Framework for Regulating Encryption in India

A study undertaken by TQH

August 2019

Authors

Simrit Chhabra, Renjini Rajagopalan & Vatsal Khullar

Research Lead

Rohit Kumar

Table of Contents

Executive Summary

As India forays into a digital revolution that - even in its formative years - has triggered massive transformative changes across the country in areas such as communications, financial inclusion, e-commerce and e-governance, the need for protecting our citizens' right to privacy and freedom of expression is more pertinent than ever before. Encryption, as a crucial enabler of these rights and liberties, has therefore gained much recognition across public and private domains as the foremost tool for information security. At the same time, the rapid advancement in the use of technology for malicious purposes (such as acts of terror, incitement of crimes, fake news, and sharing of indecent content) has blurred the lines between consumer privacy and national security, and has brought the question of regulating encryption to the forefront of our fast evolving cyber policy.

In this study, we have attempted to envision a framework for the regulation of encryption technologies in India - one that acknowledges the importance of consumer privacy and technological innovation, while not diminishing the role of the government in protecting national security. Through a critical evaluation of the encryption ecosystem, we have presented a rationale for state intervention for the purpose of correcting detrimental market failures. Thereafter, we have undertaken an in-depth analysis of regulatory frameworks across the globe, so as to study best practices in encryption regulation adopted by various countries, and to evaluate their application in the Indian context.

Keeping in mind the unique 'double-edged' nature of encryption, we have sought to balance the interests of public as well as private stakeholders. Through an analysis of the non-negotiables that must be borne in mind by any policy that hopes to oversee encryption, we have arrived at a set of recommendations that are bucketed into two categories - (1) the use of encryption for improving data protection, especially sensitive information; and (2) interception of encrypted information for law enforcement. To strengthen data protection, we recommend bolstering pecuniary damages in case of data breaches and building a publicly available repository of such breaches. We also suggest instituting preventive measures by establishing a voluntary third-party accreditation system of data protection certification/seals. With respect to interception, and to alleviate the challenges that encryption creates for law enforcement, we recommend that service providers and the government work together to develop mechanisms and modify technology, as required, to allow for lawful interception requests to be serviced. We also recommend improving checks and balances in the use of hacking by law enforcement agencies as well as extending legislative support to 'ethical' hacking.

We believe that these recommendations would not only assist our policymakers in protecting the rights and freedoms of Indian citizens', but would also help them build trust among the various encryption intermediaries in order to achieve better public-private cooperation for the country's national security efforts.

Introduction

The significance of data in our personal lives becomes increasingly apparent as our collective existence exceedingly moves online. Technology powered by data defines the way we live and communicate, access public utilities and private services like health and transport systems, and has proven vital to both economic prosperity and national security. The reliance on data in going about our daily lives, and for administering critical infrastructure, makes having to guard against data breaches an invaluable necessity. This is because data breaches have real-world, and often extremely damaging consequences. The average data breach costs $3.86 million, according to the Ponemon Institute.[1] And it is not just private businesses that fall prey to data breaches – the government machinery and government-run utilities do as well. A strong data security setup is therefore critical to helping safeguard data. This is why encryption, being a strong tool in the digital security arsenal, assumes significance.

Encryption - often interchangeably used with the term cryptography - is thought to be one of the best ways to protect data, and can be found, or is referenced to in legislations and self-regulatory guidelines across the globe.[2] In fact, encryption has a long history of use. Humans have resorted to the use of codes and ciphers over a millennia for protecting everything from trade secrets to military strategies and blueprints.[3] The Greeks were known to have used it extensively, as did the Nazis during World War II.[4] Modern encryption that protects data is similar in theory to ancient ciphers. In layman's terms, it protects data - whether at rest or in motion - from prying eyes, by cloaking it with an encryption key, without which it is impossible to transfer data into legible form (thus preventing its disclosure and rendering it useless). That said, encryption isn't a panacea - it is just one step in a long list of steps that can be undertaken to safeguard data. While strong encryption by itself does not prevent data breaches, it does prevent attackers from accessing the stolen data, thus mitigating the overall risk.[5] It is also for this reason that encryption draws flak from government security and law enforcement agencies as it can impede investigations into criminal and terrorist activities.[6]

Encryption technology has gone from being highly restricted under control agreements, to something that now enables digital transactions and everyday communication. Today, there are a number of developers and vendors that provide a variety of encryption products and services.[7] A 2016 global survey counted 865 hardware or software products incorporating encryption from 55 different countries which included products largely from the US (over 300), and Germany (112), followed by the UK, Canada, France and Sweden.[8] India's interface with encryption is seeing a very similar trajectory and an increasing number of technology players are investing in research and development to create encryption based products to offer to Indian consumers. This growing usage of encryption by service providers in the Indian ecosystem has led to calls for the government to step in and regulate it.

In September 2015, motivated by global events, including the 2013 Edward Snowden leaks, the Indian government published a draft Encryption Policy for India which was quickly withdrawn. Beginning 2017, it re-stated its intention of announcing a revised policy.

It is in this context that this study has been undertaken.

---

[1] The 13th annual Cost of a Data Breach Study, The Ponemon Institute (2018), https://www.ibm.com/security/data-breach;

[2] Encryption, The Resource Center International Association of Privacy Professionals (IAPP), https://iapp.org/resources/topics/encryption-3/;

[3] Kaveh Waddel, The Long & Winding History of Encryption, The Atlantic (16/01/2016), https://www.theatlantic.com/technology/archive/2016/01/the-long-and-winding-history-of-encryption/423726/;

[4] Ibid.

[5] Encryption Is a Critical Safeguard Against Data Breaches, Encryption Backgrounder, BSA, https://www.bsa.org/~/media/Files/Policy/Data/BSA_Encrypt_DataBreach-web.pdf;

[6] Encryption, The Resource Center International Association of Privacy Professionals (IAPP), https://iapp.org/resources/topics/encryption-3/;

[7] Encryption Policy in Democratic Regimes: Finding Convergent Paths and Balanced Solutions Report, The EastWest Institute (2018), https://iapp.org/media/pdf/resource_center/ewi-encryption.pdf;

[8] B. Schneier, KSeidel, and S Vijayakumar, A Worldwide Survey of Encryption Products (11/02/2016), https://www.schneier.com/academic/paperfiles/worldwide-survey-of-encryption-products.pdf;

The Contentious Nature of the Encryption Debate

The encryption debate often finds lines drawn in the sand, with one side - usually consisting of businesses that rely on or use data, and their customers - advocating for independence in the use of encryption. They reject policy regulation of encryption, however well-intended. The other side usually consists of government and surveillance agencies who seek to regulate encryption for fear of cyber-crimes and cyber-terrorism ('going dark').[9] They try and regulate its use by either prescribing strong encryption standards for data they deem important – such as financial records or health data[10] – or by seeking ways to reliably access or intercept data by ways of legal interventions such as a court order or legislation.

Methods of obtaining access range from case specific interception requests routed via service providers, to requiring service providers to share decryption keys that could be used on an as-needed basis, to building vulnerabilities/ backdoors into programs for uninhibited access (Clinton Administration's Clipper chip).[11] Regulations that require sharing of decryption keys or call for building vulnerabilities are strongly protested by the cryptography community - the former because it requires placing a huge amount of trust in some agency, which if breached can compromise all data; the latter because it is based on the artificial distinction between 'good guy' interceptors and 'bad guy' interceptors, when all it does is create vulnerabilities that anyone may exploit. Other methods include attempts to mandate low thresholds for encryption, or those that insist service providers utilize only locally created encryption over which the government can exercise control.[12] Again, both methods are also contested by cryptographers who criticize mandatory thresholds as easy to crack and damning to innovation and security, and local encryption as being closed-door and hence not quality tested enough. Needless to say, this is a contentious issue that continues to elude consensus.

Rationale for State Intervention: Market Failures in the Encryption Ecosystem

The encryption ecosystem in India remains largely unregulated as of today and many argue that the government should not intervene in the market. Encryption, at a conceptual level, is a manifestation of a user's *Right to Privacy* and a regulation of encryption that mandates the use of a particular technology or prescribes a lower standard of protection or builds in backdoors for interception will not only violate this *Right to Privacy,* but also affect innovation and development in the sector.

While this argument has merit, it also assumes that the encryption ecosystem operates as a perfect market and poses no externalities or systemic risks. This may not be true. A closer look would suggest that encryption is susceptible to the following **types of market failures: systemic risks, information asymmetry, and negative externalities**. It can be argued that given the potential of market failure, some state intervention may be needed to guide the market forces in the right direction and to prevent broader negative effects on the economy.

Systemic Risks

Encryption technologies have evolved drastically over the years, resulting in a variety of options being available today. However, in the absence of an authority that sets standards for the robustness of encryption technologies, there remains the risk of companies (and even government agencies) using inadequate standards for securing data. Depending on the sectors in which these companies operate, data breaches can have wider system-wide ramifications, thus posing significant systemic risk. The World Economic Forum defines systemic cyber risk as: "The risk that a cyber event (attack(s) or other adverse event(s)) at

[9] More Data Is Available to Law Enforcement Than Ever Before, Encryption Backgrounder BSA The Software Alliance, https://www.bsa.org/~/media/Files/Policy/Data/BSA_Encrypt_AvailabilityData-web.pdf;

[10] Encryption: Why it matters, BSA, The Software Alliance https://encryption.bsa.org/;

[11] Nelson, Michael R, Clinton, Clipper and Crypto, The Hill (09/10/2015), https://thehill.com/blogs/congress-blog/technology/253123-clinton-clipper-and-crypto;

[12] Swire, Peter & Ahmed, Kenesa, Encryption & Globalization, XIII Colum. Sci. & Tech. L., Rev 9 (2012), http://www.stlr.org/cite.cgi?volume=13&article=9;

an individual component of a critical infrastructure ecosystem will cause significant delay, denial, breakdown, disruption or loss, such that services are impacted not only in the originating component but consequences also cascade into related (logically and/or geographically) ecosystem components, resulting in significant adverse effects to public health or safety, economic security or national security."[13]

An example of systemic cyber risk that caused significant widespread damage across industries was the series of distributed denial-of-service (DDoS) attacks in October 2016, targeting systems operated by the Domain Name Service (DNS) provider 'Dyn'.[14] By infecting the anycast servers of Dyn with Mirai Botnets[15] that congested internet traffic, the attackers were able to render major internet platforms and related services unavailable to a large customer base across North America and Europe through a single point of failure.[16]

In the domain of encryption, systemic cyber risk can similarly exist in the form of (1) weak encryption for critical information such as financial or national security data; or (2) in the form of a handful of encrypted software potentially gaining widespread popularity, thereby exposing encrypted data to greater vulnerabilities such as the single point of failure (due to a 'bug' in the software). The presence of a regulatory authority that checks for vulnerabilities and prescribes strong data protection techniques could help portend and correct such a failure.

Information Asymmetry

Another source of market failure in the encryption ecosystem is the information gap that often exists between service providers and consumers.[17] Information asymmetry is prevalent in sectors which are intrinsically technical or complex, such as healthcare, finance and technology, wherein consumers are unlikely to understand the working of the system as well as the service providers. An example of a market where such information asymmetry exists is the insurance market, which is particularly susceptible to what is known as 'adverse selection'.[18] In the case of insurance however, it is the consumers (buyers of insurance) who have more information about their lifestyle and associated risks as compared to the insurers. As a result, insurers often find it hard to price products because they are unable to accurately assess the risks. This information gap often leads to suboptimal provision of required services in the market.

In the case of encryption, the service provider encrypting user data is likely to have more information on the system's working than the consumer, in addition to having better technical capability for understanding the finer details of the entire operation. The resulting information asymmetry could lead to 'adverse selection'. However, in this case, 'adverse selection' is likely to play out in the opposite direction with the consumer buying products that may not live up to the promises made by the service provider. Therefore, in the absence of a regulator that mandates disclosure of certain information, consumer protection and privacy is likely to be put at risk. Ideally, the regulator should be in a position to require technology providers to disclose their encryption standards to the public in intelligible language, such that consumers can take informed decisions.

---

[13] Understanding Systemic Cyber Risk, Global Agenda Council, Global Agenda Council on Risk and Resilience, World Economic Forum, http://www3.weforum.org/docs/White_Paper_GAC_Cyber_Resilience_VERSION_2.pdf;

[14] Sreekanth, Aishwarya & Sri,Prashant & Vartiainen, TeemuDyn DDoS Cyberattack – A Case Study, https://mycourses.aalto.fi/pluginfile.php/457047/mod_folder/content/0/Cyber%20Ghosts.pdf?forcedownload=1;

[15] Weagle, Stephanie, Financial Impact of Mirai Attack on Dyn revealed in New Data (21/02/2017), https://www.corero.com/blog/797-financial-impact-of-mirai-ddos-attack-on-dyn-revealed-in-new-data.html;

[16] Lewis, Dave, The DDoS Attack against Dyn One Year Later, Forbes (23/10/2017), https://www.forbes.com/sites/davelewis/2017/10/23/the-ddos-attack-against-dyn-one-year-later/#3c0baa061ae9;

[17] Greif, Avner, The Fundamental Problem of Exchange: A Research Agenda in Historical Institutional Analysis (Page 253), Department of Economics, Stanford University, USA https://web.stanford.edu/~avner/Greif_Papers/2000%20EREH%20Fundamental%20Problem.pdf;

[18] Jewitt, Ian & Leaver, Clare & Bar-Isaac, Heski, Asymmetric Information and Adverse Selection , Working Paper Series (Jan 2014), Department of Economics, University of Oxford, https://www.economics.ox.ac.uk/department-of-economics-discussion-paper-series/asymmetric-information-and-adverse-selection;

Negative Externalities

While encryption is largely used as a tool to secure data and create a safe ecosystem for information transmission, it may also create negative externalities when the technology is used to create public harm. A growing number of organized crime groups are choosing to use encrypted communications and storage strategies to carry out terrorist activities, financial crimes or other attacks against national security. Case in point is the Paris terrorist attack in November 2015, where the perpetrators used a mix of burner phones, anti-surveillance tradecraft and encrypted communication to plan and coordinate their attack.[19] In August 2015, the Islamic State released a 15-page guide titled "Sécurité Informatique" in its French online magazine Dar al-Islam, demonstrating the importance of secure communications for the group. The guide talks about how to setup Tails, connect to the Tor network to hide one's location and Internet address, create PGP keys, encrypt emails, and use other secure communication tools.[20] With the increasing use of technology in criminal and illegal activities that may threaten national security, governments and law enforcement agencies across the world are particularly concerned about their inability to intercept encrypted communication that may look suspicious. This has led to concerted attempts by governments in several countries, including the US, [21] to find ways to get access to encrypted data.

Moving Ahead with Caution

While these market failures do suggest that there is a need for some government regulation of encryption, the extent and nature of regulation as well as the institutional arrangement of checks and balances required to enforce an encryption policy still need to be determined. An overzealous state can, not only stifle innovation and growth of the market, it may also put its citizens at risk by violating their privacy.

Arriving at a Balanced Perspective: The Motivation for Undertaking this Study

With India poised to become a 5 trillion dollar digital economy, led by digital services such as IT, ITeS, e-commerce and telecom, it is important the country have a robust digital security apparatus that balances compliance with competition, and regulation with innovation. Additionally, given the sheer strength of its internet base, it is very evident that in the future, India will help inform the standards of global digital security. Therefore, it is crucial that the debate on encryption be one that is informative and capable of balancing the often opposing interests of stakeholders that occupy India's digital economy.

