(Mis)shaping the Future of Security: How Encryption Backdoors Will Affect Us All

Introduction

In December 2019, Saudi Royal Air Force 2nd Lt. Mohammed Saeed Alshamrani, at the time participating in a training program sponsored by the Pentagon as part of a security cooperation with Saudi Arabia, opened fire on his fellow students at the headquarters of the Naval Aviation Schools Command at NAS Pensacola. Three were killed and a further eight wounded, and the assailant himself was killed by a deputy sheriff at the scene (Little, 2020).

In the course of the investigations regarding the Pensacola shooting, the FBI sought to access Alshamrani's iPhone in order to reconstruct the facts leading up to the massacre. It failed to bypass its encryption however, and obtained a court order to force Apple to break into the phone on its behalf – with which Apple refused to comply, citing its fear of setting a precedent which might ultimately dismantle the security of iPhones globally (Welch, 2020). The FBI eventually succeeded in hacking into Alshamrani's phone after some months of trying and established his links to al-Qaeda, however, the time delay and encryption-breaking software that needed to be purchased made this a costly endeavor (Brewster, 2020). *"Thanks to the FBI – and no thanks to Apple – we were able to unlock Alshamrani's phone"* was the cynical comment thereto by US Attorney General William Barr (United States Department of Justice, 2020), to which Apple replied with a letter stating, among other things, that it *did* cooperate by providing all information it could – such as account information and transactional data - but that *"customers count on Apple to keep their information secure (…). We sell the same iPhone everywhere, we don't store customers' passcodes and we don't have the capacity to unlock passcode protected devices"* (Welch, 2020). *"The false claims made about our company"*, then, *"are an excuse to weaken encryption and other security measures that protect millions of users and our national security"* (ibid).

Pensacola is but an example case within a context of tug-of-war pitting law enforcement and intelligence agencies against the global tech industry, with the former increasingly gaining the upper hand. The 'crypto war' – sometimes less polemically referred to as 'backdoor', 'exceptional access' or simply 'encryption debate' – is the result of clashing conceptions of security: IT security on one hand (demanding strong encryption mechanisms) and crime prevention - including terrorism - on the other (demanding that encryption can be circumvented for investigative and prosecutorial purposes). This debate, likely because of its technical nature, has not received much attention within the general public although – as presently argued – it is too important a topic to be outsourced to the technical community and political elites. The purpose of this Article is to enhance the visibility of an issue which, if it continues going down the path it appears to be taking, may affect much more than just the privacy of citizens. We will start off with a short introduction to cryptography and the issues at stake, and subsequently evaluate the arguments made by the contending sides.

A short history of the encryption debate

The idea of cryptography is millennia old; one of the simplest encryption methods is still referred to as the 'Caesar Cipher', a system whereby each plaintext letter is shifted by a certain number of places down the alphabet, so that the message – now in ciphertext - can only be read to those who know the rule, or 'key', used to encrypt the message. If the key is 3, for example, 'hello' becomes 'khoor' and, in principle, only those who know the key can reconstruct the original message. Needless to say, cryptographic systems today are indefinitely more complex.

For most of time, cryptography was mostly the prerogative of spies and militaries (Blaze, 2011). But when computers started becoming commercially available and every-day transactions, bit by bit, moved to virtual spaces, the need to protect those spaces (and more importantly, the data stored in and moving through it) became ubiquitous. Encryption mechanisms came to be built into phones, computers and network nodes, and in 1990, Philip Zimmermann published Pretty Good Privacy (PGP), a globally freely available encryption tool employing public key cryptography - a military-grade technique - to protect e-mail communications. For the first time, the general public was able to purchase software by means of which it could hide its communications, including from its own government (Finklea, 2016).

This naturally sat uncomfortable with law enforcement agencies of States entering the 'information age', and initiated what cryptographer Matt Blaze terms the *"epic battle that would preoccupy a generation of cryptographers"* (Blaze, 2011). Governments took different approaches towards enhancing their access to encrypted data, including mandating reduced key lengths or through escrow systems i.e., the creation of a database containing copies of the keys to all communications. In the US, the Clinton administration attempted to implement the latter in 1993, known as the *Clipper Chip*: secure communication devices (such as crypto phones) were each to be equipped with a chip that was supposed to work just like a standard DES chip, but had a unique cryptographic key programmed onto it of which the government retained a copy. The idea was that the Chip would provide good protection from eavesdropping by malicious actors while at the same time, it would allow law enforcement to intercept calls made with a device equipped with the Clipper Chip when needed (Matthews, 2019). Massive resistance among the academic community, civil society and the tech industry led to the abandonment of the Clipper Chip just three years later on grounds of the enormous expense, governance issues, and the risk of the database being compromised (Abelson et al, 2015). The failure of the Clipper Chip, at least for some years, put the debate to relative rest.

