information" through encryption, so as to ensure "that the data can only be read by the person who is authorized to have access to it."[39] Further, countless bar organizations, in their requirements on attorneys to exercise reasonable care in the handling of client information, explicitly mention encryption.[40] In Canada, the Canadian Centre for Cyber Security recommends encyrption as a basic

---

35 "How do you keep trade secrets secret?" (last modified 19 March 2021), online: *Government of Canada* <www.ic.gc.ca/eic/site/cipointernet-internetopic.nsf/eng/wr03987.html> [perma.cc/5C72-SHL8].

36 "Trade Secrets Protection in the U.S." (last visited 13 February 2022), online (pdf): *United States Patent and Trademark Office* <www.nist.gov/system/files/documents/mep/marinaslides.pdf> [perma.cc/6VVS-8567].

37 US, Department of Justice, *Prosecuting Intellectual Property Crimes*, 4th ed (Office of Legal Education Executive Office for United States Attorneys, 2013) at 461 [DOJ, *Intellectual Property Crimes*].

38 US, Department of Justice Criminal Division, "Reporting Intellectual Property Crime: A Guide for Victims of Copyright, Infringement, Trademark Counterfeiting, and Trade Secret Theft" (last visited 13 February 2022) at 22, online (pdf): <www.justice.gov/criminal-ccips/file/891011/download> [perma.cc/ZDV5-WGYQ].

39 See "Security Tip (ST04-019): Understanding Encryption" (last modified 27 September 2019), online: *Cybersecurity & Infrastructure Security Agency* <us-cert.cisa.gov/ncas/tips/ST04-019> [perma.cc/SLV2-QN66].

40 For example, "#2012-13/04: The Use of Cloud Computing in the Practice of Law" (21 February 2013), online: *New Hampshire State Bar Association* <www.nhbar.org/ethics/opinion-2012-13-04> [perma.cc/JX8C-HHLZ]; "09-04: Confidentiality, Maintaining Client Files, Electronic Storage, Internet" (2009), online: *Arizona State Bar Association* <www.azbar.org/for-lawyers/ethics/ethics-opinions/> [perma.cc/4LV2-GRUB]. US, Standing Committee on Professional Responsibility and Conduct, *Formal Opinion No 2010-179* (California: The State Bar of California, 2010); US, Committee on Ethics and Practice Guidelines, *Ethics Opinion 11-01: Use of Software as a Service – Cloud Computing* (Iowa: The Iowa State Bar Association, 9 September 2011).

measure of conducting business in the country.[41] In short, encryption is a vital method of garnering trade secret protection for most digital subject matter and a common tool to ascribe digital subject matter such status.[42] Sonia Katyal has written compellingly that the "code is largely dominated by trade secrecy,"[43] to such a degree that it has become the "default avenue for protection."[44] In an economic environment where so much wealth is concentrated in algorithms, data, and software, encryption has risen in importance.[45] Importantly, without encryption a party may not be able to argue they undertook the necessary "reasonable steps" to treat the subject matter like a trade secret — obviating the possibility of such legal protection in the event of misappropriation. This point is all the more significant as the preferred modalities of IP protection pivot from traditional forms of "hard" IP like patents, towards "soft" ones like trade secrets. Moreover, as disputes over IP internationalize, adequate patent protection is seen as challenged by requiring sophisticated strategy, execution, and maintenance across multiple jurisdictions.[46] The costs and timelines associated with acquiring patent protection in this paradigm prevents smaller actors "from executing an IP protection plan with the same sophistication as their larger

---

41 "Baseline Cyber Security Controls for Small and Medium Organizations V1.2" (February 2020) at s 3.7, online (pdf): *Canadian Centre for Cyber Security* <cyber.gc.ca/sites/default/files/publications/Baseline.Controls.SMO1_.2-e20.pdf>.

42 See *ConFold Pac Inc v Polaris Indus*, 433 F 3d 952 at 959, 959 (7th Cir 2006): "[a] trade secret is really just a piece of information (such as a customer list, or a method of production, or a secret formula for a soft drink) that the holder tries to keep secret by executing confidentiality agreements with employees and others and by hiding the information from outsiders by means of fences, safes, encryption, and other means of concealment, so that the only way the secret can be unmasked is by a breach of contract or a tort."]

43 Sonia Katyal, "The Paradox of Source Code Secrecy" (2019) 104 Cornell L Rev 1183 at 1189.

44 *Ibid* at 1191.

45 This is especially true as entities from start-ups to Fortune 500 companies to governments make use of the communications technologies such as Zoom, iMessage, Slack, and Signal to facilitate their communications. The author of this paper observed during two years as an employment attorney in Silicon Valley executive members of several Fortune 500 companies, make recourse to such communications technologies as they conducted, shared, and disseminated and discussed trade secrets.