The Non-Negotiables - Baseline Requirements for any Encryption Policy

In order to give consideration to all voices, we have bracketed the concerns of the three main stakeholders as follows:

i. The government: All countries often have compelling yet competing concerns when it comes to encryption, and India is no different. On one hand, it looks to encryption as a means to secure data that is critical to national security and safeguards the individual privacy of its citizens. In such instances it may seek to prescribe levels or standards of encryption to reinforce digital security mechanisms. But while encryption products and services are most often used for legal and benevolent purposes such as to protect data and communications, they can just as easily be rendered malevolent by their use for cyber-terrorism, cyber-espionage, child pornography etc. Innovations in domestic encryption technology or the importation of the same thus pose a challenge for successive governments who are

[19] Criminal use of encryption is making things harder for law enforcement (Pg. 12), Encryption: What Is It and Why It Is Important, InternetNZ, https://internetnz.nz/sites/default/files/Encryption_discussion_starter.pdf;

[20] Walton, Richard, Protecting Euro 2016 and the Rio Olympics, CTC Sentinel, Vol 9, Issue 6 (June 2016), https://ctc.usma.edu/app/uploads/2016/06/CTC-SENTINEL_Vol9Iss614.pdf;

[21] As during the Apple Inc. vs. the United States' Federal Bureau court case in the US (2016);

constantly forced to evaluate how tech advancement compares against the necessity of allowing legitimate access to data which has been encrypted. This is because preventing crime, and being able to successfully prosecute it within the state's sovereign power, is a key component of ensuring national security. Oftentimes law enforcement agencies lawfully seize devices, but are unable to access their contents, leading to loss of vital information that could potentially save lives, prevent terrorism, or act as timely evidence to help with prosecution. In such instances, the state seeks legitimate access to data, often by willingly/ intentionally breaching encryption that secures its citizens' privacy, for the greater good of the country. **Given these concerns, any encryption policy must keep in mind two non-negotiables from the point of view of the government: room to prescribe norms for data security of its citizens, and provisions to allow for interception in matters of national security/ law and order.**

ii. Consumers (Individuals): As more Indians aspire to digital connectivity and use online spaces to perform everyday functions that range from banking to e-commerce to communications, they are beginning to realize the risks associated with electronic systems. Consumers therefore express a preference for strong, secure, and robust networks and platforms to conduct transactions on, which businesses catering to them have been attempting to provide. Consumers are also apprehensive of interception by government authorities, especially if such interception is allowed without appropriate checks and balances. It is a legitimate concern for many individuals that governments can also use such powers to target opposition and silence dissent. **As such, from a consumer's point of view, the ability to maintain the privacy of their online transactions and communications is a non-negotiable, that may only be compromised for a narrow range of clearly identified and legitimate purposes such as anticipated threats to national security or public order, or in the case of violation of some law.**

iii. Industry: The safe, uninterrupted, and efficient movement of data sustains the interconnected and interoperable global nature of today's digital environment. More and more Indian businesses are harnessing online spaces to become a part of this formal, thriving global ecosystem. Such businesses take the protection of end-user data very seriously, as integrity of data ensures increased consumer confidence, and generates greater trust in the digital economy, thereby spurring growth and innovation. Companies therefore ask that policymakers defend the integrity of encryption technologies and work to expand its use across public and private stakeholders. If under extreme duress to allow law enforcement access to data which has been encrypted, they believe it must not be unbridled access; rather it must be minimally invasive and legally mandated access backed by checks and balances. **The industry would want that India's position on encryption is not one that dilutes the overall security apparatus, or burdens them with regulatory compliance, or one that creates a trust deficit in customers, and the economy at large. More crucially, they would want to ensure that India sends the right message out as being a market-ready and investment-friendly economy.**

The aim is to present an analysis that helps deconstruct the issues faced by each stakeholder in the ecosystem – be it government, consumers or businesses - so as to arrive at a balanced perspective on how to best achieve a trusted digital economy.

Encryption in the Larger Universe of 'Data Protection'

Data - like any other physical asset - is not immune to exploitation or misuse (either by state or non-state actors), and there is a growing recognition across the world, of the need to keep the private data of citizens confidential and secure. With most information today being stored digitally and transmitted using the internet or other computer networks, it is imperative for handlers of such information to employ technologies keeping in mind the nature of digital data and the best ways to secure it

from malicious attacks (whether it is data in use, data at rest or data in transit[22]). To secure data, most systems use a combination of techniques, including (but not limited to) encryption, authentication processes (stringent password and username norms) and authorization practices (usually by restricting access to information).

Encryption: Only One Piece in the Complex Data Protection Architecture

While technological protection of the highest standard is imperative for securing digital data, it is important to keep in mind that technology is evolving rapidly - and so is the domain of data protection. There may not be a 'one size fits all' solution to making various kinds of sensitive data absolutely safe, and any regulation aimed at providing guidance to organizations and entities that work extensively with data must first stress on the importance of building an overarching ecosystem of data security - one that goes beyond a few technological controls and takes a more holistic view for keeping sensitive data safe.

Following from this logic, it is important to keep in mind that in the larger ecosystem of data protection, encryption - though one of the most popular and effective data security methods used by organizations - is by no means the only method of securing data (and neither is it a standalone solution for achieving that end). There are various ways that organizations, particularly those that use or host web-based applications, choose to secure their data from malicious attacks, some of which include tightened norms for access control, authentication management, write protection, pseudonymization and anonymization.

According to a list of "Top 10 Vulnerabilities" developed by the Open Web Application Security Project (OWASP)[23] - an international non-profit community that aims to build awareness of the most common exploits that hackers use to infiltrate and compromise data - "sensitive data exposure due to a lack of proper encryption" is **only "one of the"** insecurities faced by applications. A simple analogy for this scenario is the idea of securing one's house before leaving the premises in order to protect it from burglars: A rational person, before stepping out, chooses to bolt the windows, draw the curtains, perhaps take extra care to stow valuables in a place difficult to penetrate, and lastly, lock the prime entrance of the house as a final or added layer of security. While doing this, the person also ensures that no secondary doors leading into the house remain unlocked either, through which a trespass could be made easier for a burglar. It is important to stress that encryption is like the final lock on the house - an extra layer of security on an already secure apparatus.

Encryption, while it may be one of the most powerful ways to keep data safe, can be rendered ineffective in the presence of another vulnerability in the security architecture of an application. In that stead, a well-rounded data security strategy must not only emphasize the importance of using the most powerful tools to protect against data breach, but also encourage the deployment of operational standards, strong punitive damages for data breaches, and other measures that contribute towards an ecosystem that promotes data protection.

Vulnerabilities in the Encryption Ecosystem

Encrypted systems may also be prone to vulnerabilities and attacks. For instance, in a standard system, the encryption program may be different from the program which is used to create the message before it is sent out, or store it after it has been received. Messages may also be generated, stored, or transmitted through third party systems, which may involve multiple instances of encryption and decryption. Further, the risk may be exacerbated if the encrypted messages are being transmitted using a public channel.

[22] Note: The three states of data have been explained in detail in the Appendix

[23] OWASP Top Ten Vulnerabilities Project, Veracode, https://www.veracode.com/directory/owasp-top-10;

To make encryption more secure, end-to-end encryption is sometimes used. As part of this system, there is no point where the message is raw, i.e., unencrypted and often messages are transmitted using a private/ secure channel. However, end-to-end encryption does not imply that the message being transmitted cannot be hacked. There could be instances where a person uses a third party app keyboard on his device to type the message. If the third party app keyboard is embedded with malware, hackers could read messages as they are being typed onto a messaging app that uses end-to-end encryption.[24]

Threats such as backdoors in the system or brute force attacks may further endanger the security of the protected data. A 'backdoor' refers to a weakness in the software that may either be created intentionally, or by accident. Discovery of a backdoor by a hacker could potentially risk the encrypted data. Hackers may also use brute force attacks by trying every possible combination of the key till they find the correct key. This means that for a 56 bit encryption, over 72 quadrillion keys are possible, and under a brute force attack all of these keys may have to be tried to decrypt the data. While in practice such attacks may be infeasible at the moment, the increasing power of computing machines may make such attacks possible in the future. Further, the possibility of a breach may be exacerbated by unsafe key generation, improper key storage, not using rotating keys, or using weak algorithms.[25]

Note for Policymakers

Keeping this in mind, any policy that aims to regulate encryption with the motive of making data more secure must also acknowledge encryption's place in the overall architecture of information security - which is, that it is only one cog in an extremely complex and rapidly evolving machine that works to protect the integrity of certain data. A policy that is sapient in this regard will also recognize the limits of regulatory capacity beyond the purview of what encryption can achieve, and will aim to strike a balance between taking a completely holistic or completely granular view of data protection.

The Indian Regulatory Landscape: Past and Present

While India does not have a unified encryption framework, it has laws and policies that attempt to either limit encryption or gain access through decryption.[26] Broadly speaking, our regulatory framework is spread across a few legislation and sector-specific regulations. In fact, it is the confusion caused by varying standards prescribed by the government and regulators that has prompted calls for a single framework that sets standards for all encryption.

Relevant Legislation

The Indian Telegraph Act 1885 allows the government to lawfully intercept and monitor communication (such as phone-tapping). The Information Technology Act 2000, cognizant of the changing nature of technology, extends these powers to electronic media but also prescribes mechanisms to secure electronic transactions through means such as encryption. In addition to giving powers to the government to prescribe methods for encryption,[27] Section 43A of the Act requires handlers of sensitive personal data to adopt 'reasonable security practices and procedures' to safeguard data, and makes them liable to pay damages in cases of negligence.

---

[24] Bhushan, Kul, Whatsapp and user privacy: Your top questions answered, Hindustan Times (21/08/2017), https://www.hindustantimes.com/tech/whatsapp-and-user-privacy-your-top-questions-answered/story-uxOHtRiuNQV8NCrgC8oaVJ.html;

[25] A3:2017, Sensitive Data Exposure, Top 10 2010-A7-Insecure Cryptographic Storage, OWASP (2017), https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf;

[26] Prakash, Pranesh & Grewal, Japreet How India regulates Encryption, Center for Internet & Society (30/10/2015), https://cis-india.org/internet-governance/blog/how-india-regulates-encryption;

[27] Note: Schedule V (Glossary) of the Indian IT Rules, 2000 describes 'Encryption', as "The process of transforming plaintext data into an unintelligible form (cipher text) such that the original data either cannot be recovered (one-way encryption) or cannot be recovered without using an inverse decryption process (two-way encryption)."

Sector-Specific Regulation

Where legislation has largely been silent on encryption standards, these have been stipulated by various sector regulators in India:

- *SEBI* - SEBI specifies that: (i) data in transit should be encrypted using 128-bit encryption, and (ii) encryption will be used for internet-based trading, and that the Department of Telecom policy on encryption will govern the system.[28]
- *RBI* - RBI requires banks to protect data at rest and in transit using encryption.[29] It specifies that at least 128-bit encryption should be used, and with advances in technology, larger key lengths may be introduced periodically.[30] The RBI has also released guidelines for Non-Banking Financial Companies (NBFCs), which specify that those providing mobile financial services must provide for end-to-end encryption.[31] It also requires NBFCs using social media to use encryption and secure connections to prevent the risk of malware distribution and account takeovers.
- *UIDAI* - AADHAAR authentication API specification requires that Personal Identity Data (PID) data should be encrypted with a dynamic session key that should use 2048 bit encryption.[32]
- *Department of Telecom (DoT)*: The IT Security Guidelines state that electronic communication systems used for the transmission of sensitive information, must be equipped with suitable security software and, if necessary, with an encryption software.[33] Further, it mandates the evaluation and approval of encryption equipment, prohibits bulk encryption, and mandates the use of maximum 40 bit key length for encryption.[34] For higher level encryption, DoT mandates seeking written permission and deposit of decryption keys with them.[35]
- *Ministry of Health & Family Welfare*: The Electronic Health Records Standards, 2016 released by the Ministry[36] specify that all personally identifiable recorded patient data will have to be protected against unauthorized access, especially during transmission (e.g., healthcare provider to provider, or healthcare provider to patient). The standards specify that all electronic data must be encrypted and decrypted using the best available key strength (i.e., minimum 256-bit).

Restrictions/Exemptions on Encryption[37]

Certain communication license agreements set out restrictions on encryption. For instance, the Internet Service Provider (ISP) License Agreement requires ISPs to obtain prior governmental approval to deploy encryption which is higher than 40 bits.[38]

---

[28] Circular no. CIR/MRD/DP/25/2010 on 'Securities Trading using Wireless Technology', Chapter 2 - Trading Software and Technology, Securities and Exchange Board of India, https://www.sebi.gov.in/sebi_data/commondocs/chapter2trading_p.pdf;

[29] 'Cyber Security Framework in Banks', Reserve Bank of India, 02/06/2016, https://rbidocs.rbi.org.in/rdocs/notification/PDFs/NT41893F697BC1D57443BB76AFC7AB56272EB.PDF;

[30] Guidelines on Information security, Electronic Banking, Technology risk management and cyber frauds, Reserve Bank of India, https://rbidocs.rbi.org.in/rdocs/content/PDFs/GBS300411F.pdf;

[31] Master Direction - Information Technology Framework for the NBFC Sector, Reserve Bank of India (08/06/ 2017), https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=10999;

[32] 'Security breaches of UIDAI database', Starred Question No. 117, Rajya Sabha, answered on 10/03/ 2017, https://uidai.gov.in/images/rajyasabha/RS_SQ_117_answered_on_10032017.pdf;

[33] Waris, Salman, Dua Associates, Encryption in India, TheIndianLawyer250, (06/06/2013), http://indianlawyer250.com/features/article/81/encryption-india/;

[34] Clause 2.2 (vii) of the ISP License, Department of Telecommunication (DoT) License with Internet Service Providers (2010), www.dot.gov.in/sites/default/files/L%20A%20after%2025.01.10%281%29_0.doc;

[35] DOT - ISP License agreement, Ministry of Communications & IT, Department of Telecommunications (06/08/1999), http://dot.gov.in/sites/default/files/amendment_isp_6-8-1999_0.pdf?download=1;

[36] Notification on Electronic Health Record Standards for India, e-Health Section, Ministry of Health and Family Welfare (30/12/2016), https://mohfw.gov.in/sites/default/files/17739294021483341357.pdf;

[37] Taken from TRAI Recommendations on Privacy, Security and Ownership of the Data in the Telecom Sector (June, 2018), https://trai.gov.in/sites/default/files/RecommendationDataPrivacy16072018_0.pdf;

[38] Note: Part 1, Clause 2(vii). The Unified License agreement (Clause 37.1), the Unified Access Services License agreement (Clause 39.1), and the ISP license agreement (Part 1, Clause 2(vii)) all prohibit bulk encryption by a Telecom Service Provider (TSP);

However, this is only applicable to ISPs and TSPs. WhatsApp and other messaging services are, on the other hand, excluded from this requirement by virtue of being OTT or 'Over-The-Top' Services.[39]

Existing Framework to Intercept Communication in India

The current procedure for intercepting telecommunication is outlined in the Indian Telegraph Act, 1885, and for digital communication in the Information Technology Act, 2000.[40,41] These laws allow for communication to be intercepted on the grounds mentioned in the table below.