Edward Snowden's famous disclosure the US surveillance program (PRISM) in 2013 marked the bitter come-back of the crypto war as it came to light that several major tech companies – Microsoft, Apple, Google and Facebook, to name a few – had actively collaborated in the mass surveillance campaigns by intelligence services worldwide by systematically decrypting users' data and playing them to the authorities (Sargsyan, 2016). Tech vendors' need to restore consumer trust resulted in an exponential ramping up of hyper-strong encryption on products and services. What became the bone of contention in the ensuing stand-off between law enforcement and the tech community was the installation of near-unbreakable,

automatic client-side encryption on digital products and services: full-disk encryption secures data-at-rest from unauthorized access (for example through a user-generated PIN-code that destructs all data on a device when repeatedly entered incorrectly), and end-to-end encryption (E2EE) is a method by which data-in-transit (chats or video/audio calls) are protected using a technique whereby the message is encrypted all the way between the parties to a communication. This means that the need for third parties (i.e., the service provider) to encrypt the message as it moves across the web is eliminated – and with law enforcements' ability to force companies to provide their users' data in readable format, even upon court orders. E2EE in is considered the most secure form of encryption available today (Thompson, 2020).

In short, encryption methods that use mathematical means that categorically bar third parties from accessing communications contents lie at the heart of the contemporary encryption debate. These techniques are highly effective in keeping data, both at rest and in transit, confidential – so effective that they keep not only the 'bad guys' out, but also erode law enforcements' capability to wiretap and extract data in cases where such investigative methods might be critical to the detection of serious criminal activity, including terrorist plots.

The dark side of encryption

It is obvious that the proliferation of super-strong encryption not only protects the confidentiality of lawful interactions between well-intending persons and entities, but also shields malicious actors from detection. Terror outfits that have lost ground in military terms have secured their survival by shifting many of their activities to digital spaces, where the architecture of the web allows them to plan attacks, coordinate activities and to radicalize, instruct and train recruits across large distances. The large array of encryption technologies available today allows terrorists to conduct such activities at a minimal risk of exposure. In the words of FBI Director James Comey, *"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. We have the legal authority to intercept and access communications and information pursuant to court order, but we often lack the technical ability to do so"* (Comey, 2014). To describe loss of surveillance capabilities as a result of ever-stronger encryption, Comey coined the metaphor of law enforcement 'going dark', which has become a catchphrase in the debate.

The use of cryptographic methods by terrorists is well-documented. Already in 2007, al-Qaeda's media arm, the Global Islamic Media Front (GIMF) launched its own encryption software - Asrar al-Mujahideen, or Mujahideen Secrets – which was followed in 2013 by Asrar al-Dardashah, an encryption plugin for instant messaging (Ahlberg, 2014). ISIS, on the other hand, relies rather on publicly available tools to hide its internal communications from the prying eyes of the State; messaging services such as WhatsApp, Telegram or Signal can be installed easily and without putting oneself at risk of attracting the attention of intelligence agencies. The communication service Telegram, in addition to repeated assurances by its CEO Durov not to cooperate with law enforcement, additionally offers a self-destruct feature,

whereby messages are definitively destroyed after a time period of the users' choosing, thus preventing law enforcement from being able to retrieve information should they succeed in hacking into a suspect's phone. Telegram was therefore the 'app of choice' for terrorists for several years – it was involved in some stage of planning of the 2015 Paris attack, the Christmas market attack in Berlin and the shooting at the Reina nightclub in Istanbul (Tan, 2017).

According to law enforcement, the scope of its loss of capabilities as expressed in the 'going dark' metaphor is substantial. The Manhattan DA's office alone, as of 2016, asserted to have 175 iPhones in its possession it could not open because of encryption (Newcomb, 2016), and Paris prosecutor Francois Molins stated after the 2015 attacks that inability to penetrate encryption is one of the main problems Paris investigators face contemporarily (Savransky, 2016). Moreover, Australia's Home Affairs Minister claimed that 90 per cent of law enforcement investigations are impacted by encryption (Hutchens, 2018), and the FBI clamors that in the fiscal year to September 30th, it could not get access to 7,775 devices even though it had proper warrants (Bradbury, 2018). This is why law enforcement across the world is pushing for 'exceptional access' to encrypted devices and data (including those employing E2EE) by demanding that tech companies design 'backdoors' into their products or services. Somewhat simplified, an encryption backdoor is a *deliberately in-built method – or design oversight – that bypasses the security of a cryptographic system and thereby allows a party to access encrypted information without authorization* (Soesanto, 2018).

What is a legal encryption backdoor?

Encryption backdoors may come in different flavors: an escrow system, like the Clipper Chip described earlier, would involve depositing a copy of the keys to *any* device or communication with a 'trusted third party' (the escrow agent, e.g., government). Some corporations use key escrow systems to prevent data loss - for example as a result of displaced passcodes or attempted fraud by an employee – but the danger of the escrowed key database being compromised, and with it all data protected by the cryptographic system, is considered too large a risk to be implemented on national scale (Abelson et al, 2015).

More commonly, when policy makers refer to encryption backdoors today, what they mean is a design tweak: code that software developers can insert into programs to serve as an 'access point' to be used for surreptitious surveillance or data extraction, or an outright weakening of cryptographic standards by design requirements (e.g., mandating reduced key sizes) (Soesanto, 2018). The "Five Eyes" intelligence complex, an alliance between the intelligence agencies of the US, the UK, Canada, Australia and New Zealand, has for instance issued a statement calling on companies to *"embed the safety of the public in system designs"* so as to *"enable law enforcement access to content in readable and usable format"* (Thompson, 2020). The statement does not elaborate on how exactly this could be implemented in a secure way but expresses that end-to-end encryption is not compatible with the request for exceptional access (Shead, 2020).

