"GOING DARK" – NO EASY ANSWERS ON THE CYBERSECURITY HORIZON

Posted on November 8, 2016

Categories: Insights, Publications

Canadian Corporate Counsel, Volume 25, Number 7
Watch a video synopsis of this article here

It is difficult to name another technology as ubiquitous yet simultaneously misunderstood as encryption. At the risk of cliché, encryption is truly everywhere. It is used inside the credit and debit cards you carry, the fob with which you access your home or office, the keys you use to unlock your car and the passes you use to ride public transportation. Encryption can prevent a nosey neighbour from sniffing your Wi-Fi traffic or create a secure tunnel back to your work network while travelling abroad. With encryption, you can protect the contents of your laptop, tablet, smartphone or external storage by making its contents indecipherable to a third party without the decryption key. It secures websites, phone calls, video content, Bluetooth connections, and any number of other devices and technologies that you rely on every day.

This increasing ubiquity, coupled with the reality that modern strong encryption, when implemented property, can make encrypted data truly unrecoverable by anyone who does not possess the decryption key, gives rise to the "going dark" problem. This phrase refers to the reality that governments and law enforcement simultaneously have a decreasing ability to gain visibility into encrypted data (which can be a necessary component of their role in preventing and investigating crime). Meanwhile, the frequency with which government bodies encounter data that is protected by encryption is increasing.

This "going dark" problem came to the forefront of public debate, earlier this year, the FBI sought to compel Apple's assistance to circumvent (or perhaps more accurately, facilitate a more efficient brute force attack on) the encryption protecting the contents of an iPhone used by the perpetrators of the San Bernardino terrorist attack. Apple resisted the cooperation sought by the FBI, however the FBI was ultimately able to access the device's contents without Apple's assistance (using undisclosed methods). As a result, the merits of the dispute were not litigated in full. Although the San Bernardino decryption dispute may have fallen off mainstream radar, the larger tension between the need to encrypt information reliably and absolutely, and law enforcement's genuine need for visibility into stored and transmitted data, is nowhere near resolution.

Resolving this tension will be one of the more significant regulatory challenges of the next decade, and unfortunately, history tells us that there is no easy solution. In what follows, we examine the "going dark" problem and provide a brief overview of how various jurisdictions have historically attempted to solve it.

Not a Solution – Weakness by Design

History has shown that there is no easy solution to the competing demands for the security and privacy afforded by strong encryption on the one hand, and an ability for government to access data in appropriate circumstances on the other. Since the early days of modern encryption, governments have grappled with this dilemma.

Many early attempts to regulate encryption sought to either import some form of weakness, or backdoor into the encryption itself, or to impose limitations on encryption's use. The rationale behind prohibiting or weakening encryption by design was presumably to enable law enforcement to decrypt data without relying on cooperation from third parties. One early effort to regulate encryption was also one of the bluntest. In the late 1970s, the U.S. National Bureau of Standards ("**NBS**") published the "Data Encryption Standard" ("**DES**"), which was the first American unified federal data encryption algorithm. The National Security Agency ("**NSA**") successfully lobbied for a weaker encryption standard than was initially intended.[1] The dilemma was clear. There was need for a strong encryption standard capable of protecting privacy and securing data, but at the same time, there was fear of a standard so strong that it could be used to undermine the nation's own intelligence efforts.

In 1993, the U.S. Government proposed the Escrowed Encryption Standard ("**ESS**"). This initiative sought the inclusion of a device called the "Clipper Chip" in telephone systems. It would have permitted the state to decrypt digital information after retrieving a cryptographic key that was to be pre-deposited with the National Institute of Standards and Technology ("**NIST**") and the Treasury Department. Technology experts and government officials (including John Ashcroft and John Kerry) were quick to denounce this initiative. Not only would criminals avoid using technology employing the Clipper Chip (neutering its primary purpose at the outset), but the initiative was ripe with the potential for insider abuse, was allegedly subject to significant technical vulnerabilities, and would in fact pool decryption keys in a centralized location, which by its nature was more vulnerable to attack.[2] For these reasons, the Clipper Chip initiative was eventually abandoned.

Another early attempt by the U.S. Government to regulate encryption practices was the establishment of export controls that limited foreign access to strong cryptographic technology. Prior to 1996, encryption algorithms were classified as "munitions" in the U.S. and their export was substantially regulated. However, such regulation became substantially more difficult to enforce as internet use grew in popularity.[3] These controls were also harmful to the American economy, as e-commerce requires the use of strong cryptography.

