TRAVEL GUIDE TO THE DIGITAL WORLD:

ENCRYPTION POLICY FOR HUMAN RIGHTS DEFENDERS

“It is neither fanciful nor an exaggeration to say that, without encryption tools, lives may be endangered.”

Zeid Ra’ad Al Hussein,
United Nations High Commissioner for Human Rights

GLOBAL PARTNERS DIGITAL

Published in London 2017
by Global Partners Digital

Rarely a week goes by without encryption making the headlines. More often than not, it's presented as a dangerous, even scary technology – a friend of terrorists, criminals and malicious hackers.

But encryption has been with us since Ancient Greece, and in the digital age we all use it every day, often without even being aware of it. Whenever we shop or bank online, or chat using instant messaging, we are using encryption. It is encryption that keeps our data secure, protects us from fraud, and allows us to communicate privately.

It has also become crucial to the exercise of many of our human rights, particularly privacy and freedom of expression. For some people around the world who face discrimination, violence or persecution, encryption can even mean the difference between life and death.

Because of the secure, private space that encryption offers people, many governments have made attempts to limit it – from outright bans, to import and export controls, to giving law enforcement agencies access to encrypted information. In recent years, as the digital environment has become more strategically important for states, these efforts have intensified.

Across the world, from the United Kingdom to Colombia, Nigeria to Pakistan, efforts are being made to push through measures which weaken and compromise people's ability to use encryption.

For the sake of our rights and our security, it's crucial that we don't let this happen.

AN OVERVIEW OF THIS GUIDE

On a range of issues, human rights defenders play a critical role in ensuring that laws, policies, regulations and standards – whether set at the global, regional or national level – are consistent with human rights. Where human rights defenders are absent from policymaking, there is a risk that important policy decisions will be made on the basis of political expediency, rather than the promotion and protection of human rights. The capacity of human rights defenders to input into and scrutinise laws, policies, regulations and standards depends on their having a sufficient level of knowledge of the subject, the issues, and the relevant stakeholders and institutions.

The aim of this guide, therefore, is to equip human rights defenders with the information they need to be able to engage with, advocate to and inform policymakers on **encryption**.

CHAPTER 1 covers what encryption is, setting out a brief history of encryption technology, what it looks like today, and why people use it. CHAPTER 2 turns to the debates surrounding encryption, the relevant stakeholders and their interests, before examining some of the most common attempts being made to limit or regulate encryption. CHAPTER 3 looks at the links between encryption and human rights, particularly the rights to privacy and freedom of expression, making clear that encryption *is* a human rights issue. With that in mind, CHAPTER 4 sets out what human rights-respecting laws and policies on encryption would look like. CHAPTER 5 introduces and examines the various forums - at the international, regional and national levels - where encryption laws, policies, regulations and standards are set. Finally, CHAPTER 6 looks at some of the messages human rights defenders can use at those forums to advocate for human rights-respecting policies.

This guide is aimed at a non-technical audience, so there is a Glossary at the end. Terms explained in the Glossary are in **bold** print the first time they appear in each chapter.

CONTENTS

CHAPTER 1

WHAT IS ENCRYPTION?

What is encryption?

Defined simply, **encryption** is the ability to encode communications (or information or data) so that only the intended recipient can read or understand them.

Most of us use encryption every day without even realising it: whether that's storing information on our computers or smartphones with a PIN or password, visiting secure websites (such as those whose addresses start with 'https'), or using instant messaging apps like WhatsApp.

While the need to protect our communications and information from unauthorised interference has existed for thousands of years, methods of encryption have changed dramatically, particularly since the development of computers and other forms of modern technology. And while once used almost exclusively by a small number of individuals, encryption is now used by a vast array of different groups for different purposes. In this first chapter, we take a brief look at the history of encryption, what modern-day encryption looks like, and why people use it.

Encryption, decryption and cryptography: what's the difference?

Throughout this guide, we'll be using the terms encryption, **decryption** and **cryptography**. Encryption refers to the means of encoding communications (or information or data) so that they cannot be read by anyone other than the intended recipient. Decryption is the means by which encrypted communications are decoded so that they can be read and understood. The term cryptography covers both encryption and decryption, and refers more broadly to the study and practice of techniques for secure communication.