Table 1: Grounds for lawful interception of communication

Indian Telegraph Act, 1885[42]	Information Technology Act, 2000
Sovereignty and integrity of India	Sovereignty and integrity of India
-	Defence of India
Security of the state	Security of the state
Friendly relations with foreign states	Friendly relations with foreign states
Public order	Public order
Preventing the incitement or commission of an offence	Preventing the incitement or commission of a cognizable offence
-	Investigation of an offence

The law states that law enforcement agencies can initiate interception by getting a written approval from any of the following authorities: (i) Secretary, Ministry of Home Affairs (central government), (ii) Secretary-in charge, Home Department (state government), or in unavoidable instances by (iii) an officer not below the rank of Joint Secretary to the Government of India, (if authorized by the Union or State Home Secretary).

Chain of Command & Other Procedures

The chain of command with respect to interception runs the gamut from the *Investigating Officer* (who puts in the request) to the *Assistant Commissioner of Police,* to the *Deputy Commissioner of Police,* to the *Joint Commissioner of Police*, to the *Special Commissioner*, to the *Commissioner of Police* before reaching the *Home Secretaries*.[43] That said, under certain circumstances, the Head or the second senior most officer (at the rank of the Inspector General of Police) may also grant approval, subject to it being confirmed by the Union or State Home Secretary within a stipulated period.[44,45]

[39] Regidi, Asheeta, Supreme Court dismisses PIL against WhatsApp, but the fight for encryption is yet to begin, FirstPost (30/06/2016), https://www.firstpost.com/tech/news-analysis/supreme-court-dismisses-pil-against-whatsapp-but-the-fight-for-encryption-is-yet-to-begin-3684633.html;

[40] The Indian Telegraph Act, 1885, http://dot.gov.in/sites/default/files/Indian%20Telegraph%20Act%201885.pdf?download=1;

[41] The Information Technology Act, 2000, https://www.meity.gov.in/writereaddata/files/The%20Information%20Technology%20Act%2C%202000%283%29.pdf'

[42] Note: In addition to the relevant provisions under the Indian Telegraph Act and Rules relating to interception, a Standard Operating Procedure (SOP) has also been issued by the Department of Telecommunications (DoT), in consultation with Ministry of Home Affairs (MHA), dated 24th December 2014 for Lawful Interception and Monitoring for Telecom Service Providers (TSPs);

[43] From stakeholder conversations with law enforcement officials; names withheld on request;

[44] Rule 419A, The Indian Telegraph Rules, 1951, http://dot.gov.in/sites/default/files/358%20GI-2014%20dated%208.2.2014_6.pdf?download=1;

[45] The Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules 2009, https://meity.gov.in/writereaddata/files/Information%20Technology%20%28Procedure%20and%20Safeguards%20for%20Interception%2C%20Monitoring%20and%20Decryption%20of%20Information%29%20Rules%2C%202009.pdf;

Upon approval, these directions remain in force for sixty days, and are forwarded to certain intercepting authorities and conveyed to the licensees (i.e., service providers) to begin interception. All aspects of the interception are thoroughly documented. The directions also specify the purpose for which the intercepted communication may be used.

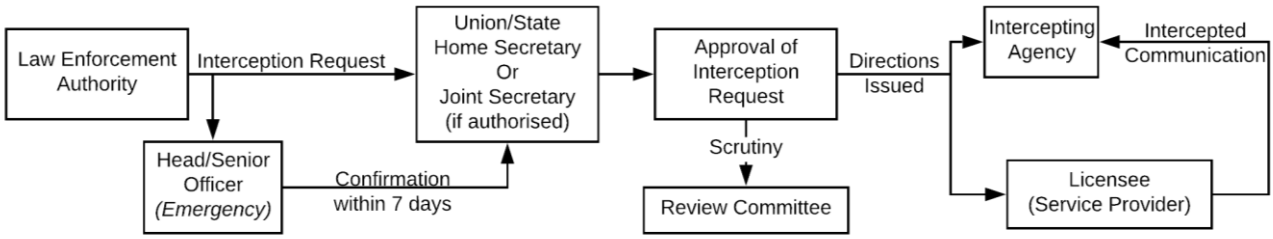
Oversight Mechanism - Review Committee

A Review Committee has been established under Rule 419-A(16) of the Indian Telegraph Rules at both the central and the state level, as per which, every order issued by the relevant government officials has to be sent to the Review Committee.[46] The Committee comprises three members: (i) Cabinet Secretary (Chair), (ii) Secretary, Legal Affairs, and (iii) Secretary, Department of Telecommunications. Committee comprising people at equivalent positions also exists at the state level.

The Review Committee is required to meet once every two months and if it is unconvinced about the legality of an interception order, it may set it aside.[47] Where such interception has been carried out as a result of an emergency, the government is to be notified within 3 working days, and the interception has to be confirmed within 7 working days, without which the interception will have to cease. Under such circumstances, in order to intercept the same message, the prior approval of Union or state Home Secretary is required. A similar Review Committee has also been established under Rule 22 of the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules 2009, and follows similar direction as the above.[48]

However, barring the inclusion of the Secretary, Legal Affairs in the Review Committee, there is no judicial oversight over the interception process. This has resulted in some researchers claiming that the grounds for interception, particularly those under the Information Technology Act (which are wider than under the Telegraph Act), may need stronger safeguards.

Figure 1: Process to intercept communication



Sources: The Indian Telegraph Act, 1885; and The Information Technology Act, 2000.

In addition to the provisions specified in these laws, the Unified Access Services License, which is granted to service providers to operate their services, also mentions various requirements and conditions to facilitate interception requests.[49] For instance, it specifies that the Telegraph Act, 1885 will prevail in case of any contradiction between the law and the license terms. Further, it requires the licensee to provide tracing facilities for intercepting communication passing through its network to all officers of the central government (including police, excise, customs, and the intelligence department). This access will have to

[46] Rule 419A of the Indian Telegraph Rules, 1951, The Center for Internet & Society, https://cis-india.org/internet-governance/resources/rule-419-a-indian-telegraph-rules-1951;

[47] Ibid.

[48] Data Interception order by Home Ministry kicks off row, The Economic Times (New Delhi) (22/12/ 2018), https://economictimes.indiatimes.com/news/politics-and-nation/data-interception-order-by-home-ministry-kicks-off-row/articleshow/67202212.cms;

[49] Ch-4, Regulatory Framework for OTT Communication Services (12/11/2018), TRAI, https://main.trai.gov.in/sites/default/files/CPOTT12112018.pdf; Model Unified Access Services License Agreement, Department of Telecommunication, http://dot.gov.in/sites/default/files/UAS%20license-agreement-19-12-2007.pdf?download=1;

be provided where it is required for investigation, crime detection, or in the interest of national security. Necessary facilities will also have to be provided to the government to prevent espionage, sabotage, or any other unlawful activity.

Indian Case Law

A. BlackBerry

In 2008, the Indian government asked BlackBerry-maker Research in Motion (RIM) to decrypt messages on demand or hand over their decryption key.[50] The messaging services (BBM) offered 2 kinds of services in India - if it was a company, they installed the local Blackberry Enterprise Server (BES) leading to all corporate consumer messages being routed through the BES with strong encryption. This business offering was its most popular service, said to have been servicing 1 million Indian users in 2010.[51] For individuals, RIM had an unencrypted BlackBerry Internet Service (BIS) network, which could be intercepted as plaintext, provided the local carrier removed any transport layer encryption it had added.[52] RIM submitted that it did not have the keys to decrypt BES messages.

After the 2008 Mumbai attacks, the Indian government sought access to BBM messages since they were reported to have been used by terrorists during the attacks. On being denied the same, they threatened to ban BBM services in India. Finally, in 2013, BlackBerry agreed to give the Indian government the ability to intercept data sent over BlackBerry devices.[53] But, by then, the Indian government appeared to have dropped its previous demands to access BlackBerry's Enterprise Servers. Instead, BlackBerry agreed to notify the authorities about which companies were using the enterprise service.[54]

B. Whatsapp

In June 2016, Sudhir Yadav, a Haryana-based right-to-information (RTI) activist, filed a petition at the Supreme Court alleging that from April 2016, WhatsApp had started to enable every message with 256-bit encryption that could not be broken; this would, according to the petitioner, prove fertile ground for terrorist activities, and pose a national security threat to India. Whatsapp, during 2016 was reported to have 160 million Indian users.[55] His PIL further contended that WhatsApp's encryption system prevented compliance with Indian laws such as Section 69 of the Information Technology Act, 2000 and Section 5 of the Indian Telegraph Act, 1885 which give the government the power to direct interception of messages under certain situations, such as a public emergency or in the interest of national security.[56] Both the laws in question were applicable to WhatsApp, and also to other messaging apps like Viber, Telegram, etc., since they amount to an 'intermediary' under the Information Technology Act, and the messages sent through them amount to a 'telegraph' under the Telegraph Act.[57] However, according to Whatsapp, it could not comply with such a demand because it uses end-to-end encryption, wherein only the sender and the receiver of the message hold the key. The petitioner was, as a result, seeking a ban on Whatsapp and

[50] Prasad, Rishabh The Irresolvable BlackBerry [BBM] Controversy, YouthKiAwaaz (2010), https://www.youthkiawaaz.com/2010/08/the-irresolvable-blackberry-bbm-controversy/;

[51] Willis, Amy, India threatens to ban Blackberry services, The Telegraph (12/08. 2010), https://www.telegraph.co.uk/technology/blackberry/7940964/India-threatens-to-ban-BlackBerry-services.html;

[52] Acharya, Bhairav, Breaking ranks with Asia: The case for encrypting India, ORF (21/02/ 2017), https://www.orfonline.org/expert-speak/breaking-ranks-with-asia-the-case-for-encrypting-india/;

[53] Shubber, Kaddhim BlackBerry gives Indian government ability to intercept messages, The Wired (11/07/2013), https://www.wired.co.uk/article/blackberry-india;

[54] Ibid.

[55] Number of monthly active WhatsApp users in India from August 2013 to February 2017 (in millions), Statista, https://www.statista.com/statistics/280914/monthly-active-whatsapp-users-in-india/;

[56] Regidi, Asheeta, Supreme Court dismisses PIL against WhatsApp, but the fight for encryption is yet to begin, FirstPost (30/06/2016), https://www.firstpost.com/tech/news-analysis/supreme-court-dismisses-pil-against-whatsapp-but-the-fight-for-encryption-is-yet-to-begin-3684633.html;

[57] Ibid.

other such apps.[58] However, the Supreme Court asked the petitioner to approach TDSAT (Telecom Disputes Settlement and Appellate Tribunal) instead, and dismissed the case.[59]

Case Study: Sharing of Unlawful Content on Encrypted Platforms

Some popular messaging apps use end-to-end encryption for messages being exchanged by users, such that the messages may be decrypted using keys only available with the sender or the receiver. Given the encryption used, law enforcement agencies often find it difficult to decrypt these conversations, making interception impossible. The messaging apps have claimed that there is no room in the technology for interception, and that these apps themselves cannot access the messages that are being transmitted.

The inability of law enforcement agencies to intercept communication over these apps has also led to these mediums being used to exchange unlawful content, such as child pornography especially via groups created for disseminating such content.[60,61] This poses a unique challenge since the apps claim that they cannot read or intercept conversations owing to the strong encryption used. The issue was also raised in a recent case filed before the Supreme Court of India relating to the removal of imagery and video content on child pornography, rape, and gang rape.[62]

Given issues in interception, many governments across the world have focused their energies on establishing group membership and tracking down offenders who bypass the law, rather than insisting that companies break encryption or introduce backdoors. For instance, authorities in Europe and South America coordinated their efforts and arrested approximately 40 people believed to have been involved in sharing child pornography on encrypted social media messaging apps.[63] In the United States, there have been similar instances where authorities have traced people storing unlawful content on encrypted storage devices. In such scenarios, courts have ordered the owner of such devices to be detained till they allow law enforcement agencies to access them.[64]

In India, authorities have also initiated similar action against offenders. For instance in August 2018, Mumbai Police arrested five people who were involved in sharing child pornography on a social media messaging group.[65] Police initiated action after one of the group members approached them with a complaint against the content being shared. The authorities then tracked down the addresses of the offenders through their phone numbers.[66] In a similar incident, the Madhya Pradesh Police tracked down members of an encrypted messaging app, who were involved in sharing child pornography on messaging groups.[67]

[58] Supreme Court to hear plea ban on Whatsapp, FirstPost (23/06/2016), https://www.firstpost.com/india/supreme-court-to-hear-plea-to-ban-whatsapp-2852498.html?utm_source=FP_CAT_LATEST_NEWS;

[59] Shukla, Suchi Supreme Court Refuses To Ban WhatsApp, Asks Petitioner To Approach Centre, NDTV News (29/06/2016), https://www.ndtv.com/india-news/supreme-court-refuses-to-ban-whatsapp-asks-petitioner-to-approach-government-1425890;

[60] 'WhatsApp has a child porn problem', Business Insider India (21/12/2018), https://www.businessinsider.in/whatsapp-has-a-child-porn-problem/articleshow/67185938.cms;

[61] 'Whatsapp has an encrypted child porn problem, Tech Crunch (20/12/2018), https://techcrunch.com/2018/12/20/whatsapp-pornography/.

[62] Order, Re: Prajwala Letter Dated 18.2.2015 Videos of Sexual Violence and Recommendations, Suo Moto Writ Petition (Criminal) No. 3/2015, 06/12/2018, https://www.sci.gov.in/supremecourt/2015/6818/6818_2015_Order_06-Dec-2018.pdf;

[63] Police break up WhatsApp child porn image sharing network across Europe and Latin America, The Straits Times (19/04/2017), https://www.straitstimes.com/world/europe/police-break-up-whatsapp-child-porn-image-sharing-network;

[64] Man jailed until he unlocks encrypted hard drives in child abuse images case, The Digital Guardian (23/03/2017), https://www.theguardian.com/technology/2017/mar/23/francis-rawls-philadelphia-police-child-abuse-encryption;

[65] WhatsApp group sharing child porn busted, 5 held, The Times of India, 04/08/2018, https://timesofindia.indiatimes.com/city/mumbai/whatsapp-group-sharing-child-porn-busted-5-held/articleshow/65263327.cms;

[66] Child porn on WhatsApp: Invite to join group shared through Facebook, claim cops, The Indian Express (09/08/2018), https://indianexpress.com/article/cities/mumbai/child-porn-on-whatsapp-invite-to-join-group-shared-through-facebook-claim-cops-5293007/;

[67] Madhya Pradesh cops bust child porn WhatsApp group, The New Indian Express (25/04/2018), http://cms.newindianexpress.com/nation/2018/apr/25/madhya-pradesh-cops-bust-child-porn-whatsapp-group-1806074.html;

Police authorities in other parts of the country, such as Uttar Pradesh, have also been successful in tracking down offenders through other means which include tracing links being shared on the internet for joining such groups.[68]

Analysis of the 2015 National Encryption Policy (NEP)

In September 2015, motivated by global events, including the 2013 Edward Snowden leaks, the Indian government came out with a draft Encryption Policy for India. Among other things, the policy suggested that encryption algorithms and key sizes will be prescribed from time to time, and if stronger keys were used, these must be deposited with the government. The policy also stipulated that a user store encrypted messages sent/ received by them in plain text form for 90 days, and reproduce them when asked for by law enforcement personnel.

Problems with the policy became apparent very quickly. Cyber security experts raised concerns over government's attempts to prescribe encryption algorithms and key sizes. This was considered regressive and inhibiting of innovation in the security space. That service providers would be required to deposit decryption keys where their encryption algorithms were above a particular standard also attracted criticism, because it would lead to setting up central key escrows, which could be vulnerable to attacks from unwanted third parties. Objections were also raised regarding the issue of forcing internet users to maintain information in text form and exposing it to additional vulnerabilities. Government noted that ambiguity in some portions may have led to misgivings, and swiftly rolled it back in the face of the confusion it created.