As a result, the Economic Strategy Institute in 1998 estimated that with continued export controls, the U.S. economy would have lost $37 to $96 billion over the period from 1998 to 2003.[4] Ultimately, in November 1996, the Clinton Administration signed an executive order transferring regulation of encryption exports to the Department of Commerce, which enabled the substantial relaxation, if not practically the elimination, of encryption export restrictions in the U.S.

Not a Solution – Mandated Assistance

Another strategy employed to varying degrees of success is to take steps to compel manufacturers, on a per-instance basis, to provide decryption assistance. Such assistance may come in the form of mandating decryption key disclosure, or the removal from hardware or software of external "non-encryption" barriers to decryption (such as password retry limits, automatic wiping, or arbitrary delays that are imposed by software). The latter approach is arguably a less offensive intrusion on the capabilities of strong encryption, in that it does not involve impairing the strength of the underlying encryption itself.

However, this too is an imperfect solution, as it requires law enforcement to rely on third-party manufacturers or service providers to provide assistance. As became apparent during the recent San Bernardino incident, third parties may be increasingly resistant to providing any form of what may be perceived as "decryption assistance". The process of addressing that reluctance through the courts may serve to be a significant practical roadblock in an environment where law enforcement may need to make relatively quick and responsive decisions based on the content of electronic communication and data.

The imperfection of this approach becomes even more pronounced where the third-party manufacturer or service provider actually lacks the ability to facilitate access (regardless of desire). Recently, WhatsApp advised that it could not comply with an FBI wiretap warrant, as it did not control the decryption keys protecting the content of messages sent through its platform.[5] This type of response may increasingly become the norm as manufacturers and service providers move to "trust-no-one" (or "**TNO**") encryption models that remove the ability for third parties (including the manufacturer or service provider itself) to access a user's data.

Global Strategies – How the World Handles "Going Dark"

In seeking insight into the potential future of domestic regulation in this space, it is also useful to review the various approaches taken and proposed in foreign jurisdictions. Just as the history of encryption's regulation has been characterized by a variety of differing perspectives and approaches, equally diverse is the range of strategies contemplated around the globe today.

In the U.K., legislators in both Houses of Parliament are currently exchanging amendments to the *Investigatory Powers Bill*[6] ("IPB") following its third reading in the House of Lords on October 31, 2016. The IPB, which may

become law in the U.K., concerns the proposed expansion of government surveillance of electronic communications. Among other things, it would allow government-sanctioned "hacking" in investigating crimes, and require companies to assist with these operations. This bill would also require companies to take "reasonable steps" to hand over data to law enforcement.

One of the potential implications of the IPB could be the prohibition of end-to-end encryption of electronic messages. End-to-end encryption effectively conceals these messages from both the manufacturer itself and internet service providers. In order to comply with the IPB, companies may have to scale back their deployment of end-to-end encryption to retain the ability to decrypt traffic. Critics of the IPB have indicated that the "reasonable steps" requirement contemplated by the legislation may impose overly burdensome assistance obligations on third parties.[7] Perhaps responding to this criticism, the IPB was revised to only require companies to remove encryption *so long as the removal is feasible and not prohibitively expensive*. At the present moment, the bill contains language that would allow the creation of regulations obligating a "relevant operator" (including postal and telecommunications operators) to remove electronic protection applied by or on behalf of that operator to any communications or data. Notably, under current U.K. law (section 49 of the U.K.'s *Regulation of Investigatory Powers Act*) individuals are already required to supply decrypted information or decryption keys to law enforcement upon court order, subject to certain safeguards.

Similarly, the U.S. Senate Select Committee on Intelligence Chairman Richard Burr and Vice Chairman Dianne Feinstein recently proposed a piece of draft legislation called the "Compliance with Court Orders Act of 2016" (the "**Feinstein-Burr Bill**"). If passed, this bill would force manufacturers to decrypt data and provide information to law enforcement in an intelligible format (or provide the technical assistance necessary to do so) when faced with a court order.[8] As above, there is an argument that such legislation could require manufacturers to build vulnerabilities into their products, and possibly disable the use of end-to-end encryption.