A BRIEF HISTORY OF ENCRYPTION TECHNOLOGY

The earliest recorded use of cryptographic devices comes from Ancient Greece, where military and political leaders needed a way of stopping the messages they were sending across the vast empire from being read by their enemies. Their solution was to encode their messages using various forms of cryptographic devices. The earliest known device was a scytale, a cylinder of wood of a specified diameter. Messages would be written through a series of letters along a leather strip which, when bound around the scytale, would reveal the message. The leather strip, unbound, would only show the letters out of the correct order, thus encrypting the message.

Between this period and the end of the Second World War, cryptography was almost entirely undertaken through what are called classical **ciphers**. A cipher is simply an algorithm, process or method for encryption or decryption. Classical ciphers use two basic techniques to encrypt messages: character substitution and character transposition. They can also use a combination of the two.

The first – character substitution – replaces each letter or character with another, with the mapping of these substitutions being the secret used to encrypt and decrypt the messages. An example is the Caesar cipher, sometimes called the shift cipher, whereby every letter in the original message is replaced with a letter corresponding to a certain number of letters up or down in the alphabet. For example. with a shift of three letters forward, A would be replaced with D, B with E, and so on. The second method – character transposition – does not change the letters or characters in the message, but rearranges them according to a particular method. In this method, the change in the order of the letters is the secret.

The use of classical ciphers peaked during the Second World War with mechanical devices like the famous German Enigma machine which used rotors, rotating disks with electrical contacts on either side. Each rotor contained a random substitution alphabet, and between three and five rotors could be used at any time. The user would press a letter on the machine, the letter would be substituted multiple times via the rotors, and an encrypted letter then lit up on a display. By using multiple alphabets and a different method of substitution for each character, these machines allowed for complex but rapid encryption and decryption of messages.

ENCRYPTION TECHNOLOGY TODAY

Technological developments since the Second World War, particularly the advent and mass use of computers, have brought about a sea change in encryption methods. Modern encryption involves applying a mathematical algorithm to data, scrambling it and making it unreadable. As part of the algorithm used, additional data – called a key – is incorporated, without which the encrypted data cannot be decrypted, even if the algorithm itself is known.

The strength of the encryption depends on two things: the particular algorithm which is used, and the **key length** (the number of binary bits strung together in the key). The longer the key length, the greater the number of possible combinations of ones and zeros of its composition (the **key space**), and therefore the greater the amount of work which would be required to try all of the possible combinations.

Attempts to go through all the possible combinations are called **brute force attacks**. One of the measures of a cryptographic system's strength is how long it could withstand such an attack.

SYMMETRIC AND ASYMMETRIC ENCRYPTION

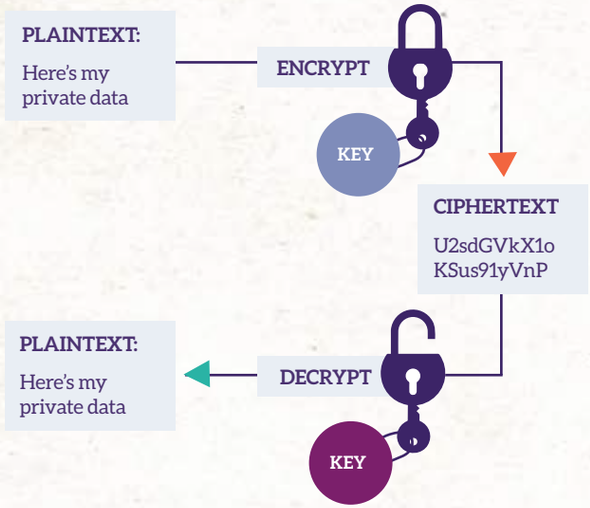
There are two main types of modern cryptographic systems: those using symmetric keys (**symmetric encryption**) and those using asymmetric keys (**asymmetric encryption**). In symmetric key systems, the same key is used to both encrypt and decrypt the communication. Asymmetric key systems, as their name suggests, use different keys to encrypt and decrypt the same communication.