In 2017, the government initiated steps to revise the encryption policy recommendations by consulting stakeholders. In 2018, it indicated its intention to re-introduce the policy.

Regulatory Frameworks for Encryption across the Globe

Despite the positive gains that encryption offers to society in terms of privacy, encryption is, in fact, a double-edged sword - it also creates the possibility of secure communications being deployed by terrorists, criminals and others whose activities are subject to government investigation and oversight. The stake held by encryption in the domain of national security has brought the question of its governance onto the centre stage of cyberspace policies, and governments across the world are taking measures to regulate, oversee, or set guidelines for encryption in ways they feel are best suited to their national interests.

For the purpose of this inter-country analysis, we look at the **two broad categories of ways that governments have chosen to regulate encryption:**

A) Prescribing rules for the way encryption can and must be used (whether through a comprehensive data protection policy, or through industry-specific/ sector-specific policies and standards), and

B) Mandating access for interception in cases of threats to law and order/ national security.

Below, we provide an overview of the same through a combination of case studies, and an inter-country comparison table. Additional details on country-specific legislation and enforcement mechanisms are available in the appendix.

Regulations/Guidelines regarding 'The Use' of Encryption for Consumer Data Protection[69]

Some countries such as the USA rely on a sectoral model, with no single overarching law that dictates how encryption must be used - instead, the use of encryption is overseen (through minimal prescription) by multi-faceted guidelines from regulators,

[68] Indore police bust WhatsApp-based global child porn racket, The Week (18/04/2018), https://www.theweek.in/news/india/2018/04/18/indore-police-bust-whatsapp-based-global-child-porn-racket.html;

[69] Refer to Appendix II for further details on sectoral and overarching models of encryption frameworks;

and is often appended by civil litigation and high regulatory fines in case of data breaches. On the other hand, the EU GDPR serves as an overarching data protection regime that subsumes encryption across sectors. Article 32 of the GDPR specifically talks about the implementation of appropriate technical and organizational measures to ensure a level of security appropriate to the risk, and defines 'appropriate technical measures' to include pseudonymization and encryption.

What stands out as a common factor in countries such as EU member states, the USA and the UK is the heavy reliance on civil law to ensure the appropriate use of encryption technologies for data protection, and less of an emphasis on setting down prescriptive mandates for companies to comply with. This idea of 'working backwards' from the point of a data breach (heavy pecuniary damages lead to the adoption of stricter information security protocols by service providers, thereby translating into a stronger ecosystem of overall data protection) is highly effective in countries with strong civil law, and generally, preemptive measures such as prescriptive standards for the use of encryption are not utilized in such cases.

On the other hand, in Japan, the "Act on the Protection of Personal Information" (APPI) requires personal information to be secured and allows sectoral regulators to scale up individually to enforce the APPI as they deem most appropriate, thereby ensuring a more preemptive regime of data protection rather than one than relies on civil law alone as a deterrent.

Table 1: Models for regulating the use of encryption – Sectoral or Overarching

Country	Model for Encryption 'Use' Regulation	Governing Legislation
USA	**Sectoral:** There is no single overarching encryption regulation. Historically US federal law has regulated data protection and consumer privacy on a sectoral basis, focusing specific regulations on financial services and health care providers.	**Financial data:** The Gramm-Leach-Bliley Act (1999) **Health data:** The Health Information Portability and Accountability Act (1996)
Australia	**Sectoral:** No single overarching law on encryption. Strong encryption standards are encouraged for financial and medical data, but not specified.	The Privacy Act 1988 is the core legislation on information security. The Privacy Amendment (Enhancing Privacy Protection) Act 2012 strengthens it.
Switzerland	**Overarching**: One overarching data protection law that prescribes guidelines for the disclosure of personal data across sectors such as financial, healthcare and telecom - thereby subsuming encryption. Sectoral laws exist, but must scale up to match the overarching data protection law.	Swiss Data Protection Act (FADP) - revised in 2017
Japan	**Overarching:** One single overarching data protection law that subsumes encryption requirements across sectors such as healthcare, financial and telecom. The law is enforced by the respective sector regulators.	Act on the Protection of Personal Information – APPI (2003)
UK	**Overarching:** One single law on Data Protection that subsumes encryption requirements across sectors such as healthcare, financial and telecom. The law is enforced by the respective sector regulators.	The Data Protection Act (2018) - UK's implementation of the EU's General Data Protection Regulation (GDPR)

Case Study: Data Privacy/Protection Certification in the European Union

Based on the premise that seals and other certification mechanisms can help bridge 'information asymmetry' and offer customers the ability to quickly verify the adequacy of a company's information security protocols, a range of countries such as the USA,[70] Japan,[71] France[72] and other members of the European Union[73] have experimented with the idea of accreditation bodies that conduct periodic data security audits, albeit with different base designs.

Before the GDPR came into force in 2016, the EU Data Protection Directive 95/46/EC (adopted in 1995) regulated the processing of personal data within the European Union. Despite the fact that this directive had no clear-cut provision on certification, various privacy seals businesses and schemes sprung up across Europe - some at the EU level (such as the EuroPriSe seal,[74] developed by an EU-funded research project), and some at the national level - based on individual member states' legislation. In all cases, the data protection certification mechanisms were not mandatory measures, but optional decisions.

In their study on the EU data privacy certifications market,[75] scholars Kamara and De Hert write that very few companies chose to go for the certifications, primarily because of the expenses involved and the lack of value addition to their businesses. It also seemed that there was a general absence of public trust and confidence in the multiple certification schemes. These factors paved the way for the official regulatory endorsement and the inclusion of certification in the EU GDPR, starting with the 2012 European Commission proposal.[76] This proposal highlighted the instrumental role certification and trust marks can play in the promotion of compliance with the GDPR, but it still did not specify who the issuing body for certificates was to be, or what the procedure of certification was.[77] The risk associated with such flexibility was the creation of a market that was overcrowded with certification products that offer no assurance of actual protection.

By 2016, there were approximately thirty active trust mark schemes within the European Union,[78] and the market was highly fragmented. According to the European Consumer Centres Network's "Can I trust the trust mark?" report, navigating the European trust mark landscape was comparable to "navigating a jungle."[79] The multiplicity of trust marks brought confusion and consumers remained under-informed about the meaning and value attached to them. Another EU-specific issue was the lack of multilingual information and coordination between the various trust mark schemes. This led to a further fragmentation of the market for data protection certifications, and the lack of proper oversight became apparent once again.[80]

---

[70] Cavoukian, Ann & Chibba, Michelle, Privacy Seals in the USA, Europe, Japan, Canada, India and Australia. Rodrigues, R. & Papakonstantinou, V. (eds.), Privacy and Data Protection Seals, Information Technology and Law Series 28, Pg 65, https://doi.org/10.1007/978-94-6265-228-6_5;

[71] Cavoukian, Ann & Chibba, Michelle, Japan - Privacy Mark. Rodrigues, R. & Papakonstantinou, V. (eds.), Privacy and Data Protection Seals, Information Technology and Law Series 28, Pg 73, https://doi.org/10.1007/978-94-6265-228-6_5;

[72] Carvais-Palut, Johanna, The French Privacy Seal Scheme. Rodrigues, R. & Papakonstantinou, V. (eds.), Privacy and Data Protection Seals, Information Technology and Law Series 28, Pg. 49, https://doi.org/10.1007/978-94-6265-228-6_5;

[73] Kamara, Irene & De Hert, Paul, Data Protection Certifications in the EU. Rodrigues, R. & Papakonstantinou, V. (eds.), Privacy and Data Protection Seals, Information Technology and Law Series 28, Pg 7, https://doi.org/10.1007/978-94-6265-228-6_5;

[74] About EuroPriSe – The European Privacy Seal, https://www.european-privacy-seal.eu/EPS-en/About-europrise;

[75] Kamara, Irene & De Hert, Paul, Data Protection Certifications in the EU. Rodrigues, R. & Papakonstantinou, V. (eds.), Privacy and Data Protection Seals, Information Technology and Law Series 28, Pg 9, https://doi.org/10.1007/978-94-6265-228-6_5;

[76] Note: European Commission 2012, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), http://www.europarl.europa.eu/RegData/docs_autres_institutions/commission_europeenne/com/2012/0011/COM_COM(2012)0011_EN.pdf;

[77] Kamara, Irene & De Hert, Paul, Data Protection Certifications in the EU. Rodrigues, R. & Papakonstantinou, V. (eds.), Privacy and Data Protection Seals, Information Technology and Law Series 28, Pg 12, https://doi.org/10.1007/978-94-6265-228-6_5

[78] Rodrigues, R. & Papakonstantinou, V. (eds.), Privacy and Data Protection Seals, Information Technology and Law Series 28, Pg 92, https://doi.org/10.1007/978-94-6265-228-6_5

[79] Trust marks report 2013 "Can I trust the trust mark?", The European Consumer Centres' Network https://www.konsumenteuropa.se/globalassets/rapporter/trust_mark_report_2013.pdf;

[80] Balboni, Paolo & Dragan, Theodora, Controversies and Challenges of Trustmarks: Lessons for Privacy and Data Protection Seals. Rodrigues, R. & Papakonstantinou, V. (eds.), Privacy and Data Protection Seals, Information Technology and Law Series 28, Pg 93, https://doi.org/10.1007/978-94-6265-228-6_5;

The EU GDPR dealt with some of the problems mentioned above by laying down more precise specifications regarding certifications and trust marks. The relevant provisions are included in Articles 42 and 43 of the GDPR, complemented mainly by Articles 57, 58, 64, 70 and 83. **Data protection certification under GDPR is completely voluntary** (Article 42(3)).[81] Additionally, the data protection certification mechanism laid down in the GDPR relies on third-party certifications. In contrast with self-regulation schemes such as Privacy Shield,[82] the certification mechanism under GDPR is audited by third party independent certification bodies, and supervised by data protection authorities (i.e., Information Commissioners) in individual member states of the EU.

According to scholars Kamara and De Hert, the GDPR's position on data protection certification seems to be an attempt to satisfy both market and industry needs for certification schemes, seals, and marks, while addressing self-regulation skeptics, as well as the demands for regulatory oversight, to strike a fine balance between opposing interests.[83]

Regulations/Laws regarding Interception of Encrypted Information

Interception by law enforcement agencies is often cited as the biggest bone of contention between the government and the industry/ civil society members, and our analysis of international examples indicates that a peaceful (and stable) common ground is difficult to locate. Various countries have chosen to regulate the use of encryption for the purposes of national security - through court issued warrants, licensing, or mandating backdoor access for law enforcement agencies, and their governments have frequently faced opposition from civil society groups for the same. Where governments have not received adequate cooperation from private enterprises (and other governments), they have also, as in the case of USA and UK, chosen to subvert encryption through hacking to cater to their states' national security interests.

Countries such as China, Russia, and Australia have laid down regulations to govern or limit the use of encryption by private companies in a manner that allows the state to maintain supervisory access over all information collected and processed by the companies. In Russia, for instance, the Federal Law[84] specifies that a license will be required for the following activities related to encryption: (i) distribution, (ii) operation, (iii) providing services, and (iv) development and manufacturing of encryption facilities and related telecommunication systems. The People's Republic of China Cyber Security Law, enacted in 2017, covers telecom operators, internet firms, network operators, financial institutions, insurance companies, securities companies, foundations, and providers of cyber security and network services.[85] Compliance with the law is mandatory, and it prescribes penalties for non-compliance.

In a similar vein, the Australia Parliament recently passed the "Assistance and Access Bill"[86] which gives Australian law enforcement agencies the power to issue cooperation notices to technology entities with the purpose of gaining access to specific users' encrypted messages and data. According to some cyber security experts, this could be the catalyst for the creation of a 'global weak point' for international tech companies.[87] The new law will allow Australian law enforcement agencies to compel tech companies to grant them access to encrypted data containing user information, even if the service utilizes end-to-end encryption. Moreover, if a company claims that it cannot access the information, authorities could demand

[81] Kamara, Irene & De Hert, Paul, Data Protection Certifications in the EU. Rodrigues, R. & Papakonstantinou, V. (eds.), Privacy and Data Protection Seals, Information Technology and Law Series 28, Pg 25, https://doi.org/10.1007/978-94-6265-228-6_5;

[82] The Privacy Shield Framework, https://www.privacyshield.gov/EU-US-Framework;

[83] Kamara, Irene & De Hert, Paul, Data Protection Certifications in the EU. Rodrigues, R. & Papakonstantinou, V. (eds.), Privacy and Data Protection Seals, Information Technology and Law Series 28, Pg 14, https://doi.org/10.1007/978-94-6265-228-6_5;

[84] Russian Federal Law on Encryption, https://www.wto.org/english/thewto_e/acc_e/rus_e/WTACCRUS58_LEG_37.pdf;

[85] Cybersecurity Law of the People's Republic of China, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/;

[86] Pierce, Jadzia, Australia Proposes New Encryption Legislation, Inside Privacy, https://www.insideprivacy.com/international/australia-proposes-new-encryption-legislation/;

[87] Australia data encryption laws explained, BBC, https://www.bbc.com/news/world-australia-46463029;

that they build tools to do so.[88] In the wake of the Bill's assent, Apple sent a letter to the Australian government in which it stated that encryption is a public good that is beneficial to citizens and actually protects against cyber-attacks and terrorism.[89] Civil society members in Australia have also expressed concerns regarding the global implications of this legislation, saying that this could set a precedent and have an adverse impact on individual privacy across the globe.[90]

In countries like Japan however, if law enforcement agencies require access to encrypted data for criminal investigation, they may approach the courts to seek permission and the court may pass an order requiring a person to cooperate with the authorities and assist them in decrypting data. However, the person cannot be penalized if he or she refuses to cooperate.[91]

Some countries, such as the USA and the UK, have overarching legislation on surveillance and investigation that subsume encrypted communications without particularly singling them out. The legislative framework in these countries is detailed out in the case studies that follow.

Case Study: Interception of Encrypted Information in the United States of America

Early users of encryption methods in the US were industry players such as the banking and finance sectors. In 1993, the Clinton administration attempted to introduce the "Clipper Chip[92]" - an encryption software to be used by technology companies that could also give the government and law enforcement agencies 'backdoor' access to encrypted data on personal devices. Legal scuffles, sharp public criticism, and dissent from technology and privacy experts led to what was known as the 'crypto wars', which culminated in the US government dismantling its efforts at propagating the software. A major concern among US-based technology companies was also that weak encryption standards on their devices was creating adverse impressions about their products internationally, especially in light of the availability of stronger encryption software outside the U.S., and limiting their sales and growth.