While the Feinstein-Burr Bill is reportedly losing momentum and is not expected to pass[9], its subject matter is ripe for debate. The California and New York legislatures are currently sitting on similar draft legislation that would attempt to limit smartphone encryption. Read for the first time earlier this year, California's Assembly Bill No. 1681 would, on or after January 1, 2017, make a manufacturer that is unable to decrypt a smartphone on-demand subject to a civil penalty of $2,500 for each instance.[10] This bill is currently in committee. New York's Assembly Bill A8093A, also currently under consideration, contains a similar provision.[11]

India has taken an approach to encryption that is in many ways a throwback to the early attempts at regulation discussed above by capping the strength of encryption mechanisms in certain circumstances.[12] Further, in 2015, India's Department of Electronic and Information Technology ("**DEITy**") proposed a new draft encryption policy. The policy would have forced persons to store for 90 days plain text copies of all their

encrypted messages to be made available to law enforcement on demand, rendering such security measures all but redundant.[13] DEITy quickly withdrew the policy following fierce public outcry.

India is not the only nation to draw from historical U.S. approaches to regulation. Australia's Defence Trade Controls Act 2012 ("**DTCA**")[14] is a contemporary example of encryption export controls. The DTCA prohibits the export of communications protected by certain strong encryption mechanisms without a permit. The DTCA provides for stiff penalties for breach, including up to10 years in jail. The International Association for Cryptologic Research submitted a petition to block the DTCA, stating that the legislation as drafted "cuts off Australia from the international cryptographic research community and jeopardises the supply of qualified workforce in Australia's growing cybersecurity sector".[15] The DTCA nonetheless came into force as drafted.

In May 2016, the European Police Office ("**Europol**") and the European Union Agency for Network and Information Security ("**ENISA**") issued a joint statement acknowledging the dilemma involved in balancing privacy rights with the important objectives of law enforcement. [16] The statement stressed the importance of proportionality in law enforcement's ability to employ intrusive investigative tools in investigating cyber related crimes and proposed that law enforcement select the least intrusive measure to achieve their investigative purpose. While intercepting encrypted communication with respect to solely an individual suspect may be proportionate, the statement noted that "breaking the cryptographic mechanisms might cause collateral damage". The joint statement also called for the sharing of best practices among various international jurisdictions regarding methods that lawfully allow bypassing encryption already in use by some jurisdictions. The statement asks policymakers and the judiciary to collaborate to issue clear policy guidance on the proportionality of the use of such investigative tools. The statement concludes by commenting that:

"When circumvention is not possible yet access to encrypted information is imperative for security and justice, then feasible solutions to decryption without weakening the protective mechanisms must be offered, both in legislation and through continuous technical evolution."

While the joint statement represents thoughtful collaboration in pursuit of a unified solution to the "going dark" problem, there remains philosophical differences with respect to this issue globally. For instance, while countries such as Germany and the Netherlands have both disavowed encryption backdoors,[17]the U.K.[18] and the U.S. emphasize the need of law enforcement to have unimpeded access to encrypted data.[19]

The Current Landscape in Canada

In Canada, Section 8 of the *Canadian Charter of Rights and Freedoms* protects against unreasonable search and seizure by government agencies. The mechanics of Section 8 require that the government obtain lawful authority prior to conducting a search regarding a subject matter to which an individual has a reasonable expectation of privacy.

The determination of whether an individual has a reasonable expectation of privacy turns on whether the individual has a subjective expectation of privacy and whether that expectation is objectively reasonable.[20] Establishing that an individual has a subjective expectation of privacy is relatively easy and this can normally be inferred from the manner in which an individual treats the information in question.[21] Establishing that this subjective expectation is objectively reasonable is the greater burden for an individual to overcome when objecting to government intrusion into their private affairs.

An evaluation of whether a reasonable expectation of privacy is objectively reasonable is a normative process.[22] Where the subject matter involves informational privacy, courts must consider whether the information obtained by law enforcement reveals personal information that individuals in a free and democratic society would not want the state to obtain. Case law demonstrates that information revealing intimate details about our lifestyle or personal choices is the kind of information that attracts constitutional protection.[23]

The Supreme Court has repeatedly recognized the privacy interests associated with technological devices. The Court has found that searches of technological devices have the potential to implicate important privacy interests that are different in both nature and extent from the search of ordinary "places".[24] In *R v Spencer* the Court further held that individuals maintain a reasonable expectation of privacy in their online activities in certain circumstances.[25]

Despite the reasonable privacy interest that individuals may have in technological devices, Canadian law enforcement agencies are permitted to impede this interest if they obtain lawful authority to do so (i.e. a search warrant). Indeed, where the requisite authority is obtained, law enforcement possesses significant legal tools to help them access and identify information that has been made "dark" using encryption methods. This includes the authority to obtain an "assistance order" requiring any person to assist law enforcement in carrying out a search.[26]