The benefit of symmetric key systems is that they are quick and efficient. They are particularly useful where the same party is both encrypting and decrypting the data – for example, someone who wants to keep their files secure and private on their computer, and therefore does not need two different keys.

When more than one party is involved, however, symmetric key systems may not be the best option. They generally require every party to know the key, which means, at some point, one party will have to hand the key to another. Doing this through common communication routes – like email, or SMS – carries risks of interception. These systems also depend on all parties trusting each other to keep the key secure, which may not always be possible.

There are examples of symmetric key systems which evade these problems by not requiring parties to know the keys. For example, some communications service providers use symmetric key systems whereby the key is not known by the users, but is stored on the devices which they use to communicate. Although the keys are the same, they are not known by the communications service providers, being generated by the devices themselves, and unique to those devices, so they cannot be discovered.

Symmetric encryption



Plaintext and ciphertext

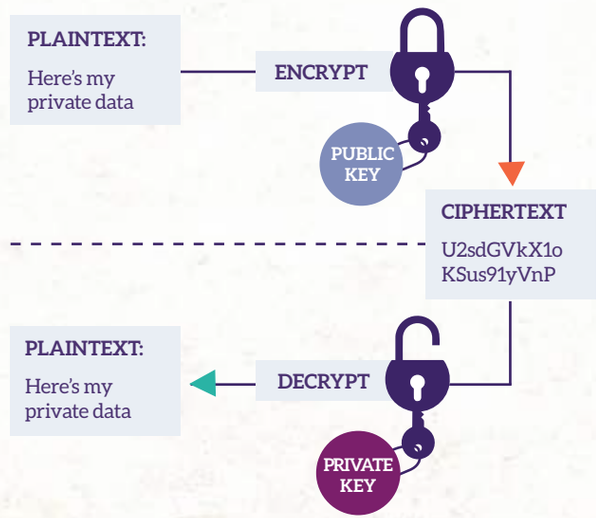
In modern day encryption, the terms plaintext and ciphertext are often used. Plaintext refers to the communication or data in its original, readable form. Ciphertext refers to the communication or data while it is encrypted and unreadable.

With asymmetric key systems, the two keys are linked. Usually a '**public key**' is used to encrypt the communication, and a '**private key**' alone will decrypt the communication (although sometimes it is the reverse, as we will see shortly). While the decryption process here is more intensive and time-consuming than with symmetric systems, the advantage is that the public key can be widely distributed by the owner, and even made publicly available, with no danger of the communication being decrypted, since the private key is known only to the person who possesses it.

This can be particularly useful to journalists or human right defenders, who might need to be contacted with confidential information or tip offs from strangers.

A further benefit to the use of public and private keys is that it allows the creation of a **digital signature**. In the offline world, seeing a person's signature on a document means that we can be sure that it was that particular person who signed it. With a digital signature, the person 'signing' the document uses their private key to encrypt it, and makes the public key publicly available. Because the public key and private key are linked, if the encrypted document can be decrypted using the public key, then this means that only the corresponding private key could have encrypted the document. And, because only one person has that private key, the person receiving the document can be sure that only they could have encrypted it. Digital signatures can be used by anyone who wants to be able to prove that it was they who authored a document or sent a particular communication, such as businesses sending documents to clients, or universities which send electronic transcripts to students.

Asymmetric encryption and public/private keys



THE STAGES OF DATA ENCRYPTION

There are three stages at which data can be encrypted.

Data at rest means, in simple terms, data that isn't currently being used – for example, files stored on a computer or a mobile device. Encrypting data in this stage is, to use an offline parallel, akin to locking a will in a safe. As with a safe, generally only one party will need the ability to lock and unlock it, so a symmetric key system would often be appropriate here.

This is not to suggest that data at rest can always be easily secured. Sometimes, data at rest may need to be read by a certain process – for example, while it is being scanned by certain pieces of anti-virus software. In such instances, unencrypted copies of the data will be created as temporary files on the device, creating a vulnerability in the cryptographic chain which could be exploited by an attacker.