Despite uproar from the tech industry, the IT community and civil society, various governments have paved the way for mandatory encryption backdoors while some others have simply banned services that use E2EE. In the Western world, the most infamous example is Australia's Assistance and Access Act 2018 which, among other things, seeks to give law enforcement and intelligence agencies the power to force providers of internet services to *"remove one or more forms of electronic protection"* and to ensure that *"information obtained in connection with an execution of a warrant or authorization is given in a particular format [read: plaintext]"* (Loki Network, 2019). Australian agencies can furthermore issue Technical Capability Notices (TCNs), legally enforceable instructions to create or modify features to give an agency a new technical capability (ibid). When confronted with the question how this will affect communication services using E2EE which, after all, make it mathematically impossible to create such a technical capability, Australian (then)-Prime Minister Malcolm Turnbull replied that *"the laws of mathematics are very commendable, but the only law that applies in Australia is the law of Australia"* (Roberts, 2017). It shall be left at the discretion of the reader to decide whether this statement refers to a little-known factum regarding the inapplicability of mathematical rules in some parts of the world, or whether it might suggest shocking levels of incompetence.

In practice, Australia's laws might either lead to companies offering E2EE-supported products (including WhatsApp, Facebook's Messenger, Signal, and many more) to re-design the cryptographic protections they have developed in the past years (read: to roll them back) or to a ban of such products/services by companies refusing to comply with TCNs or similar requests. The latter has happened, for example in Russia, which banned Telegram after it refused to comply with orders to hand decryption keys to the government (Lyons, 2020), and in Pakistan with BlackBerry in a similar case (Toor, 2016). Notably, in both cases the companies were eventually allowed back in, which suggests a certain level of difficulty in enforcing bans on software in light of the generative nature of modern Internet, in which services and software can be made available without centralized vetting (The Berkman Center for Internet & Society). The only way such bans could effectively be implemented is through use of mechanisms that equal digital isolationism – as in the case of China, which employs technological means (it's 'Great Firewall of China') and social control (surveillance and penalties) to prevent its population from using services such as Facebook, Google and Twitter (Koty, 2017). Needless to say, these mechanisms come at an exorbitant cost for a population's access to information in general and present an acceptable option only for governments that prioritize social control over citizens' rights and freedoms.

Although most tech giants still vow not to bow to demands for encryption backdoors, it is conceivable that they will succumb to the pressure once a sufficiently large number of major economies attacks their products. In light of the fact that both the EU (Koomen, 2019) and the US (Pfefferkorn, 2020) are considering laws similar to the AA Bill, this possibility might materialize not too far in the future.

Discussion - The proportionality of legally mandated encryption backdoors

Encryption backdoors are far from unproblematic. Yet, is it not true that the objectives exceptional access requirements pursue – protecting national security, public order and, not least, human life - are strong enough to justify some collateral damage?

It is generally accepted that legal measures, especially those that affect fundamental rights, must be compliant with the principle of proportionality. The exact manner in which the proportionality test is applied may differ somewhat across jurisdictions, however, the elements from which it is typically deduced are 1) *legitimacy* (the measure pursues a legitimate objective), 2) *adequacy* (the measure is suitable to achieving the objective) and 3) *necessity* (there is no other, less intrusive way of achieving the objective). If these criteria are all met, the costs and benefits of the law have to be balanced, and only if the benefits exceed the costs can the law be considered proportional (Andelkovic, 2017). The following sections aim at providing a realistic evaluation of justifications brought forth by those defending legally mandated backdoors; subsequently, we will assess whether they are capable of passing the proportionality test. Let us first look at some arguments, and how they are countered by opponents of encryption backdoors.

I: Only accessible by authorized agents with a judicial warrant

The framing of backdoors as *legal* or *secure* backdoors, and the debate surrounding them as the *exceptional access* debate, as well as the description of encryption techniques with in-built backdoors as *responsible encryption* all serve the purpose of conveying the image of backdoors as solely serving to aid law enforcement in fulfilling its legitimate mandate. Governments usually assert that backdoors in cryptographic systems would allow law enforcement to occasionally access user data pending a judicial warrant, and only when a specific criminal act has occurred (Green, 2020). However, whatever friendly wrapper is put around the backdoor debate does not take away from the fact that a backdoor, in terms of functionality, is little more than a deliberately inbuilt vulnerability that may not only serve the pursuance of the rule of law, but also opens doors to misuse and malicious hacking.

Cryptographers, IT security specialists and computer enthusiasts almost univocally agree that a 'good guys only' backdoor is a technical impossibility (Soesanto, 2018). Acclaimed computer scientist Harald Abelson, for example, warns that *"providing access over any period of time to thousands of law enforcement agencies will necessarily increase the risk that intruders will hijack the exceptional access mechanisms"* (Abelson et al, 2015), and in the words of tech reporter Ben Wolford, *"if there is a "master key" to unlock millions of accounts, every hacker on the planet will be after it"* (Wolford, 2018). Schneier elaborates how interception backdoors would erode critical security features of encrypted chat programs: *"It would have to add a feature that added additional parties to a chat from somewhere in the system – and not by the people at the endpoints. It would have to suppress any messages alerting users to another party being added to the chat. Since some chat programs, like iMessage and Signal, automatically send such messages, it would force those systems to lie to their users. Other*

systems would simply never implement the "tell me who is in this chat conversation" feature which amounts to the same thing" (Schneier, 2019).