In terms of the overall surveillance and investigation of sensitive data in the United States, three primary laws govern the domain: The Foreign Intelligence Surveillance Act (FISA), The USA Patriot Act, and The USA Freedom Act. FISA was enacted in 1978 and governed both the physical and electronic surveillance of primarily foreign powers and agents. The Patriot Act, enacted shortly after the September 11, 2001 terrorist attacks, was essentially an amendment to FISA that expanded the surveillance powers of American Authorities[93] (FBI, CIA, NSA and American Armed Forces) in their acquisition of confidential information on individuals, including those not directly linked to terrorist groups. Under the Patriot Act, the FBI could order a person or company to produce documents to protect against the risk of terrorists or foreign spies without a court order.[94] Although the Patriot Act was set to expire in 2015, many provisions of the Patriot Act were extended by the Freedom Act, but with more limitations on surveillance due to public scrutiny in the wake of the Edward Snowden revelations regarding bulk surveillance and interception.[95] Since 2015, the National Security Agency and other agencies can now only request company records regarding a specific person, account, or device, after providing substantial evidence that the entity

[88] Porter, John, Australia passes controversial anti-encryption law that could weaken privacy globally, https://www.theverge.com/2018/12/7/18130391/encryption-law-australia-global-impact;

[89] Statt, Nick,Apple argues stronger encryption will thwart criminals in letter to Australian government, https://www.theverge.com/2018/10/12/17971444/apple-iphone-stronger-encryption-letter-australian-assistance-and-access-bill-2018;

[90] Porter, John, Australia passes controversial anti-encryption law that could weaken privacy globally, https://www.theverge.com/2018/12/7/18130391/encryption-law-australia-global-impact;

[91] Government Access to Encrypted Communications: Japan, United States Library of Congress, https://www.loc.gov/law/help/encrypted-communications/japan.php;

[92] Karsten, Jack & West, Darrell, A Brief History of US Encryption Policy, The Brookings Institute, https://www.brookings.edu/blog/techtank/2016/04/19/a-brief-history-of-u-s-encryption-policy/;

[93] Leclerq, Quentin, Extraterritorial Effects of the US Patriot Act – Privacy Rights of Non-American Citizens, Lecours + Hebert, https://lecourshebert.com/en/extraterritorial-effects-usa-patriot-act-privacy-rights-non-american-citizens/;

[94] Bischoff, Paul, A Breakdown of the Patriot Act, Freedom Act and FISA, Comparitech, https://www.comparitech.com/blog/vpn-privacy/a-breakdown-of-the-patriot-act-freedom-act-and-fisa/#What_is_the_Patriot_Act;

[95] Lyon, David, Surveillance, Snowden and Big Data, Sage Journals https://journals.sagepub.com/doi/full/10.1177/2053951714541861;

under scrutiny is associated with a foreign power or has ties with terrorism. The Freedom Act also requires intelligence agencies to bring more transparency in their data collection mechanisms, including the removal of gag orders that used to prevent tech companies from informing customers when their private data was being given to the federal agencies.[96]

Specific to the communications sector in the US, The Communications Assistance for Law Enforcement Act (CALEA) of 1994 forced telephone companies to redesign their network architectures to make it easier for law enforcement to wiretap digital telephone calls. In 2005, CALEA was expanded by the Federal Communications Commission (FCC) to include Internet Service Providers (ISPs) and VoIP services like Skype. However, the obligations under CALEA fall only upon telecommunications carriers, and they relate only to the interception of information in transit.[97]. Shortly thereafter, the FBI began referring to the challenges created by encryption as 'going dark'[98], and sought to bring all internet communications under the purview of CALEA. Among other things, the FBI was particularly interested in introducing a new requirement that all communications systems give it 'backdoors' into their encryption systems. The proposal was met with public discontent and never came to pass, but it threw into sharp focus the national security vs. privacy debate that has traditionally guided the discourse on encryption-regulation in the United States.

The FBI vs. Apple Case

A more recent example of the same debate - one that took the US by storm in 2016 - was the FBI's attempts to force Apple Inc. to develop a software that would enable the Bureau to undertake criminal investigations and prosecutions by extracting data from encrypted Apple devices.[99] Apple maintained that the FBI was, instead of taking the proper legislative course of action, abusing the "All Writs Act of 1978" (which says that federal courts can issue 'all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law')[100] and proposing a risky precedent of exposing their customers to greater risk under the garb of national security. With the FBI taking Apple Inc. to court, the case marked one of the largest confrontations on encryption in the history of the United States. While the hearing in the case never took place (since FBI sourced a third-party to unlock the particular iPhone in question[101]), it spurred the narrative on data privacy in the country, culminating in a call for the ENCRYPT (Ensuring National Constitutional Rights for Your Private Telecommunications) Bill[102] that could set standards for encryption-services nationwide. The proposed ENCRYPT Bill will prevent governments from storing keys for on-demand use by law enforcement agencies, and also prevent governments from compelling companies to weaken their encryption products and services.[103]

Use of hacking by the government in the USA

The deployment of hacking by the government in the US expanded with the perpetuation of FBI's 'going dark' narrative, and it is now known that private-sector digital forensics companies in the USA such as Cellebrite[104] make devices that investigators

[96] Bischoff, Paul, A Breakdown of the Patriot Act, Freedom Act and FISA, Comparitech, https://www.comparitech.com/blog/vpn-privacy/a-breakdown-of-the-patriot-act-freedom-act-and-fisa/#What_is_the_Patriot_Act;

[97] Hurwitz, Justin, Encryption, Congress Mod (Apple + Calea), Pg. 404, Harvard Journal of Law and Technology, https://jolt.law.harvard.edu/assets/articlePDFs/v30/30HarvJLTech355.pdf;

[98] Savage, Charlie, US Tries to Make it Easier to Wiretap the Internet, The New York Times (29/09/2017), https://www.nytimes.com/2010/09/27/us/27wiretap.html?ref=charlie_savage&pagewanted=1&pagewanted=all;

[99] Kharpal, Arjun, Apple. vs. FBI: All You Need to Know, CNBC (29/03/2016), https://www.cnbc.com/2016/03/29/apple-vs-fbi-all-you-need-to-know.html;

[100] Richards, Neil & Hartzog, Woodrow, Apple v the FBI: why the 1789 All Writs Act is the wrong tool, The Guardian (25/02/2016), https://www.theguardian.com/technology/2016/feb/24/apple-v-the-fbi-why-1789-all-writs-act-is-the-wrong-tool;

[101] Pramuk, Jacob, Govt successfully breaks into San Bernardino shooter's iPhone, CBN (28/03/2016), https://www.cnbc.com/2016/03/28/doj-expected-to-withdraw-ca-case-against-apple-usa-today-citing-govt-official.html;

[102] The US ENCRYPT Act of 2016, https://www.congress.gov/bill/114th-congress/house-bill/4528/text;

[103] Ruiz, David, The ENCRYPT Act Protects Encryption from U.S. State Prying, Electronic Frontier Foundation (11/06/2018), https://www.eff.org/deeplinks/2018/06/encrypt-act-protects-encryption-us-state-prying;

[104] Law Enforcement in the USA and Cellebrite, https://www.cellebrite.com/en/law-enforcement/;

can use in the field or in a forensics lab to extract and analyze data from locked devices while maintaining data integrity for later evidentiary use in court. That is, by accessing the device, investigators may gain access to messages they could not read 'on the wire' due to end-to-end encryption. Information about the use of such means by the government has received a strong reaction from civil society and privacy rights groups who assert that indiscriminate use of lawful hacking can create a culture of data insecurity and make citizens' data less secure and therefore vulnerable to dangerous, third-party malicious attacks.[105]

Case Study: Interception of Encrypted Information in the United Kingdom

The "Regulation of Investigatory Power Act (RIPA), 2000" is the primary law governing surveillance and investigation in the United Kingdom.[106] It provides a framework involving warrants and oversight, said to be in compliance with the European Convention on Human Rights.[107] Section 49 of RIPA also confers on authorities the power to demand that encryption keys be handed over to them, in case they possess a lawfully seized device containing encrypted information. Such authorities have to seek prior permission from a judge, and the entire process is overseen by the Intelligence Services Commissioner appointed under the Act. In addition to the 2000 Act, the United Kingdom has other laws as well which allow for interception of communication. The government has also acknowledged that it uses powers under the Intelligence Services Act, 1994, and Police Act, 1997 to authorize hacking.[108]

In the wake of revelations by Edward Snowden, the United Kingdom set up a committee in 2014 to review operation and regulation of investigatory powers available with law enforcement and intelligence agencies. This review was particularly focused on interception of communication.[109] The report of the committee highlighted the evolving nature of encryption and certain difficulties faced by authorities while decrypting information. It suggested that an Independent Surveillance and Intelligence Commission be set up and given powers related to interception, encryption, and decryption.

Following recommendations by this committee and a few others, the United Kingdom enacted the Investigatory Powers Act, 2016 (colloquially known as the Snooper's Charter).[110] The Act introduced new powers and re-emphasized existing ones for the intelligence and law enforcement agencies to carry out targeted and bulk interception of communications. It created an Investigatory Powers Commission (IPC) comprising of former and senior judges to oversee the use of all investigatory powers. The Act required that communication service providers retain a user's 'internet connection records' for one year; it also allowed for 'equipment interference' which is the practice of hacking into people's devices and computers to access data. Companies in the UK were also legally obliged to assist agencies with targeted interception of data and have the ability of remove/ bypass encryption.[111] The law separates 'equipment interference' or government hacking into two categories: bulk and targeted. Targeted hacking allows the law enforcement agencies to focus on an individual or a specific device, while bulk hacking can be used against a group of individuals to obtain overseas communication.

[105] Government Hacking and the Subversion of Digital Security, Electronic Frontier Foundation, https://www.eff.org/issues/government-hacking-digital-security;

[106] The Regulation of Investigatory Powers Act, 2000, https://www.legislation.gov.uk/ukpga/2000/23/pdfs/ukpga_20000023_en.pdf;

[107] Briefing Paper on the Investigatory Powers Bill, UK House of Commons Library (11/03/2016), http://researchbriefings.files.parliament.uk/documents/CBP-7518/CBP-7518.pdf;

[108] Ibid.

[109] Anderson QC, David, A Question of Trust: Report of the Investigatory Powers Review (11/06/2015), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/434399/IPR-Report-Web-Accessible1.pdf;

[110] Investigatory Powers Act, 2016, http://www.legislation.gov.uk/ukpga/2016/25/pdfs/ukpga_20160025_en.pdf;

[111] UK Surveillance Powers Explained, BBC (05/11/2015), https://www.bbc.com/news/uk-34713435;

Subsequent to its enactment, the law was challenged in the UK High Court, which ruled that it was incompatible with EU law.[112] The government accepted that it was inconsistent since it did not limit the retention of data only for the purposes of combating 'serious crimes' and was not subject to prior review by a court or an independent body. The government therefore introduced this requirement among other changes during an amendment to the law in 2018.[113]

Table 2: Grounds for intercepting communications in various countries

Country	Grounds	Sanctioning Authority
India	1. Sovereignty and Integrity of India 2. National Security 3. Friendly relations with foreign states 4. Public Order 5. Preventing incitement or commission of offence	1. Secretary, Ministry of Home Affairs 2. Joint Secretary, Government of India (if authorized) 3. Secretary, Home Department (state government)
Australia	1. National Security 2. Defence of Australia 3. Conduct of International Affairs 4. Murder, kidnapping, narcotics, terrorism, arson, drug trafficking, bribery, corruption, money-laundering, cyber-crime, or loss of life	1. Attorney General 2. Director General of Security, Australian Security Intelligence Organization (in certain circumstances)
China	1. National Security 2. Investigate criminal activities 3. Terrorism	(No known explicit requirement)
Japan	1. Matters related to crime 2. Drug and Organized Crimes	1. Court Order
USA	1. Violation of criminal laws 2. Sabotage 3. Terrorism 4. Fraudulent identity 5. Kidnapping, murder, extortion, rioting, and piracy 6. Arson, bribery, possession of weapons, trafficking, slavery, and bank fraud 7. Counterfeiting, narcotics or currency fraud 8. Extortionate credit transactions	1. Court Order 2. Attorney General, Deputy Attorney General, and Associate Attorney General
UK	1. National Security 2. Prevent or detect crime 3. Safeguard economic well being	1. Secretary of State (i.e., Home Secretary)

Sources: **India** - Telegraph Act, 1885, Information Technology Act, 2000; **China** - National Cyber Security law of China, 2017, National Security Law, 2015; **United States of America** - Title 18, Crimes and Criminal Procedure, The Foreign Intelligence Surveillance Act, 1978; **Australia** - Telecommunications (Interception and Access) Act, 1979; **United Kingdom** - Regulation of Investigatory Powers Act, 2000.; **Japan** - Act on Wiretapping for Criminal Investigation.

[112] Cobain, Ian, UK has six months to rewrite snooper's charter, high court rules, The Guardian (27/04/2018), https://www.theguardian.com/technology/2018/apr/27/snoopers-charter-investigatory-powers-act-rewrite-high-court-rules;

[113] Data Retention and Acquisition Regulations 2018, https://www.legislation.gov.uk/ukdsi/2018/9780111170809;

Use of Hacking: By Ethical Hackers and Governments

Ethical Hacking: As a Way of Strengthening the Data Protection Ecosystem

The difference between hacking and ethical hacking is intent. While hackers (also known as 'black hats') break into systems and use the points of entry to promote illegal activity or steal confidential information, ethical hackers (known as 'white hats') also break into systems, but do so with an altruistic purpose in mind.[114] In cases of ethical hacking, it is usually done with prior knowledge and permission, and with the express purpose of understanding vulnerabilities so as to prevent malicious hacking. Most ethical hackers are contracted by either businesses or the government to aid them, or work with public establishments as consultants or employees. However, many also serve as security researchers in public interest, by analyzing, exploring, and fixing the vulnerabilities that are scattered across the digital landscape, unsolicited.[115]

The legal twilight zone surrounding ethical hacking

Despite the benefits to ethical hacking, it remains a hazardous occupation in many countries. This is because laws governing ethical hacking are currently inadequate and vague,[116] thereby causing them to attract civil or criminal suits. This is amply illustrated by the 2013 case of a Dutch Member of Parliament Henk Krol who was fined €750 (US$1,000) by the district court of Oost-Brabant for breaking and entering the system of the Dutch medical laboratory Diagnostics for You.[117] The journalist turned MP who had hacked into the system just months before he was elected to the Dutch parliament, insisted that he had acted in his capacity as a journalist and ethical hacker at the time of the breach, and sought to highlight vulnerabilities in the system.[118] While the Dutch court was willing to accept the public interest angle to his case, they fined him on account of going public without giving the medical lab enough time to fix the problem,[119] and for the "disproportionate" amount of records he accessed, saying he had gone "further than necessary" to achieve his aim.[120]

The above usually emanates from the fact that for an act to be considered a crime, it usually requires both ill intention and the physical act to go together; however, most countries that have laws penalizing cyber intrusions - such as Germany (under S.202a of the German Criminal Code[121]) or Belgium (under Art. 550(b) of the Criminal Code[122]) - only require the physical act of unauthorized intrusion, and do not specifically require the unlawful element of maliciousness or ill-intent to be attached to it. The US, known for being home to one of the largest community of 'bug bounty-hunters', also suffers from poor protection being afforded to them. There are two major federal statutes under which security researchers might be held liable in the course of their work in the US - the Computer Fraud and Abuse Act (CFAA) and S.1201 of the Digital Millennium Copyright

---

[114] Synopsys, What is ethical hacking?, https://www.synopsys.com/software-integrity/resources/knowledge-database/ethical-hacking.html;

[115] Rodriguez, Katitza, From Canada to Argentina, Security Researchers have rights - Our Report, Electronic Frontier Foundation (16/10/2018), https://www.eff.org/deeplinks/2018/10/canada-chile-security-researchers-have-rights-our-new-report;

[116] Pal, Kaushik, Do Ethical Hackers need Legal Protection, (24/01/2018), Technopedia.com, https://www.techopedia.com/do-ethical-hackers-need-legal-protection/2/33135;