In *R v TELUS Communications Co.* ("**Telus**"), the court recently considered whether obtaining an assistance order requires independent lawful authority to impede an individual's privacy interest.[27] In this case, law enforcement sought the assistance of a third party service provider to identify the personal subscriber information relating to anonymized data obtained through a transmission data recorder warrant. The court found that the law enforcement agency had already obtained the necessary authorization to access the private information through the original warrant and that the assistance order was simply supplementary.[28] In finding that an assistance order does not require independent authority to impede an individual's privacy interest, the court noted the following about the lawful access sections of the *Criminal Code*:

These sections ought not to be interpreted in a manner that simply creates a technical maze, through which

the police are to be put, with no certainty whether the path that the police ultimately take will have them arrive at the desired endpoint, especially when, had the correct path been taken, the desired information would nonetheless have been obtained.[29]

Law enforcement also has additional tools in the context of mobile carriers. The Solicitor General's Enforcement Standards ("**SGES**") set out various decryptability requirements that must be met as a condition of obtaining a wireless spectrum license in Canada. The SGES came into force in 1990, and was amended in 2008. Standard 12, for example, provides that if network operators or service providers initiate encoding, compressors or encryption of telecommunications traffic, law enforcement agencies will require the network operators or service providers to provide intercepted communications in decrypted form.[30]

Bill C-13, the *Protecting Canadians from Online Crime Act* came into force on March 9, 2015. This recently passed legislation, while a shadow of more onerous proposed legislation, enforces the search powers of the government, in the digital domain.[31] While the SGES applies to mobile providers, this Act applies to all telecommunication service providers. The Act contains provisions with respect to entities that possess or control computer data or certain financial data, such as Internet service Providers (ISPs), telecommunications service providers (TSPs) and financial institutions. The Act has amended the *Criminal Code* to authorize a peace officer or public officer to require individuals to preserve computer data that is in their possession or control.[32] Critics of the Act emphasize that it lowers the threshold applicable to obtaining various orders relating to computer data, transmission data, and tracking data.

The Road Ahead

Proposed strategies for regulating encryption are varied, nuanced, and rarely satisfy the interests of all stakeholders. However, the lack of a satisfying solution is hardly unexpected. The reality is that there are no simple solutions or easy answers ahead, and both historically employed and proposed future solutions are fraught with significant negative side effects.

It is arguably imprudent to weaken encryption by design. If you cut a hole through a vault door, it is difficult to convince the world that the hole will only be used by the good guys and never by the crooks. No matter how well a vulnerability or backdoor is disguised or protected from misuse, purists will argue that any vulnerability imposed on an encryption scheme represents a point of weakness that can be exploited by a malicious actor. Further, the approach of imposing a known weakness or providing for backdoor access invites difficult questions as to who the "good guys" are. Which agencies in government would be entrusted with the keys to utilize backdoor access to a particular platform, and which foreign states would be extended the same courtesy provided to domestic authorities? In an era when data breaches are seemingly a weekly event, what happens when the repository of keys, credentials, or knowledge necessary to utilize an imposed vulnerability or

backdoor is compromised?

Similarly, it is impractical to adopt a practice of restricting the use or development of existing or future encryption through regulation. Encryption is fundamental to the operation of significant components of business, society, and daily life. Pushing back against its widespread employ would be not only impractical, but also damaging to the economy, and arguably ineffective at actually preventing encryption's utilization by determined criminals.

Further, encryption, at its core, is simply a methodology (or many) for executing complex mathematical operations in a manner that produces a particular output. The distribution of knowledge is incredibly difficult to unwind in an era where the internet serves as a seemingly eternal repository for anything and everything that people have an interest in retaining. Walking encryption back (ignoring for a moment the significant negative consequences that this would have) would be impractical. Security researchers and cryptographers around the world have a strong grasp of the workings of modern strong encryption, and no amount of regulation can undo that reality.