Secondly, even if we assume that it would be technically possible to design a backdoor only accessible to State actors, how can be ensured that such actors do not abuse them? The NSA's PRISM program is a case to the point; similarly, it has come to light that in the UK, local authorities used surveillance capabilities conferred to them to combat terrorism and other serious crimes under the Regulation of Investigatory Powers Act (RIPA) for nefarious objectives such as monitoring members of the public walking their dogs and feeding pigeons (Tamplin, 2016). The risk that law enforcement officers could use their capabilities to retrieve data for personal motives too is real: An Associated Press (AP) investigation demonstrated that police officers across the US misused confidential law databases to get information on romantic partners, business associates, neighbors, journalists and others for reasons that have nothing to do with daily police work (Cournoyer, 2016).

In short, encryption backdoors can hardly be described as responsible, and yet less as secure, and they can and will be abused for purposes other than upholding the rule of law.

II: The right to life trumps the right to privacy

The debate around encryption backdoors is often reduced to a discussion about the relative merit of the right to privacy. Is not the objective of upholding public order and preventing terrorism of higher value than the right to privacy? Spinello, for example, argues that *"Apple's policy [of resisting the FBI's demand for exceptional access] fails to acknowledge the primacy of physical security rights over privacy rights"* (Spinello, 2020). Framing the debate on encryption backdoors in these terms implies a profound lack of understanding of what is actually at stake.

Contemporary systems – social, economic, political - depend on digital transactions, and this dependence is destined to increase further with the proliferation of 5G connectivity. In order for such systems to function, we need to trust not only in the confidentiality of perhaps nefarious private communications but also that of financial transactions; we need to have assurances that sensitive data related to our health as well as other personal records, corporate secrets and intellectual property are stored safely, and human rights activists and investigative journalists need to ensure that their sources are not exposed. Perhaps still more importantly, we need to protect critical infrastructure such as power grids and transport systems from malicious interference, and governments need to ensure the integrity of electoral processes while at the same time protecting their agencies from being spied on by foreign governments. All of the above rely heavily on encryption for their integrity and confidentiality (De Felice & Bell, 2020), and increasing interconnectivity between ICT systems means that malware can spread rapidly across networks. We only need to point to a few out of many more cases in order to demonstrate the severity of the impact when hackers succeed in circumventing encryption:

- In 2009, a wide-reaching spying network, likely operated by hackers close to the Chinese Communist Party, was uncovered; 'GhostNet' had infiltrated at least 1,295 computers in high-value political, economic and media locations of 103 countries (SecDev Group, 2014);
- In the same year, a hacker from Miami hacked into 250 American financial institutions, stealing tens of millions of credit card details (The United States Department of Justice, 2009);
- In 2010, US and Israeli intelligence agencies infected computer networks in Iran through a Windows vulnerability. The worm, Stuxnet, was programmed to spread to certain models of programmable logic controllers (PLCs), which link ICT systems with industrial machinery, and altered their programming, leading to acceleration of uranium centrifuges and damaging or destroying equipment in the process (Fruhlinger, 2017);
- In 2015, Russian hackers compromised power distribution companies in Ukraine, causing power outrages of up to six hours (Bock, 2015);
- In 2020, a hacking group believed to have links to the Russian intelligence, S.V.R., hacked into various US State Departments including the Pentagon and the United States Treasury as well as nuclear labs (Schneier, 2020).

As the trend of using cyber warfare to manipulate, spy on and pressure political rivals accelerates, hackers are increasingly well-funded and have developed strong capabilities to detect and exploit vulnerabilities in the most sophisticated encryption systems; this has triggered what is sometimes called a technological 'arms race' between hackers and cyber security experts (including cryptographers). Terrorist groups have thus far not succeeded in executing large-scale cyberattacks, but statements by al-Qaeda suggest that the group is actively working to expand its hacking capabilities (Weimann, 2004), while the IS has long been infamous for its interest in cyber technologies. One can only imagine the consequences of a group like the IS hacking into a State's financial institutions or energy facilities or, worse, remote warfare systems.

As described earlier, laws aiming to subvert encryption such as Australia's Assistance and Access Bill considerably weaken cyber security by introducing attack surfaces from which hackers can access networks, especially where such laws target the strongest protection techniques at our availability. Such regulations furthermore discourage investment in research and development: after all, why would tech firms continue to invest in developing more sophisticated and expensive encryption technology, knowing that they could be mandated to roll back their newest technologies, regardless of the costs? Arguably, in light of the scope of damage that cyberattacks can incur, the tech industry should be equipped with maximum capabilities to strengthen the resilience of IT systems against sophisticated cyber criminals likely to take advantage of any compromise the tech industry is forced to make.

Instead of misleadingly framing the 'exceptional access' debate in terms of security versus privacy, it is, in light of the above, more instructive to understand it in terms of *competing visions of security* - cyber security (requiring strong encryption) versus detection and prosecution of terrorists and other criminals (hindered by strong encryption) – as suggested by Pell (Pell, 2015). Both objectives are valid; policy-making should therefore be informed by an analysis of the *relative* merit of each. This Article has demonstrated the importance of promoting strongest possible encryption in the previous paragraphs, yet still the case against restrictive encryption laws becomes the more convincing when we acknowledge that the baseline rationale for legally mandated backdoors – that they are *necessary* and *adequate* for terror prevention – can themselves be dismantled.