46 The golden standard of protection has long been seen as involving filing and registering in the United States, Europe, and Japan. However, even the strength of this nation- and regional-based approach is called into question by the mobility of intangible assets.

commercial counterparts."[47] With trade secrets offering a more flexible alternative, and a wider and longer array of protection, the focus turns towards identifying the administrative, legal, and technological measures sufficient to gain such protections. Among those, encryption is a key technological measure.

IV. Rethinking IP and Public Safety

As stated above, IP is increasingly perceived as a national security question. In the United States, theft of trade secrets by private actors has been punishable as commercial espionage since 1996, separate and apart from economic espionage conducted by, or at the direction of or the benefit for, a foreign entity.[48] Unlike in Canada, the Federal Department of Justice in the United States has taken a very aggressive position on prosecuting criminal theft of IP — one that overtly and directly links such instances of theft with harms to the state. Prosecutorial guidelines advise attorneys general:

> The criminal enforcement of IP rights plays a critical role in safeguarding U.S. economic and national security interests ... our national security interests can be undermined by foreign and domestic competitors who deliberately target leading U.S. industries and technologies to obtain sensitive trade secrets that have applications in defense, security, or critical infrastructure.[49]

When Republican Utah Senator Orrin Hatch introduced the *Defend Trade Secrets Act*, a federal overhaul of the existing trade secrets law that created a federal private right of action — removing many of the procedural hurdles created by the existing state-only rights of action — national security was invoked as the basis for the law.[50] During its debate in Congress, the bill was extolled for its power to "help U.S. competitiveness, job creation, and our nation's future economic security."[51] Much of this discourse was

---

47 Matt Malone, "Criminal Enforcement of Trade Secret Theft: Strategic Considerations for Canadian SMEs" (2020) 10:11 Technology Innovation Management Rev 40 at 40.

48 See 18 USC § 1831.

49 See also DOJ, *Intellectual Property Crimes*, *supra* note 37 at 2.

50 Lauren Rayner Davis, "Secrecy for the Sake of It: The Defend Trade Secrets Act" (2017) 83:1 Brook L Rev 359.

51 US, *Congress Rec*, vol 162, 65 at H2028 (2016).

tailored towards the threat to American jobs presented by IP theft and addressing the fact trade secrets were the only type of IP not covered by any civil federal law.[52] As well, the Computer Crime and Intellectual Property (CCIPR) Section of the Federal Department of Justice, a 40-attorney strong unit, is given the mandate to:

> [A]dvise federal prosecutors and law enforcement agents; comment upon and propose legislation; coordinate international efforts to combat computer crime; litigate cases; and train all law enforcement groups. Other areas of expertise possessed by CCIPR attorneys include encryption, electronic privacy laws, search and seizure of computers, e-commerce, hacker investigations and intellectual property.[53]

In this paradigm, where IP is viewed as the object of a potential attack, IP is construed as nothing less than the assets of the nation — albeit possessed by private actors.[54] Although such an understanding is explicit in the language of the International Statement — and in the widely-remarked comments to the Canadian business community by Canadian Security and Intelligence Service Director David Vigneault when he noted "the greatest threat to our prosperity and national interest"[55] is economic espionage, in particular of IP — Canada has few prosecutions to demonstrate it takes this concern seriously.

This state of affairs carries important consequences for national security. Many in the national security community witnessing these costs have seized on this concern to advocate for an acceleration in cyber security online — even as they argue out of the other side of their mouth for technologies that circumvent end-to-end encryption. In effect, this is what the International Statement itself does. Yet others such as Bruce Schneier have concluded, in terms of the traditional national security apparatuses in most liberal democracies, that the security of communications online

---

52 *Ibid.* See Rep. Collins noting that "[t]rade secrets theft jeopardizes our economic security and threatens jobs."

53 "Computer Crime and Intellectual Property Section" (last visited 13 February 2022), online: *United States Department of Justice* <www.justice.gov> [perma.cc/5XMM-VNP6].

54 Bruce Schneier, *Beyond Fear: Thinking Sensibly about Security in an Uncertain World* (New York: Copernicus Books, 2003) at 13 [Schneier, *Beyond Fear*].

55 *Remarks by Director David Vigneault at the Economic Club of Canada* (Speech) (Toronto: Canadian Security Intelligence Serve, 4 December 2018), online: *Canadian Security Intelligence Service* <www.canada.ca/en/security-intelligence-service/news/2018/12/remarks-by-director-david-vigneault-at-the-economic-club-of-canada.html> [perma.cc/BMU6-HC3H].