Data in process (or data in use) refers to data which is being viewed, processed or manipulated – for example, a document or email which is being read or edited, or a message in the process of being written. In the offline world, this would be comparable to someone person removing their will from the safe to edit it. They've taken the document out of storage, but they still don't want anyone except them to be able to see or change it at this stage. As long as it is encrypted while in process, it will remain private and will not able to be edited (or even viewed) by anyone else. Again, only one person will generally need to access the document, so they can use the same key (i.e. the symmetric key system) to encrypt and decrypt it.

Finally, the encryption of **data in transit** refers to data while it is being communicated or sent over a data network (e.g. between mobile phones, or from a computer to a printer or data storage server). In the offline world, this would be comparable to the person sending their will by post to their lawyer. They don't want the will to be intercepted or edited by anyone else while it is in the post.

If the data is encrypted in transit, only they and the lawyer will be able to view the will. And if the person uses a digital signature when encrypting the document, the lawyer will be sure that it was that person who sent it.

In these circumstances, it's important to know at what point the data is encrypted and whether it remains encrypted over the entire period of transit. Is the data encrypted before it is sent, or afterwards? And is it decrypted at any particular points (for example, as it sits in the cloud waiting to be read) and then encrypted again before being sent further on in its journey?

There are only two contexts in which data in transit is truly encrypted from start to finish (known as **end-to-end encryption**). The first is where the data is encrypted at its journey's starting point, before being sent, and only decrypted after it has arrived at its journey's end point. The second is where an encrypted 'tunnel' is created, spanning from the device from which the data is sent, to the final device in which it is received, and that tunnel is not terminated at any point of the journey until the data reaches its final destination. Some applications which claim to provide end-to-end encryption actually temporarily un-encrypt and then re-encrypt the data at certain stages along its journey. Where the data passes through a number of stages, and each stage involves an encrypted 'tunnel', the data might nonetheless be un-encrypted momentarily and then re-encrypted when it is transmitted from one stage to the next, between tunnels.

WHY DO PEOPLE USE ENCRYPTION?

People use encryption every single day. In most cases, it is not done deliberately or consciously, with people simply using services that already incorporate encryption. Some actors, however, might derive particular benefits from deliberate use of encryption in their communications.

Keeping data and communications private and secure. This is perhaps the most common reason that people use encryption. Encryption allows us to shop, bank, send and receive communications without fear of interference or surveillance.

This can be particularly important for, among other groups, human rights defenders, whose communications and data can, in many countries, put themselves and others they work with at risk.

Receiving the data as it was intended. Encryption ensures data integrity; in other words, that the data received is exactly the same as that which was sent, without any addition, deletion or modification. Individual users benefit from this because, when they receive communications or data, they can be confident that they are receiving exactly what the sender wrote or sent. So, a human rights defender receiving information about a human rights violation can be sure that he is receiving exactly what his source intended, without any editing by a government official who has intercepted the communication.

Trusting the source of a message. Where digital signatures are used, this means that, just like when receiving a document in the offline world which has a signature, the user can be sure of who sent the message. So, for example, a journalist who needs to be able to trust her sources can be sure that the information she receives was sent by a particular source and not an imposter.

Holding people to their word. Non-repudiation means that a person who creates a message cannot later deny they wrote it. This is useful in some circumstances such as the signing of a contract between two parties, and is increasingly used by businesses as an alternative to physical signatures. If both parties digitally sign the contract with a digital signature then one cannot claim later on that they did not agree to its terms of the contract.

Encryption is not anonymity!

Encryption and anonymity are two separate concepts, although the differences are sometimes misunderstood. Anonymity – whether online or offline – refers to the ability to hide your identity. Encryption is the ability to keep private the communications, data or information that you wish to share. You can have one without the other, e.g. an anonymous hacker publishing information publicly but from an account that does not reveal her identity (anonymity but not encryption), or friends communicating using a communications app which uses end-to-end encryption (encryption but not anonymity). And you can, of course, do both at the same time, e.g. a whistleblower using encrypted communications services from an account that does not reveal their identity.

There are some methods of encryption which do automatically add anonymity to the communications – for example those systems which make up the 'dark web' or 'deep web', and software such as Tor which anonymises a person's communications and internet use. However, many do not, and may leak metadata, which can reveal who is communicating and with whom over the encrypted channel.