[117] Essers, Loek, Dutch MP fined for hacking into medical file system, Good Gear Gudie (15/02/2013), https://www.goodgearguide.com.au/article/453927/dutch_mp_fined_hacking_into_medical_file_system/;

[118] Leyden,John, Dutch MP must cough €750 for hacking into medical lab, The Register UK (19/02/2018), https://www.theregister.co.uk/2013/02/19/dutch_mp_ethical_hacking_fine/;

[119] Essers, Loek, Dutch MP fined for hacking into medical file system, Good Gear Gudie (15/02/2013), https://www.goodgearguide.com.au/article/453927/dutch_mp_fined_hacking_into_medical_file_system/;

[120] Leyden, John, Dutch MP must cough €750 for hacking into medical lab, The Register UK (19/02/2018), https://www.theregister.co.uk/2013/02/19/dutch_mp_ethical_hacking_fine/;

[121] Note: Data espionage (Section 202a, German Criminal Code): (1) Whosoever unlawfully obtains data for himself or another that were not intended for him and were especially protected against unauthorized access, if he has circumvented the protection, shall be liable to imprisonment not exceeding three years or a fine; (2) Within the meaning of subsection (1) above data shall only be those stored or transmitted electronically or magnetically or otherwise in a manner not immediately perceivable – https://www.lewik.org/term/15706/data-espionage-section-202a-german-criminal-code/;

[122] Note: Article 550(b) of the Criminal Code: §1 specifies, "Any person who, aware that he is not authorized, accesses or maintains his access to a computer system, may be sentenced to a term of imprisonment of 3 months to 1 year and to a fine of (Bfr 5,200-5m) or to one of these sentences." Further provisions speak about fraudulent intent and drive up the penalty even further - http://www.cybercrimelaw.net/Belgium.html;

Act (DMCA).[123] Each Act makes illegal a particular subset of hacking, by focusing on individuals gaining unauthorized access to protected technological devices, and leaves little leeway for security researchers to escape liability.[124] Additionally, both these statutes criminalize the very investigation involved in security research, as opposed to any use or publication of the results.[125]

The India scenario

Indian hackers have long topped bug bounty charts of Facebook, Uber, Google and other companies,[126] and India also has colleges and Universities offering dedicated courses in ethical hacking. Despite this, like many of its global counterparts, Indian laws do not offer any greater clarity, preferring to let ethical hacking remain a grey area. Section 43 of the Information Technology (IT) Act, 2000, prescribes penalties and compensation for damage done to computer systems,[127] where '*any person, without permission of the owner or any other person who is in charge of a computer, computer system or computer network*' commits any of the acts described. This is a highly enumerative provision that includes several actions and covers a variety of activities that could make security researchers liable under civil charges. In 2008, S. 66 of the IT Act was amended to impose criminal charges for actions undertaken under S. 43, when the same are done 'dishonestly' or 'fraudulently', leading to an imprisonment term which may extend to three years or with fine which may extend to five lakh rupees or both. For security researchers/ ethical hackers, this means that even if their actions do not possess the intention required to convict them under S. 66, they could still attract civil penalties under Section 43 if they trespass computer systems without any intention to harm. In other words, India's IT law does not protect ethical hackers unless probably they are employed by the government under Section 84 wherein their actions are protected in good faith.[128]

The absence of adequate legal protection puts Indian ethical hackers/ security researchers in a quandary on whether or not to pursue and publicly reveal security flaws they may encounter, which could prove to be fatal for the country's national security apparatus and businesses in the long term. The 2014 *Net Losses: Estimating the Global Cost of Cybercrime* report jointly released by the Center for Strategic and International Studies (CSIS) and McAfee, estimated that the likely annual cost to the global economy from cyber-crime was more than $400 billion, with India alone assessed to be losing 0.21% of its GDP to cyber-crime each year.[129] It therefore suggested that organizations build robust cyber-defense strategies to combat the same. This includes proactively identifying threats, responding to them once detected, via thorough investigation, and finally incorporating findings into assessments to ensure security protocols are adequately updated. Given the pro-activeness angle, there is a definite need to ensure that India's security researchers/ hackers are incentivized.

However, with Indian laws defining crimes in the context of unauthorized access, most hackers and security researchers are reluctant to report security flaws.[130] When they do, under best case scenarios, organizations patch vulnerabilities without acknowledging efforts of the Indian hacker.[131] In fact, reports allude to Indian hackers reaching out to public organizations like the ISRO or the BSNL to report flaws, and being ignored at best, or being slapped with legal notices at worst.[132] **Such a scenario is extremely disheartening, because ethical hacking can, if incentivized, provide an alternate method to**

[123] Etcovich, Daniel, and Thyla van der Merwe. 2018. Coming in fromthe Cold: A Safe Harbor from the CFAA and the DMCA §1201 for Security Researchers. Berkman Klein Center Research PublicationNo. 2018-4. Assembly Publication Series, Berkman Klein Center forInternet & Society, Harvard University, https://dash.harvard.edu/bitstream/handle/1/37135306/ComingOutoftheCold_FINAL.pdf?sequence=1

[124] Ibid.

[125] Ibid.

[126] Christopher, Nilesh, BSNL, ISRO cases show India not a country for ethical hackers, The Economic Times (13/03/ 2018), https://economictimes.indiatimes.com/tech/internet/bsnl-isro-cases-show-india-not-a-country-for-ethical-hackers/articleshow/63278882.cms;

[127] "Penalties & Adjudication", under the IT Act, MEITY, http://meity.gov.in/content/offences;

[128] Section 84 in The Information Technology Act, 2000

[129] Net Losses: Estimating the Global Cost of Cybercrime, The Center for Strategic and International Studies (CSIS) (05/06/2014), https://www.csis.org/analysis/net-losses-estimating-global-cost-cybercrime;

[130] Christopher, Nilesh, BSNL, ISRO cases show India not a country for ethical hackers, The Economic Times (13/03/2018), https://economictimes.indiatimes.com/tech/internet/bsnl-isro-cases-show-india-not-a-country-for-ethical-hackers/articleshow/63278882.cms;

[131] Ibid.

[132] Ibid.

strengthening the country's digital security apparatus, without having to resort to prescribing standards for encryption.

Use of Hacking by Governments of Different Countries

With encryption being increasingly seen as an investigative barrier, law enforcement agencies sometimes resort to hacking (exploiting vulnerabilities in IT systems, implanting software etc.) as a technique to gain access to a system to intercept communications or read stored information. They assert that such practices improve security without systematically weakening encryption through backdoors or other similar methods.[133]

Law enforcement may rely on ethical hackers for assistance too, since all agencies are not equally equipped with adequate tools to tackle cyber-crime and cyber-terrorism. For example, in the United States, the Food and Drug Administration (FDA) consulted with ethical hackers in order to assess vulnerabilities in the medical devices of Medtronic.[134] In India, there have been some reported instances of ethical hackers assisting the police in solving crime, however the exact mechanics of collaboration are not clear. In 2017, a media report suggested that a group of engineering students helped the Gurgaon Police in investigating a cyber-crime case relating to defamation and harassment.[135]

Laws relating to government hacking in different jurisdictions

Globally, the law in a jurisdiction may not explicitly mention government hacking, but may deal with it under the larger ambit of interception. While in some instances the law is well defined with respect to hacking for legitimate interception purposes, it can also exist in a legal vacuum. In such instances, hackers working for the government do not necessarily suffer from criminal liability, but their authority to access data for investigation and possibly surveillance exists in a grey area.

Where the law explicitly allows hackers to aid the government in intercepting information, such hackers are said to indulge in 'lawful' hacking. In France, a 2016 amendment to the Code of Criminal Procedure allows for the possibility of remotely accessing computer data by a law enforcement agency, provided there is judicial oversight.[136] Similar is the case with Poland. In the United Kingdom, provision for lawful hacking has been provided by the Investigatory Powers Act 2016, and is defined as 'equipment interference'.[137] While Italy is in the process of drafting a proper legislation for lawful hacking, currently law enforcement agencies are permitted to employ lawful hacking tools once they get approval from the public prosecutor and the judge presiding over the investigation.[138] Germany lies in an interesting position – while the German Code of Criminal Procedure carries no specific provision on lawful hacking, the 2009 Federal Police Office Act permits law enforcement agencies to intercept data with means of information technology systems, subject to certain conditions.[139] A court order is required to engage in lawful hacking, and all data collected is to be screened to identify any data concerning the private life of

[133] Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices, Study for the Libe Committee by the European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs (2017), http://www.europarl.europa.eu/RegData/etudes/STUD/2017/583137/IPOL_STU(2017)583137_EN.pdf;

[134] Newman, Lily Hay, A New Pacemaker Hack Puts Malware Directly on the Device, Wired (18/09/2018), https://www.wired.com/story/pacemaker-hack-malware-black-hat/;

[135] Dhankar, Leena. Ethical hackers help police check rising cybercrimes in Gurgaon. https://www.hindustantimes.com/gurugram/ethical-hackers-advise-caution-to-net-users/story-S3hcmpPn3HrtDb5s5FysRK.html;

[136] Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices, Study for the Libe Committee by the European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs (2017), http://www.europarl.europa.eu/RegData/etudes/STUD/2017/583137/IPOL_STU(2017)583137_EN.pdf;

[137] Wong, Ian Joon, The UK Government has been hacking for years - and now its legal! The Quartz (17/02/2017) https://qz.com/617582/the-uk-government-has-been-hacking-for-years-and-now-its-legal/;

[138] Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices, Study for the Libe Committee by the European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs (2017), http://www.europarl.europa.eu/RegData/etudes/STUD/2017/583137/IPOL_STU(2017)583137_EN.pdf;

[139] Ibid.

an individual, which must be deleted immediately, and is considered inadmissible in court.[140] Law enforcement agencies are also required to notify anyone targeted by lawful hacking.[141]

Lawmakers and experts both recognize that **government hacking has the "potential for increased invasiveness when compared with traditional coercive activities (e.g. wiretapping, house searches etc.)"** because in many cases, a hack can provide law enforcement with several gigabytes or terabytes of data, which may include a much larger volume of sensitive information about a person than may have been available through traditional means. This is also the reason why different UN bodies have recommended the need for appropriate safeguards as well as the importance of **judicial authorizations**.[142]

Security risks of government hacking

Even as there is increasing use of hacking by governments across the world, there is no doubt that the same has a series of risks attached to it, beginning with the threat to an individual's fundamental right to privacy as well as freedom of expression and information. There is also the concern that use of governmental hacking by law enforcement could potentially weaken the security apparatus of the overall system, leaving it vulnerable to malicious abuse. This is often a result of how investigative agencies tend to focus on 'zero day vulnerabilities' (which are vulnerabilities that are 'discovered and exploited prior to public awareness or disclosure to the vendor'[143]), which they may then choose not to reveal to vendors. Such a system may also offer security firms an impetus to discover more zero-day vulnerabilities and create a zero-day market, though the ethics of doing so may be questioned.[144] Also, there is a chance that the government may lose control of these hacking tools or vulnerabilities due to say, insufficient security measures, leading to hostile elements making use of the same.[145] For example, in 2016, a group of hackers broke into an NSA server and stole numerous hacking tools, which they later posted online for free – a move which had far-reaching consequences.[146] Moreover, lawful hacking would be difficult to monitor and regulate if used by various law enforcement agencies at different levels of the government.[147] Equally problematic is the possibility of over-reach by investigative bodies.

Use of hacking by the government in India

In India, government hacking, if it exists, operates in a grey area. The Information Technology Act, 2000 is the major law regulating government monitoring of information. While it does not explicitly speak about hacking by the government, it does make legal, avenues for government interception, which could potentially include hacking. The Act requires intermediaries to extend support to government agencies for accessing and decrypting information.[148] However it does not detail out the means that the government may employ when the required support is either not extended, or proves to be ineffective.

[140] Ibid.

[141] Ibid.

[142] Ibid.

[143] Bellovin, S.M., Blaze, M., Clark, S. and Landau, S., Lawful hacking: Using existing vulnerabilities for wiretapping on the Internet. Nw. J. Tech. & Intell. Prop., 12, p. i. 2014.

[144] Pfefferkorn, Riana. "Security Risks of Government Hacking". https://cyberlaw.stanford.edu/files/publication/files/2018.09.04_Security_Risks_of_Government_Hacking_Whitepaper.pdf

[145] Ibid.

[146] Nakashima, Ellen, Powerful NSA Hacking Tools have been revealed online, The Washington Post (16/08/2016), https://www.washingtonpost.com/world/national-security/powerful-nsa-hacking-tools-have-been-revealed-online/2016/08/16/bce4f974-63c7-11e6-96c0-37533479f3f5_story.html?utm_term=.e0aef0ba7682;

[147] Encryption Policy in Democratic Regimes: Finding Convergent Paths and Balanced Solutions Report, The EastWest Institute (2018), https://iapp.org/media/pdf/resource_center/ewi-encryption.pdf;

[148] Section 69 (1) of the Information Technology Act read with the "Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009";

Meeting the Non-Negotiables: Possible Solutions to Big Challenges

The meteoric rise of the internet and related services indicate that data will play a crucial role in deciding the course of India's economic and political future. Keeping this in mind, it is important to recognize that there is immense value in creating an ecosystem of overall information security in the country (across sectors and verticals), which can serve as the bedrock for creative and futuristic technologies to flourish. This is why the issue of regulating encryption - as one of the foremost mechanisms of keeping data safe - is one that every government must approach with caution and good judgement.

All through this study, we have applied two lenses to the regulation of encryption – (1) its use for protecting information; and (2) interception of encrypted information for law enforcement. Basis the analysis discussed in the preceding pages, we now try and present a set of potential solutions that could possibly help align the diverging objectives – of respecting privacy and maintaining law and order - to meet the non-negotiables of all stakeholders – consumers, businesses and the government.

Recommendations with respect to the 'Use' of Encryption for Data Protection

I. Working Backwards: Bolstering Pecuniary Damages and Building a Repository of Data Breaches

A) Pecuniary Damages

Various jurisdictions around the world have laws which impose heavy fines or penalties for data breaches. This is often combined with a requirement to notify users if their data has been hacked. Both these legal requirements help put pressure to ensure that service providers voluntarily use state of the art technology for data security. Often, these encourage organizations to use high levels of encryption to protect data, even in the absence of specific guidelines with respect to the same.

While Section 43A of the Information Technology Act in India requires service providers to undertake 'reasonable security practices and procedures'[149] and makes them liable to pay compensation for data breaches when an aggrieved party approaches the adjudicating authority, the penalties and/ or other legal requirements are not as strict as in the case of the EU GDPR.

The EU-GDPR, which came into effect in 2018, specifies the fine which may be imposed on an organization in case of an offence (such as violations in obtaining consent, failure to implement measures related to data security, or violations of provisions related to transferring data to third countries). Offences have been clubbed under two broad categories. Under the first category, a fine of up to EUR 10,000,000 or 2% of the worldwide annual turnover of the company in the preceding financial year may be imposed. Under the second category, a fine of up to EUR 20,000,000 or 4% of the worldwide annual turnover of the company in the preceding financial year may be imposed.[150]

Some instances where heavy fines have been imposed on companies for data breaches are discussed below. We also discuss instances where fines would have been higher, had the breach taken place under a newly enacted legal GDPR framework.