III: Encryption backdoors will prevent law enforcements from 'going dark'

Law enforcement agencies like to justify their calls for encryption backdoors by claiming that strong encryption prevents it from doing its job in upholding public order, and that cryptographic designs that permit 'exceptional access' would remedy this issue. However, while public order and terrorism prevention are without question valid objectives, the argument proffered here is that legal 'backdoor' requirements are, in fact, neither strictly necessary nor adequate tools in the fight against terror.

Necessity

The necessity of 'exceptional access' requirements can be questioned because the premise that law enforcement is, in fact, 'going dark' is in itself misleading: in fact, law enforcement and intelligence have today much better and more effective surveillance capabilities than they had in the '90s' (Abelson et al, 2015). In the Pensacola case, as well as in similar high-profile disputes between Apple and the FBI (see e.g., CBC News, 2016), the latter after all managed to get access to the shooter's phone without Apple's help. The details around State-sponsored hacking remain undisclosed as in most jurisdictions such activities fall into legal grey zones, but it is assumed that the FBI purchased state-of-the-art hacking technologies from third parties, that is, companies that specialize in exploiting software vulnerabilities (Collier & Farivar, 2020). A recent report by Upturn, a US-based civil society organization, uncovered that more than 2,000 local law enforcement agencies across the country are in possession of so-called mobile device forensic tools (MDFTs) – powerful hacking tools that can, among other things, remove a locked iPhone's time delay and self-destruct features, and hence remove key protections to Apple's device encryption (Koepke, 2020). The existence of such tools, and their apparently widespread use by law enforcement, is in itself worrisome from a democratic point of view, but the bottom line is that there are alternatives to legal backdoors, which are already in use.

Intercepting data during transmission (e.g., eavesdropping on WhatsApp calls, live-reading of E2E encrypted chats) may be more difficult than breaking full disk encryption, as there are currently no technologies – at least no publicly known ones - to intercept live communications

protected by E2EE: as mentioned, tech companies have purposefully made this mathematically as good as impossible. That said, a Berkman report of 2016 convincingly argues that *"technological developments point to a future abundance in unencrypted data, some of which can fill gaps left by the very communication channels law enforcement fears will "go dark" and beyond reach"*. (The Berkman Center for Internet & Society, 2016). What the report refers to are, firstly, the growth of the Internet of Things (IoT) – i.e., physical objects that connect to the internet and send and receive data, such as smart televisions, light bulbs, door locks, watches and other wearables – and secondly, to the availability of metadata, that is, e-mail addresses, mobile device location information and time stamps which are typically unencrypted and which can provide critical information for an investigation (ibid). It is agreed on by judges, lawyers and researchers alike that secondary data can be highly beneficial for investigative and prosecutorial purposes. Data Scientist Charles Givre, for example, used "smart" devices in his own home to prove how data retrieved from these devices make it possible to build a highly accurate picture of one's character and daily routines simply by "following the IoT" (Kirchner, 2015), and in *Carpenter v. United States*, the prosecution of a suspected robber succeeded because his movements could be reconstructed based on location points retrieved from his cellphone (Holland, 2020). Secondary data typically is unencrypted and can be shared with law enforcement without incurring the externalities associated with encryption backdoors.

The bottom line is that there are valid reasons to doubt that law enforcement is, in fact, 'going dark', which in turn puts the necessity of surveillance backdoors for law enforcement to question. These doubts are shared by some government agents, such as expressed in a statement by former NSA Deputy Director Rick Ledgett, who said that the world might be growing *"dimmer"* but not *"dark"* (Landau, 2018). Certainly, direct access to communications contents would make life easier for law enforcement; however, is it even desirable to make surveillance that easy?

Adequacy

The principle of adequacy demands that a law with restrictive effects on citizens' rights must be *"suitable to achieve the purpose that was sought by the lawmaker"* (Cianciardo, 2010). In the present context, this means that in order to meet adequacy requirements, it must be demonstrated that legally mandated encryption backdoors are effective tools in the fight against terrorism and other crimes facilitated by encryption.

Attempts at forcing providers of communication services to implement encryption backdoors fail to meet this criterion because, firstly, they are unlikely to actually lead to the introduction of backdoors but rather to an exit of the tech industry. It has already been mentioned that the tech industry is very vocal in opposing demands for exceptional access requirements; and this resistance is not only motivated by security and ethics, but indeed also by business considerations: if it becomes known that a service communications service provider has agreed to implement a backdoor for its products it will incur reputational damage and cause its customers worldwide to switch to other providers. Therefore, a globally operating service

provider will likely incur less damage by simply exiting (or accepting being banned by) a jurisdiction with 'backdoor' requirements rather than complying with its laws. Skype's experience is a case to the point: when it became known in the context of the Snowden revelations that it had installed a backdoor for law enforcement, Skype incurred a loss of credibility and quickly lost market share to providers of similar services (Endeley, 2018). At the same time, small and medium-size national providers of internet services based in a State with strict encryption laws will be locked out of international markets as their products are viewed as untrustworthy (Cotton, 2019).