CHAPTER 2

WHAT IS THE DEBATE AROUND ENCRYPTION?

What is the debate around encryption?

Despite the importance, and ubiquity, of **encryption**, most people remain unaware of it. This is understandable – much of it takes place on our devices automatically, without any active user input – but it does mean that there is ground for misconceptions to arise.

There are, in theory at least, a number of different lenses through which the debate around encryption could be framed:

- **The technical lens.** Through this lens, encryption is seen chiefly as a technical – or even mathematical – issue. Computers are getting faster and therefore able to encrypt and decrypt data faster. This means that longer **key lengths** can be used, improving the security of the encryption. However, it also means that attempts to decrypt encrypted data through **brute force attacks** can be undertaken more quickly. And if users of encryption do not keep up with technical developments, but those who seek to hack into or intercept our communications and data do, such attacks will become easier. This raises questions over how to support the development of stronger encryption while mitigating such risks to users.
- **The economic lens.** Encryption can also be looked at through an economic lens. There are financial benefits to greater and better use of encryption as individuals' and businesses' data breaches can be reduced, and trade secrets lost through digital surveillance minimised.
- **The security lens**. As we will go on to look at it in more detail in this chapter, there is a debate which, at its simplest, is framed as privacy versus security. Security and law enforcement agencies want restrictions on the use of encryption so that it cannot be exploited by terrorists and criminals. Others oppose such restrictions on the basis that they would undermine the privacy and security of all users of encryption.

Because there is little media interest in the uncontroversial, everyday benefits of encryption (like making online transactions safe), when encryption does make the news, it tends to be in the context of terrorism or crime, often accompanied by commentary from government, security services or law enforcement stressing the need to place restrictions or controls on the use of encryption to keep people safe. As such, it this third, security-focused lens through which public debate on encryption has tended to be exclusively framed. This is a phenomenon known as securitisation.

In this chapter, we take a closer look at this debate: examining its key premises and parameters, the tensions and sides within it, the different stakeholders involved, and the issues and proposals at stake.

THE FAULT LINE

Few people in the encryption debate are actually calling for a total ban on encryption. Even the strongest advocates for restrictions on encryption for the purposes of law enforcement usually recognise that encryption is a crucial means of making digital information and communications secure. There are many stakeholders engaged in the debate on the use of encryption and they take an array of different roles and positions. While these positions are many and nuanced, they often diverge at a key fault line: the question of whether there should be restrictions, limitations or controls on the use of encryption.

Those who support restrictions or controls generally point to the potentially harmful uses of encryption (such as coordinating crime or terrorist attacks) and the difficulty and expense of case-by-case **decryption** (usually in the form of brute force attacks). Restrictions on encryption, they argue, would deny these malicious actors a safe space, and would let our law enforcement agencies do their job more easily.

Others contest this notion. They argue that weakened standards on encryption would not just be used by law enforcement, but would also be exploited by criminal hackers and others for the purposes of crime and terrorism, making everyone less safe and secure, and eliminating or reducing the many benefits provided by encryption.

PRIVACY VERSUS SECURITY?

The debate on encryption – and, indeed, on many other issues, including surveillance and cybersecurity – is often framed as privacy versus security – with 'privacy' representing the position of those who want strong encryption to be available, as opposed to 'security', representing those who support restrictions or controls on its use.

In this framing, privacy and security are understood as participants in a zero-sum game, in which strengthening one means weakening the other. A politician advocating for tighter restrictions on encryption might therefore acknowledge some adverse consequences for privacy, but argue that these concerns are outweighed by the need for stronger security.

But this framing is increasingly contested. Many advocates now argue that privacy and security are, in fact, mutually reinforcing principles; and policies which respect the privacy of users, like strong encryption, also make everyone more secure.

There's plenty of evidence to support this. We know that strong, widespread encryption reduces the risk of data breaches and hacks, protects online transactions and banking services, and discourages street-level theft of smartphones and other digital devices. This is not just beneficial for individuals; it can also reduce the workload of law enforcement agencies. And the state, through its own use of encryption, is also better able to protect its own security, through a more resilient cyber infrastructure.