1. *Facebook fined by UK:* The United Kingdom Information Commissioner's Office imposed a penalty of GBP 500,000 on Facebook in October 2018 for a serious data breach (~ Rs. 4.6 crore as on January 22, 2019).[151] This fine was imposed as a consequence of Facebook's role in the Cambridge Analytica scandal. As part of the scandal, information of close to 87

[149] The Information Technology Act, 2000, https://indiacode.nic.in/bitstream/123456789/1999/3/A2000-21.pdf;

[150] The European Union General Data Protection Regulation, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=en;

[151] UK watchdog fines Facebook 500,000 pounds for data breach scandal, The Economic Times (25/10/2018), https://economictimes.indiatimes.com/news/international/world-news/uk-watchdog-fines-facebook-500000-pounds-for-data-breach-scandal/articleshow/66363788.cms;

million users was shared with the political consultancy firm. The fine imposed on Facebook would have been much higher under the EU GDPR which had not been enacted at that time.[152]

2. *Hilton fined for data breach:* The New York Attorney General imposed a fine of USD 700,000 on Hilton Hotels for two incidents that took place in 2015.[153] These incidents involved the hacking of the company's information system, resulting in the leak of credit card and other information of 3,50,000 customers. Despite finding out about the first breach in December 2014, and the second breach in July 2015, the hotel chain informed its customers only in November 2015. Many security experts commented that the fines were grossly inadequate and constituted only 0.00006% of the hotel's annual revenue, and may therefore be an insufficient push to make the company comply with the law. Under the new European Union GDPR, the fine on a company like *Hilton* would be to the tune of USD 420 million.
3. *Uber fined for data breach:* In 2016, ride-hailing app Uber was fined USD 148 million when data pertaining to 600,000 drivers and 57 million user accounts was hacked.[154]
4. *AT&T fined for data breach:* The AT&T breach exposed data of approximately 280,000 customers in the US. The breach occurred when employees at AT&T's call centres in Mexico, Colombia, and Philippines accessed sensitive customer data without authorization. Some employees sold this data to third parties to unlock stolen cell phones. Eventually, AT&T agreed to pay USD 25 million to the Federal Communications Commission to settle the investigation.[155]

Therefore, a possible solution for India may be found in the approach adopted under the GDPR, which mandates the levy of heavy pecuniary damages in case of a data breach, thereby ensuring self-compliance by companies.

B) Repository of Data Breaches

In order to protect the interests of consumers, it may be important to ensure that they have complete information about the level of data security employed by a particular service provider, before they choose to use a product or give consent for data processing. One way to facilitate this will be making previous instances of data breaches readily available. This could be done by creating repositories where information related to data breaches is stored, and is available for consumers to search. Such repositories may be sourced from breach notices issued by a service provider, or through other mediums after breaches have been reported and confirmed.

Currently, similar repositories are being operated by private companies, such as the 'Privacy Rights Clearinghouse', in the United States.[156] In addition to increasing awareness among users, this may also encourage service providers to strengthen their data security architecture to minimize breaches and keep their credibility and business intact.

India too, could consider creating such repositories - either a single repository that consolidates all breach information in one place, or different repositories controlled by sectoral regulators. The exact mechanics of implementation may be worked out in consultation with the industry and civil society.

---

[152] The biggest ICO fines for data protection breaches, Computer World UK (27/11/2018), https://www.computerworlduk.com/galleries/data/biggest-fines-issued-by-ico-3679087/;

[153] Hilton Was Fined $700K for a Data Breach. Under GDPR It Would Be $420M, Digital Guardian (06/04/2018), https://digitalguardian.com/blog/hilton-was-fined-700k-data-breach-under-gdpr-it-would-be-420m;

[154] Biggest data breach penalties for 2018, CSO Online (30/10/2018, https://www.csoonline.com/article/3316569/data-breach/biggest-data-breach-penalties-for-2018.html;

[155] AT&T data breaches revealed: 280K US customers exposed, CNBC (08/04/2015), https://www.cnbc.com/2015/04/08/att-data-breaches-revealed-280k-us-customers-exposed.html;

[156] Data Breaches, Privacy Rights Clearinghouse, https://www.privacyrights.org/data-breaches;

II. Instituting Preventive Measures: Voluntary Data Protection Seals

Since penalties are applied after a breach or violation has already happened, it has been recommended that the government also institute preventive measures to boost data security. Regular data security audits to assess the strength of technology deployed by service providers has been one proposal under consideration.

While this proposal is otherwise well intentioned, it is likely to face issues in implementation: technology related to data protection, encryption, and hacking is evolving at a fast pace. A particular methodology to safeguard data may be appropriate at the time of the audit, but may become outdated or obsolete in light of new developments in the space within a matter of few months. In such a scenario, a data security seal granted at the time of audit may no longer accurately reflect the security level of the data, and may therefore prove misleading. Experts have also argued whether a single security score can capture all nuances of a security program.[157] **Therefore, a data security seal may at most only provide a baseline, and not an advanced comparison on the security status of a software/ service provider.**

As discussed in the case study on EU data protection seals, the GDPR also encourages member states to establish data protection certification mechanisms.[158] These certification mechanisms seek to ensure that companies processing data comply with minimum standards of data security. Article 42(3) of the GDPR specifies that these data protection audits should be voluntary, and available through a transparent process. The audits are aimed at ensuring compliance with the GDPR and adoption of minimum data protection standards. They do not prescribe a score to the audited company as envisaged under the Draft Personal Data Protection Bill in India, thereby refraining from bringing in gradation in terms of data security and avoiding risks associated with auditing technology that is rapidly evolving.[159]

Similar to the approach adopted by the GDPR, the policy framework for regulating encryption in India should encourage the creation of an ecosystem where voluntary[160] data protection certifications are sought after by service providers. This approach will help increase compliance in general and also bridge information asymmetry between service providers and consumers, while also increasing their familiarity with data protection principles.

III. Enabling Legislation to Support Ethical Hacking

The 2017 joint communication on "Resilience, Deterrence and Defense: Building strong cyber security for the EU" recognized the need to acknowledge and enable the important role of 3rd party security researchers in discovering vulnerabilities in existing products and services.[161] **Despite foreign acknowledgements like this seeking to cement the role that ethical hackers and security researchers' play, India has come nowhere close to creating an environment conducive to ensuring ethical hackers feel confident revealing flaws in security systems.**

Thus, ethical hackers who are security researchers by persuasion, will, in the absence of a clear set of rules to resort to, be in a dilemma on how to proceed when confronted with a security flaw. Some of the most pertinent ones are:

---

[157] Collet, Stacy, What's in a security score? CSO, 04/08/2016, https://www.csoonline.com/article/3103293/security/what-s-in-a-security-score.html;

[158] Article 42, European Union General Data Protection Regulation, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=en;

[159] The Draft Personal Data Protection Bill, https://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf;

[160] Note: The two policy measures - imposing fines for data breaches, and mandatory data protection audits - may not be compatible. Let's say Company A has been audited by an auditor empaneled by the regulator, and has been given a data security score of ten out of ten. This score has been generated by comprehensively taking into account various aspects related to data security (such as the strength of encryption used, plugging vulnerabilities when data is switching states, and use of state-of-the art data protection methods). Let's say a month after the audit, there is a major data breach where personal information of users is compromised. In this scenario, the company would be subjected to the levy of a fine under the policy. This may lead to a conflict since the company had been certified as fully compliant with the required data protection standards by an auditor empaneled by the regulator. Further, it had also been given the highest possible data security score, indicating that the data protection system was believed by the auditor to be impenetrable. In this scenario, it may be inappropriate for the regulator to impose a penalty on the company for data breach.

[161] European Commission, Joint Communication from the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy on "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU" (13/09/2017) p.6.13, https://www.ceps.eu/events/software-vulnerabilities-disclosure-european-landscape;

a) Do you suspect a security flaw in systems that are of public interest? Are you morally obligated to pursue it if you are aware that not doing so, could lead to a breach of public interest? If so, how much access is too much access, when it comes to proving such security flaws?
b) Can you in good faith, inform the vendor/ owner of the operating system, of the flaw you have discovered, and expect to be legally protected from your unauthorized but non-malicious entry?
c) Where such security systems carry information vital to national security, are you obligated to/ is it appropriate to go to the press if the said vendor/ owner is not acknowledging or otherwise handling the flaw themselves?
d) Would publicly revealing the flaw cause more or less damage than not outing it at all?

Though there is a vast swathe of global opinion on what action is most appropriate for ethical hackers facing such a dilemma, much of it seems to be handled on a case by case basis, rather than with a clear set of rules. However, having to resort to litigation or judicial interventions can prove to be inconvenient and time-consuming, so some measures need to be instituted in the meanwhile. The international best practices detailed below can be such measures:

Vulnerability Disclosure Policies

Vulnerability Disclosure Policies (VDPs) are policies that carry in them safe harbor (or good faith) provisions and ensure responsible disclosure norms.[162] Ideally, a good VDP defines how organizations handle incoming alerts (legally and technically), the process by which vulnerabilities can be reported, and how the same may be externally disclosed by the organization.[163] Together, these provide security researchers the channels by which to safely declare vulnerabilities, while providing them a certain level of immunity to do so. Many organizations often reveal their VDP frameworks online, and so do governments, such as in the US where numerous departments like the United States Department of Defense and the United States Justice Department have VDPs available on their websites.[164] Likewise, government departments and organizations in India can be required to carry similar VDPs to guide ethical hackers/ security researchers with the way and manner of broaching a security flaw they may have discovered.

Changing penal codes to decriminalize ethical hacking

While VDPs incentivize security researchers and ethical hackers, it is equally important to ensure that criminal laws are allied to this. The Dutch courts provide an example of how laws may be reconciled. In the absence of a substantive change in criminal laws, the Dutch courts sought to ascribe the principles of motive, subsidiarity and proportionality in cases of ethical hacking.[165] They first sought to establish criminal intent (was there malice?), secondly, they sought to access the actions of ethical hackers immediately after the hack (such as, did they inform relevant authorities?), and finally, they considered the aspect of proportionality (did the ethical hacker go beyond merely finding a vulnerability, to exploiting the weakness?). While a good test for looking up criminal intent and liabilities may vary across jurisdictions, a 3-pronged test like this serves as a good starting point to think about a framework for addressing the issue, should issues of ethical hacking ever be touched upon by Indian courts.

[162] Vulnerability Disclosure Policy Basics: 5 Critical Components, HackerOne Blog (10/08/2017), https://www.hackerone.com/blog/Vulnerability-Disclosure-Policy-Basics-5-Critical-Components;

[163] Ibid.

[164] Vulnerability Disclosure Policy Basics: 5 Critical Components, HackerOne Blog (10/08/2017), https://www.hackerone.com/blog/Vulnerability-Disclosure-Policy-Basics-5-Critical-Components;

[165] Falot, Nathalie, Criminal Liability for Ethical Hackers in the EU, Considerati Algemeen, https://cert.lv/uploads/pasakumi/Nathalie_Falot.pdf;

IV. Requiring Cooperation from Service Providers in Emergent Cases

Advancements in encryption technology carry significant benefits in terms of securing customers' sensitive data, which consequently translates into increased use of digital platforms and communications. However, there is no denying that encryption technology also gives rise to a number of challenges for law enforcement, making it inordinately difficult to derive intelligence. The term 'surveillance intermediaries', coined by Cyber Law expert Professor Alan Rozenshtein, refers to companies that are situated between law enforcement agencies and customers' personal information, and that are obligated to protect consumer privacy but must also help the law enforcement agencies when presented by a warrant or a lawful request in emergent cases pertaining to national security, law and order, or otherwise (as mandated by law).

As per our analysis, there are essentially two primary categories of surveillance intermediaries:

1) The first category consists of service providers that utilize an encryption technology that can easily be overridden to decode encrypted text upon a request from the government; and
2) The second category consists of service providers that express inability to assist the government - either due to lack of trust in the surveillance system, or due to their individual stance (on consumer privacy) and reputational incentives, or due to their use of end-to-end encryption or other such technologies that they suggest cannot be intercepted and decrypted,[166] thereby potentially creating hindrances for law enforcement.

In India, interception requests made to service providers under the Indian jurisdiction are governed either by the Telegraph Act (Section 5(2) or Rule 419(a), the IT Act (Section 69), or the CrPC (Section 91). All service providers registered in India are bound by these laws to supply decrypted information when approached with a request through due process, and the failure to do so may result in punitive measures, including fines and imprisonment.

Government's access to private data, if uninhibited (through backdoors or otherwise) is undoubtedly detrimental to individual rights and freedoms, but it is not so if the power to intercept is exercised sparingly, on a case by case basis, with restraint and by following a due process. The provisions of the Telegraph Act and the Information Technology Act mentioned above are simply parallels of the very important mechanisms available to law enforcement agencies in the physical space (where they are allowed to use force to enter a person's property without consent in specific cases). Without these, any law enforcement agency is likely to be severely crippled.

Given this, it is important for service providers and the government to work together to develop mechanisms and modify technology, as required, to allow for lawful interception requests to be serviced. On their part, policymakers can work to strengthen the checks and balances in the system to build greater trust from the point of view of improving compliance.

Increasing post-facto accountability in government interception by codifying practices

As outlined in a previous section, the current procedure for intercepting telecommunication is outlined in the Indian Telegraph Act, 1885, and for digital communication in the Information Technology Act, 2000.[167,168] These laws allow for communication to be intercepted on a set of pre-identified grounds, and call for the creation of a Review Committee (both at

[166] Note: In stakeholder conversations, several experts have contested the claim that service providers cannot tweak the technology to assist law enforcement in specific cases
[167] The Indian Telegraph Act, 1885, http://dot.gov.in/sites/default/files/Indian%20Telegraph%20Act%201885.pdf?download=1;
[168] The Information Technology Act, 2000, https://www.meity.gov.in/writereaddata/files/The%20Information%20Technology%20Act%2C%202000%283%29.pdf;

the central and state level) that must analyze, post-facto, every interception order for legitimacy on the basis of the following three criteria:[169]

1. Whether the purpose of interception can reasonably be placed under one or more grounds of lawful interception mentioned in the Telegraph Act or the Information Technology Act?
2. Whether the protocol for interception was followed by the law enforcement agencies? and
3. The outcome of the interception activity.

While the Telegraph Act and the Information Technology Act both necessitate the creation of the Review Committee, and endow it with powers to block illegitimate interception (while also asking it to escalate cases of unlawful interception to the Indian judiciary), the Committee is entirely executive in nature and lacks judicial oversight. Thus, some civil liberty organizations[170] have, understandably, made a case for judicial participation in the Review Committee to ensure better checks and balances. However, there are many within the government who disagree with this view.[171] They draw attention to the checks and balances ***within*** the executive[172] and highlight practical considerations with respect to judicial involvement, namely how overburdened the Indian judiciary already is and how placing a judicial member in the Review Committee is unlikely to be effective unless at least half of the committee is judiciary-based.

That said, there is certainly **merit in exploring judicial involvement in the Review Committee** if it helps build trust in the government's accountability mechanisms and improves private cooperation in legitimate surveillance efforts. There is also a case to be made for **enhancing and codifying the practices and principles of the Review Committee so as to prevent arbitrariness in vetting-procedures.**

Our stakeholder interactions have revealed that in each meeting, the Review Committee evaluates thousands of cases on the basis of the three broad criteria mentioned above, and then picks a random sample of a few hundred cases for a deep-dive. These practices, while followed by the Review Committee, are not codified by law and are hence not binding. A legal codification will enable the government to strike a better balance between India's national security interests, and the Indian citizen's right to privacy.

V. Building Checks and Balances in the Use of Hacking by Law Enforcement

Although hacking looks far better in principle as a concept as opposed to other measures like lowering encryption standards or building in backdoors in technology, the government must resort to it as a tool for use only in extraordinary circumstances. This requires that the government develop a strong framework to regulate it.