Even if governments are serious about implementing exceptional access requirements, this would hardly stop terrorists from using secure communication channels as enforcement of such regulations would be extremely difficult: mal-intending actors (as well as well-intending ones wanting to protect their privacy) will simply abandon products/services produced in a State that has legal backdoor requirements and purchase secure ones from overseas. Freely available third-party or open-source encryption software can easily be purchased and sideloaded on weakly encrypted communication software (Cole, 2020); as has been mentioned earlier, al-Qaeda has even released its own encryption software back in the 2000s. All the while, software that conceals an internet user's IP address, such as virtual private networks (VPN) or The Onion Router (TOR), make circumvention of legal obstacles to the use of encryption easy.

Conclusion

The proportionality of a measure, as has been mentioned, is a function of the legitimacy of the objective it pursues, its necessity and adequacy and, lastly, the weight of its projected benefits relative to its costs. While it is indisputable that upholding public order and preventing terrorism are legitimate goals, encryption backdoors are neither necessary nor adequate in achieving this objective. Such measures moreover come at potentially exorbitant costs regarding privacy (because they facilitate mass surveillance), the economy (because they render the tech industry uncompetitive), and security (because they make information systems easier to attack). In the worst case, such encryption backdoors may be used for cyber-attacks by terrorist groups, thus enabling the very phenomenon they aim at containing. They are therefore grossly disproportionate – as almost any scholar or professional with an IT background who has written on the topic will agree.

> *"The almost proud absence of technological expertise on the pro-'government access' side […] has made this debate so worrying"* writes cryptographer Professor Matthew Green on his blog, and: *"the idea of deliberately engineering weakened crypto is, quite frankly, terrifying to experts. It gives us the willies"* (Green, 2015).

The fact that governments increasingly consider such laws despite repeated alarm-ringing by experts indeed is frightening, but easy to explain from a political perspective: counterterrorism is a sexy topic that can score politicians points with their votership, while the importance of cryptography, despite of its ubiquity, is little understood. Terrorism tends to be used as a 'joker card' by governments, democratic and undemocratic, that routinely

serves to justify intrusive legal and social control mechanisms. While preventing the proliferation of terrorism remains a security challenge not to be sidelined, policy that focusses on some vaguely defined end without scrutinizing the means are capable of eroding the very foundation of those democratic societies they aim at protecting.

This Article constitutes an attempt to contribute to the public visibility of the exceptional access debate by explaining what is at stake in the least technical manner possible. It aims to demonstrate that *any* concession the tech industry might be compelled to make with regard to the strength of their cryptographic techniques might have catastrophic consequences. The logical conclusion is that any debate on legally mandated backdoors should be abandoned at once – at least until States are able to present a 'backdoor' technique to the public that can be implemented posing a risk to data security. This argument has been brought forth by a number of cryptographers; a panel of top experts in the field, for example, demands that *"anyone proposing regulations should first present concrete technical requirements which industry, academics, and the public can analyze for technical weaknesses and for hidden costs"* (Abelson et al, 2015) and similarly, Susan Landau, Professor in Computer Science, proposes that legislators should let the *"computer security community do what it does best: to find security vulnerabilities in the technique"* (Landau, 2018). However, as of now, no government has been able to present a technique capable of permitting 'exceptional access' only to authorized personnel at the exclusion of malicious actors.

In the meantime, the best way forward lies in establishing constructive collaboration partnerships between the tech industry and law enforcement. Providers of internet services should cooperate with law enforcement on an ad hoc basis and pending the existence of legal warrants by providing the data they *can* provide. For those providers using E2EE, this may mean sharing of metadata and technical assistance. Providers that do store their users' private decryption keys on their servers may also decrypt those data on law enforcements' behalf, again on individual basis rather than systematically and pending adequate judicial oversight. It must also be ensured that they make sufficiently clear to their customers that their products permit third party access. At the same time, the tech industry must be assured that it is backed by the State in building up its defenses in the wake of an age in which data is a gold mine, and attacks on information systems the new way of waging war.

Bibliography

Abelson, H. et al (2015). Keys under Doormats: Mandating insecurity by requiring government access to all data and communications. *Computer Science and Artificial Intelligence Technical Report.* Available at https://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf

Ahlberg, C., 2014. How Al-Qaeda Uses Encryption Post-Snowden. *Recorded Future.* Available at https://www.recordedfuture.com/al-qaeda-encryption-technology-part-1/

Andelkovic, L., 2017. The Elements of Proportionality as a Principle of Human Rights Limitations. *Facta Universitatis Series Law and Politics* 15(3).