should trump signals intelligence conducted by law enforcement — effectively privileging the diffusion of end-to-end encrypted technology.[56] "Instead of working to deliberately weaken security for everyone," he writes, "the NSA should work to improve security for everyone."[57] In other words, the efforts of law enforcement to gain access to communications via their calls for legislative and technical reform in the realm of end-to-end encryption has downplayed the degree to which encryption serves as the principal bulwark for protecting IP, having deleterious effects on national security for this same reason. Thwarting end-to-end encryption with the use of embedded vulnerabilities would do no less than pose a significant and critical threat to this bulwark. Bruce Schneier's famed observation – namely, actions taken to ensure security often have the opposite effect, in terms of making people feel secure even when the opposite is true[58] – is precisely what embedded vulnerabilities promise to achieve. As the former general counsel of the FBI during the time of its dispute with Apple over access to the San Bernardino shooter's phone has now conceded five years later: "in order to execute fully their responsibility to protect the nation from catastrophic attack and ensure the continuing operation of basic societal institutions, public safety officials should embrace encryption."[59] His change of mind was instigated, he noted, by observing networks in today's world operate in an environment that can be characterized as zero-trust. Cybersecurity in liberal democracies has not acknowledged the degree to which a poor cyber health posture in this zero-trust environment has allowed China in particular, to engage in "wanton looting" of IP in liberal democracies.[60]

---

56 Bruce Schneier, "It's Time to Break Up the NSA", *CNN* (last modified 20 February 2014), online: <www.cnn.com/2014/02/20/opinion/schneier-nsa-too-big/index.html > [perma.cc/6DVB-TPEM].

57 *Ibid*.

58 Schneier, *Beyond Fear*, *supra* note 54.

59 Jim Baker, "Rethinking Encryption" (22 October 2019), online (blog): *Lawfare* <www.lawfareblog.com/rethinking-encryption> [perma.cc/Z93P-ZDNN].

60 *Ibid.* In his view, without cyber-security, there simply is no security — words that have been noted by Chinese President Xi Jinping himself: "[W]ithout cybersecurity, there is no national security." See Rogier Creemers, Paul Triolo & Graham Webster, "Translation: Xi Jinping's April 20 Speech at the National Cybersecurity and Informatization Work Conference" (30 April 2018), online (blog): *New America* <www.newamerica.org> [perma.cc/JJE9-4MP7].

In an ideal environment, governments would lead by display and demonstration in establishing norms for cybersecurity. Yet governments in liberal democracies have shown repeated incompetence in safeguarding data, whether it is protecting the judiciary from cyber-attacks (undermining private actors' willingness to share confidential information necessary to the dispute of resolutions),[61] or to safeguard critical infrastructure itself.[62] In Canada, such cyberattacks against government, post-secondary institutions, and hospitals, as well as core infrastructure occur with increasing regularity.[63] A failure to lead by example has rendered a situation where many do not trust the government with their data, which partly motivates public resistance to law enforcement bodies' calls for embedded vulnerabilities in the first place. To be sure, there are other areas of research and reform that call out for invitation. For example, one of the primordial considerations for law enforcement in the encryption debate is access to data, and yet such bodies rarely intervene in the discussion around trade treaties to express concern over the impact of data portability provisions. Similarly, thinking through where and how liability is assigned for data breaches may also balance some of the concerns of law enforcers' desire to access with citizens' desire for privacy, as it may encourage private sector actors to offer better protections. But as the end-to-end encryption debate rages in its current form as epitomized in the International Statement, seeking to create embedded vulnerabilities does nothing less than endanger national prosperity while advocating for weakened cyber-infrastructure, creating threats in the short- and long-term alike.

V. Conclusion

This paper on the International Statement has argued the encryption debate overlooks the necessity of encryption for the protection of IP, a

---

61 Brian Krebs, "Sealed U.S. Court Records Exposed in SolarWinds Breach" (7 January 2021), online: *Krebs on Security* <krebsonsecurity.com> [perma.cc/V6VQ-G2XW].

62 Nathan Bomey & Kevin Johnson, "What you need to know about the FireEye hack: Cybersecurity attack against US government", *USA Today* (18 December 2020), online: <www.usatoday.com> [perma.cc/BLP8-TQTU].

63 See Rachel Aiello, "'Vulnerability' led to Canadians' data being accessed in series of cyberattacks", *CTV News* (17 August 2020), online: <www.ctvnews.ca> [perma.cc/H78E-Y67S]. See also Brigitte Bureau, Catherine Cullen & Kristen Everson, "Hackers only needed a phone number to track this MP's cellphone", *CBC News* (24 November 2017), online: <www.cbc.ca> [perma.cc/WCE6-2QNT].

crucial component of national security. Its purpose was to highlight the role of trade secrets in this discussion, and to emphasize the importance of its protection as a matter of public safety. Encryption has served a vital role in the shifting strategies of corporate entities seeking to protect their IP in a way that is adaptable to the speed of contemporary innovation; in particular, the doctrine of trade secrets has served a critical role in the protection of IP based on code. However, while public safety authorities recognize in their rhetoric the need to safeguard IP assets to guarantee national security, they do not connect the dots in accepting the degree to which the threat to IP posed by weakening encryption is itself a threat to national security. When IP is viewed through a national prosperity discourse, the profusion of end-to-end encryption can be seen as vital to protecting national prosperity.