For one, hacking by the government must not be allowed to exist in a legal vacuum. It must include built-in checks and balances such as judicial authorizations/ court mandated processes, especially given its invasiveness when compared to traditional coercive activities such as house searches. Wherever possible, the government must consider lawful hacking with compelled provider assistance, and have processes in place to enable the same, and should resort to lawful hacking without assistance (i.e. circumventing the system) as last resort.[173] And where, during the process of monitoring and interception, the Indian government comes across vulnerabilities in any system, they should have policies that mandate

[169] Information received from a member of the Law Enforcement in India who requested to be kept anonymous;

[170] Surveillance – Is there a Need for Judicial Oversight, Software Freedom Law Center, https://sflc.in/surveillance-there-need-judicial-oversight;

[171] From stakeholder conversations with law enforcement officials; names withheld on request;

[172] Conversations with law enforcement officials suggest that a typical request for interception is initiated by an 'Investigating Officer' at the junior level and goes through multiple levels, eventually culminating in an authorization by the Union or State Home Secretary;

[173] Encryption Policy in Democratic Regimes: Finding Convergent Paths and Balanced Solutions Report, The EastWest Institute (2018), https://iapp.org/media/pdf/resource_center/ewi-encryption.pdf;

disclosure to service providers, such as how the US and Canada have in place.[174]. Additionally, Indian laws must require government agencies to work alongside private and public companies/ networks, primarily those in technology and security spaces, to patch vulnerabilities within a specific period of time, to prevent them from being exploited.

Lastly, but not the least, an oversight mechanism (potentially the same review process available under the Telegraph and Information Technology Act) must require for *ex-post facto* examination of the interception process, so as to ensure adequate checks and balances. To facilitate this, it would be beneficial to have processes in place that require law enforcement agencies to create logging trails, institute regular audits, and submit timely status reports to see if the surveillance that was undertaken followed all the necessary legal procedures.[175]

[174] Waterman, Shaun, Responsible vulnerability disclosures is becoming an international norm, CyberScoop (22/09/2017), https://www.cyberscoop.com/vep-international-responsible-disclosure-canada-uk-netherlands/;

[175] Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices, Study for the Libe Committee by the European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs (2017), http://www.europarl.europa.eu/RegData/etudes/STUD/2017/583137/IPOL_STU(2017)583137_EN.pdf;

Appendix I

How Encryption Works

Encryption refers to the process of converting plain text into unintelligible text, to ensure that it cannot be read by unauthorized persons. It is used by militaries for safe transmission of classified communication, and civilian establishments for communicating private information, storing personal health data, or securing financial data. The process is explained below:

- Plain text is the message that needs to be encrypted. For example, the plain text is 'It is a sunny day'.
- Cipher text is the key which is used to encode the message. For instance, in the table below, the first row indicates the plain text, and the second row indicates the key to encrypt this text. In this key, each alphabet has been shifted three times to the right.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c

- Encryption involves the conversion of plain text into cipher text. Using the above example, the message 'It is a sunny day' can be encrypted to 'Lw lv d vxqqb gdb'.
- Decryption involves converting encrypted text back into plain text so that it can be read by the receiver.

While the above example seeks to demonstrate how encryption works, in modern times more sophisticated encryption algorithms are used, enabling the creation of stronger encryption codes. With the availability of computers, messages are encrypted using bits (i.e., either 0 or 1 in the binary system). Various key sizes may be used to encrypt data, depending on their strength. For instance, a 40-bit encryption refers to a key size of 40 bits, implying that a total of 2^{40} possible keys exist.[176] Any unauthorized person may have to try all of these possible combinations to decrypt an encoded message. A higher bit encryption rate indicates higher security of the message.

Types of Encryption and its Dynamically Evolving Nature

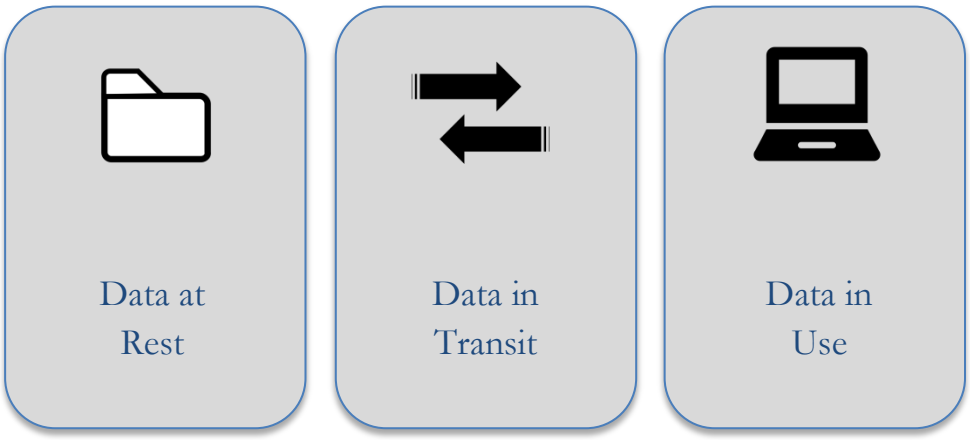
Cryptographers primarily use two different methods of encrypting data, known as symmetric encryption and asymmetric encryption. But several new methods have also emerged. Increasingly combinations of symmetric and asymmetric methods are being used. 'Quantum Key Distribution' is yet another innovation. In a dynamic environment, the number of cryptography methods may further diversify making the future uncertain. This may pose a challenge for policymakers who must be prepared to adapt to an ever-changing form of technology.

Encryption and the Three States of Digital Data

Literature on data protection and information security usually categorizes digital data into the following three kinds - data at rest, data in transit and data in use - collectively known as the 'three states of data'.

[176] The number of possible keys for any encryption is 2^n where 'n' refers to the size of the encryption (i.e. no. of bits);

The Three States of Data



The vulnerabilities associated with data vary with each of its states, and hence, the security protocols for each state of data must be different from the other two.

A. Data at Rest

Any information that is not being accessed, and that is stored in physical or logical media, is known as data at rest. Files stored on servers, records on databases and documents on flash drives are some examples of how data is stored at rest.[177] Encryption of data in this state is one of the most potent mechanisms of securing information, such that decrypting it may require excessive use of brute force.

B. Data in Transit[178]

Data in transit, as the term implies, is data on the move from one point to another. Even with encryption, securing data while in transit is more complicated than securing it at rest, since it is a moving target. Such data, which is accessible over a particular network, could be intercepted by anyone else on the network who is technologically capable, or who has access to the physical media the network uses. If accidentally misdirected by a careless employee or purposefully attacked by a particularly adept hacker, in-motion data can potentially travel beyond the firewall into an uncontrolled environment. Another challenge with data in motion is understanding all the different parties that have access to it while it is in transit.[179]

C. Data in Use

Data in Use refers to 'active data' assets under constant change as they are processed by applications. They are usually held in non-persistent storage such as computer memory and CPU caches. Of the three states that data can exist in, in-use data is more vulnerable than its counterparts simply by definition – it must be accessible to those who need it, yet it must stay protected from malicious penetration. This becomes particularly difficult when the number of people and devices that need access to the data increases, eventually translating into a greater risk that it can fall into the wrong hands. The key therefore is controlling access to the data as tightly as possible.[180]

[177] Encryption of Data at Rest, Protecting the Three States of Data, http://sealpath.com/protecting-the-three-states-of-data/;
[178] Manes, Casper, Protecting Data with Encryption while in Transit, Tech Talk, https://techtalk.gfi.com/protecting-data-with-encryption/;
[179] O'Dwyer, Michael, Why Data in Motion is at its most vulnerable, Ipswitch, https://blog.ipswitch.com/data-in-motion-vulnerable;
[180] Encryption In-Use: Challenges and Realities: https://vaultive.com/data-in-use-encryption/;

For securing data in transit and data in use, encryption, authentication and authorization go hand-in-hand - in fact, the former is commonly used as an added layer of security for data that is sensitive enough to warrant the use of the latter two (such as confidential data that is not publicly accessible and requires authentication).

Appendix II

Consumer Privacy and Data Protection: Global Frameworks for the Use of Encryption

Countries such as the US, and members of the European Union have data protection regimes based on a 'sectoral model', meaning that personal information is protected by various laws or guidelines applicable to particular industries or sectors (primarily financial services, healthcare and the communications industry).

In the US, for instance, financial data is governed by the "The Gramm-Leach-Bliley Act" (1999),[181] which requires financial institutions to employ appropriate technical and physical safeguards to protect customers' personal information against anticipated threats. While there is no explicit clause in the Act that mandates encryption in the financial services sector, the Federal Financial Institutions Examination Council Handbook[182] highlights the need for financial institutions to employ encryption to mitigate the risk of disclosure or alteration of sensitive information in storage and transit. With regard to healthcare data, the US "Health Insurance Portability and Accountability Act" (HIPAA)[183] of 1996 makes specific references to encryption to protect medical information, although encryption standards are not prescribed. In addition to sector-specific legislation (as mentioned above), data protection laws in the US are also state-specific, with a number of states enacting their own legislation that mandate the use of encryption. One example of this is the comprehensive data protection and privacy law passed by the Commonwealth of Massachusetts in 2010, which expressly requires encryption of electronically communicated personal data.[184]

Like the US, Germany follows a sectoral model as well, wherein a host of laws are applicable to 'critical' sectors, including health and finance. These sectors have their own legislation which mandate data security measures to be taken by organizations.[185]

On the other hand, some countries have an overarching data protection law that subsumes encryption (across sectors), such as Japan's "Act on the Protection of Personal Information" (APPI). Article 20 of the APPI specifies that personal information (including communications) must be securely protected,[186] stored, and transmitted, and the APPI envisages sectoral regulators to enforce the common law for their respective sectors. Japan's Financial Services Agency (JFSA), for instance, has issued guidelines regarding the APPI in the financial field. While encryption is not expressly mandated,[187,188] it is presumed to be the recommended tool for information security.

---

[181] GLBA Requirements for Data Encryption, Stratozen, https://stratozen.com/glba-requirements-for-data-encryption/;

[182] FFIEC IT Examination Handbook, https://ithandbook.ffiec.gov/media/274793/ffiec_itbooklet_informationsecurity.pdf;

[183] Scholl, Matthew& Stine, Kevin & Hash, Joan & Bowen, Pauline & Johnson, Arnold & Smith, Carla Dancy & and Steinberg, Daniel I., An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/nist80066.pdf;

[184] Standards for the Protection of Personal Information of Residents of the Commonwealth, Section 17.04; https://www.mgiworld.com/media/2078756/mass-law-cmr17.docx;

[185] Germany Cybersecurity: 2019, ICLG; https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/germany;

[186] Japan's Amended Act on the Protection of Personal Information, https://www.ppc.go.jp/files/pdf/Act_on_the_Protection_of_Personal_Information.pdf;

[187] The Legal Obligations for Encryption of Personal Data: Japan, Vormetric Data Security, http://enterprise-encryption.vormetric.com/rs/vormetric/images/2014-The-legal-obligations-for-encryption-of-personal-data-in-Europe-Asia-and-Australia.pdf;

[188] Yamamoto, Ryuichi, Large-scale Health Information Database and Privacy Protection, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5333617/;

Similarly, in Australia, "The Privacy Act of 1988"[189] is the core legislation on information security across industries and sectors, with the "Privacy Amendment (Enhancing Privacy Protection) Act"[190] of 2012 introducing principles to strengthen overall data protection. In addition to this, the Office of the Australian Information Commissioner[191] places heavy emphasis on encryption of personal information in its regulatory guidance published in April 2012 - The "Data breach notification: A guide to handling personal information security breaches". Organizations in Australia are also required to notify the Office of the Australian Information Commissioner as well as the individual(s) affected in the event of a serious data breach.[192]

In the UK, the "Data Protection Act" of 1998 mandates that the entity collecting and storing the data has an obligation to keep the data secure and prevent unauthorized access.[193] The Information Commissioner's office (ICO) - UK's independent data protection regulator as per the Data Protection Act - has taken a stance that regulatory action may be pursued if personal data is compromised due to encryption software. The ICO recommends that data controllers[194] should have policy regarding encryption that includes guidelines for the staff.[195] In the financial sector, the Financial Services Authority (FSA) states that data controllers are responsible for securing the customer data and protecting it from fraudsters, and frowns upon the use of unencrypted devices, such as portable devices, to store customer data.[196] They also advise data controllers to test their data protection and backup procedures. If the data is being held by third party off-site, it should be encrypted.

In Switzerland, the Federal Act on Data Protection requires that personal data must be protected through adequate technical and organizational measures.[197] The Swiss Financial Market Supervisory Authority (FINMA) requires banks and securities dealers to encrypt data when it is being transmitted through an open network, such as the internet.[198] It requires banks to ensure confidentiality of client information by using technical measures such as anonymisation, encryption, or pseudonymization.[199] Depending on the level of confidentiality and threat, the bank may choose the most appropriate method to secure data.

The General Data Protection Regulation (GDPR) adopted by the European Union is binding on all member states.[200] While outlining the basic rules, it allows member states to introduce more specific provisions and adapt the application of the GDPR. Article 32 of the GDPR[201] mandates the use of appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: the pseudonymisation and encryption of personal data.[202] In order to ensure compliance, the GDPR requires member states to establish data protection certification mechanisms (private parties empaneled by the government) under their jurisdiction.

---

[189] Privacy Act 1988, Australia, https://www.legislation.gov.au/Details/C2014C00076;

[190] Privacy Amendment (Enhancing Privacy Protection) Act 2012, https://www.legislation.gov.au/Details/C2012A00197/41a1f43a-a31b-41cb-80b5-d698b8e70f18;

[191] Data Breach Notification Guide Office of the Australian Information Commissioner, April 2012, https://www.oaic.gov.au/images/documents/privacy/privacy-resources/privacy-guides/Data_breach_notification_guide_April2012FINAL.pdf;

[192] Notifiable Data Breaches scheme, Office of the Australian Information Commissioner, https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme;

[193] Obligations of Data Controllers under the UK DPA: https://www.bbc.com/bitesize/guides/z6kj6sg/revision/5

[194] Note: The GDPR defines "Data Controller" as "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data", https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/controllers-and-processors/what-are-controllers-and-processors/#2;

[195] Guidance on Encryption, Information Commissioner's Office, UK, https://ico.org.uk/media/for-organisations/encryption-1-0.pdf;

[196] Data Security in Financial Services, FSA Report, https://www.fca.org.uk/publication/archive/fsa-data-security.pdf;

[197] The Switzerland Federal Act on Data Protection (FINMA), https://www.admin.ch/opc/en/classified-compilation/19920153/index.html;

[198] Frequently Asked Questions, FINMA website, https://www.finma.ch/FinmaArchiv/ebk/e/faq/faq4.html#4J;

[199] Operational Risks - Banks, Circular 2008/21, Swiss Financial Market Supervisory Authority, KPMG (Translation issued in 2016), https://assets.kpmg.com/content/dam/kpmg/ch/pdf/ch-finma-circular-2008-21-en.pdf;

[200] The European Union General Data Protection Regulation, Official Journal of the European Union, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=en;

[201] Article 32 of EU GDPR, "Security of Processing", http://www.privacy-regulation.eu/en/article-32-security-of-processing-GDPR.htm;

[202] Article 32 of EU GDPR, "Security of Processing", http://www.privacy-regulation.eu/en/dossier_encryption_demo.htm;