Blaze, M., 2011. Key Escrow from a Safe Distance: Looking Back at the Clipper Chip. *Conference: Twenty-Seventh Annual Computer Security Applications Conference, ACSAC 2011, Orlando, FL, USA.*

Bock, P., 2015. Lessons Learned From a Forensic Analysis of the Ukrainian Power Grid Cyberattack. *ISA Cybersecurity.* Available at https://blog.isa.org/lessons-learned-forensic-analysis-ukrainian-power-grid-cyberattack-malware

Bradbury, D., 2018. The Flaw in Encryption Back Doors. *Sector.* Available at https://sector.ca/the-flaw-in-encryption-back-doors/

Brewster, T., 2020. FBI Hacks iPhones in Pensacola Terrorist Shooting Case, But The War With Apple Goes On. *Forbes.* Available at https://www.forbes.com/sites/thomasbrewster/2020/05/18/feds-hack-iphones-in-pensacola-case-apple-not-needed-after-all/?sh=d3c7f1575e99

CBC News, 2016. FBI breaks into iPhones of San Bernardino shooter without Apple's help. *CBC.*

Available at https://www.cbc.ca/news/technology/fbi-san-bernardino-iphone-break-1.3509899

Cianciardo, J., 2010. The Principle of Proportionality: The Challenges of Human Rights. *Journal of Civil Law Studies* 3(1)

Cole, T., 2020. The Dangers of Government-Mandated Encryption Backdoors. *Security Boulevard.* Available at https://securityboulevard.com/2020/10/the-dangers-of-government-mandated-encryption-backdoors/

Collier, K. & Farivar, C., 2020. The FBI cracked another iPhone – but it's still not happy with Apple. *NBC News.* Available at https://www.nbcnews.com/tech/security/fbi-cracked-another-iphone-it-s-still-not-happy-apple-n1209506

Comey, J.B., 2014. Going Dark: Are Technology, Privacy and Safety on a Collision course? *Brookings Institution*. Available at https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course

Cotton, J., 2019. Australia's encryption laws: What's the impact? *iStart.* Available at https://istart.com.au/news-items/australias-encryption-laws-whats-impact/

Cournoyer, C., 2016. Across U.S., Police Abuse Confidential Databases. *Governing.* Available at https://www.governing.com/archive/Across-US-Police-Abuse-Confidential-Databases.html

De Felice, A. & Bell, M., 2020. Encryption: finding the balance between privacy, security and lawful data access. *Digital Europe.* Available at https://www.digitaleurope.org/resources/encryption-finding-the-balance-between-privacy-security-and-lawful-data-access/

Endeley, R.E., 2018. End-to-End Encryption in Messaging Services and National Security – Case of WhatsApp Messenger. *Journal of Information Security* 9(1)

Finklea, K., 2016. Renewed Crypto Wars? *CRS Insight (Report).* Available at https://www.hsdl.org/?view&did=790479

Fruhlinger, J., 2017. What is Stuxnet, who created it and how did it work? *CSOOnline.* Available at https://www.csoonline.com/article/3218104/what-is-stuxnet-who-created-it-and-how-does-it-work.html

Green, M., 2015. A history of backdoors. *Cryptoengineering (Blog).* Available at https://blog.cryptographyengineering.com/2015/07/20/a-history-of-backdoors/

Green, M., 2020. EARN IT is a direct attack on end-to-end encryption. *Cryptoengineering.* Available at https://blog.cryptographyengineering.com/2020/03/06/earn-it-is-an-attack-on-encryption/

Holland, H.B., 2020. A Third-Party Doctrine for Digital Metadata. *Cardozo Law Review* 41(4).

Hutchens, G., 2018. Coalition calls on Google and Facebook to get on side with encryption bill. *The Guardian.* Available at https://www.theguardian.com/technology/2018/oct/10/coalition-calls-on-google-and-facebook-to-get-on-side-with-encryption-bill

Kirchner, L., 2015. Your Smart Home Knows a Lot About You. *ProPublica.* Available at https://www.propublica.org/article/your-smart-home-knows-a-lot-about-you

Koepke, L. et al, 2020. Mass Extraction: The Widespread Power of U.S. Law Enforcement to Search Mobile Phones. *Upturn.* Available at https://www.upturn.org/reports/2020/mass-extraction/

Koomen, M., 2019. The Encrytion Debate in the European Union. *Carnegie Endowment for International Peace.* Available at https://carnegieendowment.org/2019/05/30/encryption-debate-in-european-union-pub-79220

Koty, A.C., 2017. The Great Firewall of China. *China Briefing.* Available at https://www.china-briefing.com/news/chinas-great-firewall-implications-businesses/

Landau, S., 2018. The Five Eyes Statement on Encryption: Things Are Seldom What They Seem. *Lawfare (Blog).* Available at https://www.lawfareblog.com/five-eyes-statement-encryption-things-are-seldom-what-they-seem

Landau, S., 2018. The Five Eyes Statement on Encryption: Things Are Seldom What They Seem. *Lawfare (Blog).* Available at https://www.lawfareblog.com/five-eyes-statement-encryption-things-are-seldom-what-they-seem

Little, J., 2020. NAS Pensacola attack: A minute by minute timeline oft he 15 minutes that changed Pensacola. *Pensacola news journal.* Available at https://eu.pnj.com/story/news/2020/12/04/nas-pensacola-shooting-navy-releases-timeline-events/3812080001/

Loki Network, 2019. The Assistance and Access Bill 2018: One year later. *Loki Network.* Available at https://loki.network/2019/12/06/the-assistance-and-access-bill-one-year-later/

Lyons, K., 2020. Russia lifts its ban on the Telegram messenger app. *The Verge.* Available at https://www.theverge.com/2020/6/18/21295535/russia-telegram-ban-lifted-security