The "going dark" dilemma is a difficult problem without an easy solution. Compounding this challenge is the reality that both lawmakers and their constituents often poorly understand encryption and its implementation. In the interim, while we seek to strike the right balance, the best we can hope and push for is a rational and well-reasoned debate that resists the temptation impulsively to adopt band-aid solutions that do more damage than good.

by Rohan Hill, Mitch Koczerginski and Bill Olaguera, Articled Student

[1] Matt Curtin, *Brute Force Cracking the Data Encryption Standard* (New York: Springer, 2005) at 14.
[2] Abelson, Hal et al. "The Risks of Key Recovery, Key Escrow, and Trusted Third Party Encryption" (www.crypto.com/papers/escrowrisks98.pdf).
[3] In 1999, a study found 805 encryption products worldwide. That study was intended to measure the effectiveness of blocking exports of advanced encryption technology. It concluded that blocking it did not prevent people in other countries from obtaining the products (www.networkworld.com/article/3032188/security/schneier-terrorists-will-switch-to-more-secure-alternatives-to-avoid-encryption-backdoors.html).
[4] Erik R. Olbeter and Christopher Hamilton, "Finding the Key: Reconciling National and Economic Security Interests in Cryptographic Policy" (Washington, D.C.: Economic Strategy Institute, March 1998) (www.members.tripod.com/encryption_policies/us/olbeter_0498_key.htm).
[5] www.wired.com/2016/03/fbi-crypto-war-apps/.
[6] IPB details, including progress of bill (www.services.parliament.uk/bills/2015-16/investigatorypowers.html);

excellent discussion by Computer World UK current to March 16, 2016 (www.computerworlduk.com/security/draft-investigatory-powers-bill-what-you-need-know-3629116/). Read more about Apple's complaint here (www.theguardian.com/technology/2015/dec/21/apple-uk-government-snoopers-charter-investigatory-powers-bill); also discussed in Extreme Tech (www.extremetech.com/extreme/217478-uk-introduces-law-to-ban-civilian-e).

[7] Apple's official submission, p. 79, para 36 (www.parliament.uk/documents/joint-committees/draft-investigatory-powers-bill/written-evidence-draft-investigatory-powers-committee.pdf).

[8] www.bgr.com/2016/04/08/iphone-encryption-laws-usa and Dianne Feinstein's website (www.feinstein.senate.gov/public/index.cfm/press-releases?ID=EA927EA1-E098-4E62-8E61-DF55CBAC1649).

[9] The Register UK article (www.theregister.co.uk/2016/05/27/backdoor_bill_dead/). Interestingly, the CIA and NSA were essentially ambivalent to these laws (unlike the FBI), since they feared that any new law would interfere with their own encryption efforts.

[10] www.leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201520160AB1681.

[11] www.nysenate.gov/legislation/bills/2015/a8093/amendment/original.

[12] www.indiancaselaws.wordpress.com/2015/02/10/digital-encryption-laws-in-india/.

[13] www.indiatoday.intoday.in/technology/story/govt-goes-after-privacy-proposes-end-to-encryption-in-india/1/478952.html.

[14] www.defence.gov.au/deco/DTC.asp.

[15] www.iacr.org/petitions/australia-dtca.

[16] www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/on-lawful-criminal-investigation-that-respects-21st-century-data-protection.

[17] www.networkworld.com/article/3032188/security/schneier-terrorists-will-switch-to-more-secure-alternatives-to-avoid-encryption-backdoors.html .

[18] www.zdnet.com/article/while-us-and-uk-govts-oppose-encryption-germany-promotes-it-why (on Germany promoting encryption).

[19] www.zdnet.com/article/fbi-director-mobile-encryption-could-lead-us-to-very-dark-place (on Comey's 2014 comments).

[20] *R v Spencer*, 2014 SCC 43 at paras 17-18 [*Spencer*]; *R v Tessling*, 2004 SCC 67 at para 42 [*Tessling*].

[21] *Spencer* at para 19; *R v Cole,* 2012 SCC 53 at para 53 [*Cole*]; *Tessling* at para 44.

[22] *Spencer* at para 18.
[23] *R v Plan*, [1993] 3 SCR 281 at para 213.
[24] *R v Fearon*, 2014 SCC 77 at para 51 [*Fearon*]; *R v Vu*, 2013 SCC 60 at paras 38, 40-45 [Vu].
[25] *Spencer, supra* note 20.
[26] *Criminal Code*, RSC 1985, c C-46 at s 487.02 [*Criminal Code*].
[27] *R v TELUS Communications Co.*, 2015 ONSC 3964, [2015] OJ No 3226 [*Telus*].
[28] *Ibid* at para 42.
[29] *Ibid* at para 55.
[30] www.theglobeandmail.com/news/national/article14331614.ece/BINARY/SGES.pdf.
[31] Christopher Parsons and Tamir Israel, "Canada's Quiet History of Weakening Communications Encryption", *The Citizen Lab,* (11 August 2015), <citizenlab.org>.
[32] *Criminal Code* at s 487.012(1).

A Cautionary Note