Matthews, T., 2019. The Clipper Chip: How Once Upon a Time the Government Wanted to Put a Backdoor in Your Phone. *Exabeam.* Available at https://www.exabeam.com/information-security/clipper-chip/

Newcomb, A., 2016. New York DA Says He Can't Access 175 iPhones From Criminal Cases Due to Encryption. *Abc News.* Available at https://abcnews.go.com/Technology/york-da-access-175-iphones-criminal-cases-due/story?id=37029693

Pell, S.K., 2015. You Can't Always Get What You Want: How Will Law Enforcement Get What It Needs in a Post-CALEA, Cybsecurity-Centric Encryption Era. *NCJL & Tech.*, *17*

Pfefferkorn, R., 2020. There's nowo an eve worse anti-encryption bill than EARN IT. That doesn't make the EARN IT Bill ok. *The Center for Internet and Society.* Available at http://cyberlaw.stanford.edu/blog/2020/06/there's-now-even-worse-anti-encryption-bill-earn-it-doesn't-make-earn-it-bill-ok

Roberts, R., 2017. Prime Minister claims laws of mathematics 'do not apply' in Australia. *Independent.* Available at https://www.independent.co.uk/news/malcolm-turnbull-prime-minister-laws-mathematics-do-not-apply-australia-encryption-l-a7842946.html

Sargsyan, T., 2016. The privacy role of information intermediaries through self-regulation. *Policy Review* 7(1)

Savransky, R., 2016. Head prosecutor of Paris attacks: Encryption program a 'gigantic black hole'. *The Hill.* Available at https://thehill.com/blogs/blog-briefing-room/news/272850-head-prosecutor-of-paris-on-encryption-programs-were-dealing

Schneier, B., 2019. Evaluating the GCHQ Exceptional Access Proposal. *Schneier on Security (Blog).* Available at https://www.schneier.com/blog/archives/2019/01/evaluating_the_.html

Schneier, B., 2020. Russia's SolarWinds Attack. *Schneier on Security (Blog).* Available at https://www.schneier.com/blog/archives/2020/12/russias-solarwinds-attack.html

SecDev Group, 2014. Tracking GhostNet: Investigating a Cyber Espionage Network. *Information Warfare Minitor.* Available at http://www.nartv.org/mirror/ghostnet.pdf

Shead, S. (2020). US, UK and other countries warn tech firms that encryption creates 'severe risks' to public safety. *CNBC.* Available at https://www.cnbc.com/2020/10/12/five-eyes-warn-tech-firms-that-encryption-creates-severe-risks.html

Soesanto, S., 2018. No middle ground: Moving on from the crypto wars. *European Council on Foreign Relations (Policy Brief).* Available at https://ecfr.eu/publication/no_middle_ground_moving_on_from_the_crypto_wars/

Spinello, R.A., 2020. The ethical consequences of "going dark". *Business Ethics: A Eur Rev*. 1(11)

Tamplin, H., 2016. Councill secretly spied on people walking doogs and feeding birds for five years. *Metro.* Available at https://metro.co.uk/2016/12/26/councils-secretly-spied-on-people-walking-dogs-and-feeding-birds-for-five-years-6345051/

Tan, R., 2017. Terrorists' love for Telegram, explained. *Vox.* Available at https://www.vox.com/world/2017/6/30/15886506/terrorism-isis-telegram-social-media-russia-pavel-durov-twitter

The Berkman Center for Internet & Society at Harvard University, 2016. Don't Panic: Making Progress on the "Going Dark" Debate. *Harvard University.* Available at https://cyber.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf

The Berkman Center for Internet & Society at Harvard University, 2016. Don't Panic: Making Progress on the "Going Dark" Debate. *Harvard University.* Available at https://cyber.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf

The United States Department of Justice, 2009. Major International Hacker Pleads Guilty for Massive Attack on U.S. Retail and Banking Networks. *Office of Public Affairs.* Available at https://www.justice.gov/opa/pr/major-international-hacker-pleads-guilty-massive-attack-us-retail-and-banking-networks

Thompson, A.W., 2020. The "Five Eyes" Still Can't See straight on Encryption. Availabe at https://www.newamerica.org/oti/blog/the-five-eyes-still-cant-see-straight-on-encryption/

Toor, A., 2016. BlackBerry won't be leaving Pakistan after all. *The Verge.* Available at https://www.theverge.com/2016/1/4/10707370/blackberry-continues-operating-in-pakistan-data-request

United States Department of Justice, 2020. Attorney General Willian P. Barr and FBI Director Christopher Wray Announce Significant Developments in the Investigation of the Naval Air Station Pensacola Shooting. *Office of Public Affairs.* Available at https://www.justice.gov/opa/pr/attorney-general-william-p-barr-and-fbi-director-christopher-wray-announce-significant

Weimann, G., 2004. Cyberterrorism: how real is the threat? *United States Institute of Peace. (Special Report).* Available at https://www.usip.org/sites/default/files/sr119.pdf

Welch, C., 2020. The FBI successfully broke into a gunman's iPhone, but it's still very angry at Apple. *The Verge.* Available at https://www.theverge.com/2020/5/18/21262347/attorney-general-barr-fbi-director-wray-apple-encryption-pensacola

Wolford, B., 2018. The real problem with encryption backdoors. *Protonmail (Blog).* Available at https://protonmail.com/blog/encryption-backdoor/