At the same time, weak encryption does not just diminish the privacy of individuals – it also diminishes security. If limitations are placed on the use of encryption, or vulnerabilities created, exploitation of these by criminals and other malicious actors (whether against individuals, businesses or even the state itself) becomes much more likely. Reflecting this, some have argued that 'security versus security' might be a more appropriate way to frame the debate.

THE STAKEHOLDERS

The chart below attempts to set out some of the key roles played by each of the main stakeholder groups in the encryption debate. We'll examine these stakeholders and their positions in more detail later in the chapter. The chart is not meant to be exhaustive of every role played by every actor in every group, and the extent and reason for involvement in a given role varies greatly from group to group. Indeed, even within the same group, different stakeholders may take very differing roles and positions, reflecting the multifaceted nature of the encryption debate.

STAKEHOLDER	DEVELOPER	USER	REGULATOR	OPPONENT
STATES	✓	✓	✓	✓
INTERNATIONAL ORGANISATIONS		✓	✓	✓
THE PRIVATE SECTOR	✓	✓		
CIVIL SOCIETY		✓		✓
INDIVIDUALS		✓		

Developer: 'Developer' means that the stakeholder group actually develops and produces encryption technology.

User: 'User' means that the stakeholder group uses encryption for some purpose.

Regulator: 'Regulator' means that the stakeholder group regulates encryption in some way, through law or policy.

Opponent: 'Opponent' means a stakeholder group that supports some restrictions, limitations or controls on the use of encryption.

States

The 'state' includes all branches of government of an internationally recognised nation or territory. This includes government departments, security and law enforcement agencies, regulators, and other public bodies. As noted in chapter 1, a state may be a user of encryption for a range of purposes, such as protecting the data it collects on individuals or ensuring the secrecy of sensitive communications. The state may benefit from the use of encryption in other ways, such as by reduced levels of certain crimes, both cybercrimes (such as data theft, hacking or identity fraud) and 'offline' crime such as theft of smartphones and other digital devices (see Message 2 in chapter 6). It may be a regulator via the passage of encryption-related legislation or by setting up a body which regulates communications.

The state has many facets, each of which may have a different perspective on encryption. Security and law enforcement agencies may, for example, want restrictions on the use of encryption, so that they can more easily access communications which facilitate the commission of crime or terrorism. By contrast, government departments relating to economy, business or digital issues may support the use of strong encryption, judging that strong data protection creates a favourable climate for investment and growth. And government departments dealing with foreign affairs will likely want international standards to reflect their own country's standards on encryption – which means they might want to see them weakened or strengthened, depending on the country.

International organisations

In many cases, international organisations like the United Nations and its subsidiary organs, specialised agencies, and affiliated organisations, as well as the Organisation for Economic Co-operation and Development, have been instrumental in developing and facilitating the implementation of encryption policies (see chapter 5). These processes are largely state-led meaning that the outcome policies reflect the interests and positions of the states involved. Agreements arrived at through these bodies have tended to support strong encryption as a means of protecting human rights (see chapters 3 and 4) and promoting the digital economy. There are some processes within international organisations, however, which are not state-led: for example, reports produced by UN Special Rapporteurs (see chapters 3 and 4). However, again, these processes have tended, so far, to result in policies or positions which are supportive of strong encryption. Finally, as we will see in chapter 5, there are also a number of technical international bodies which set encryption-related standards and which may or may not include representatives of governments. These bodies focus on the technology of encryption and the development of universally agreed and used technical standards. Like states, international organisations are likely to employ encryption in their internal communications and operations.

Private sector

Businesses and the private sector (as we will look at more closely in chapter 5), are by and large the creators and distributors of encryption products and services. They are also likely to use encryption to ensure their relationships and interactions with clients, customers and partners remain confidential. Encryption also allows businesses to protect their intellectual property and conduct financial transactions securely.

As such, they are likely to support strong encryption so that their products remain commercially attractive and to protect their own uses of encryption.

Civil society

As noted in chapter 1, encryption is often a vital tool for human rights defenders, especially those working on controversial issues, or representing oppressed or persecuted groups. As such, encryption is particularly valuable for those who live or work in countries with authoritarian or repressive governments. Civil society organisations, along with other stakeholders, will use encryption to share information, organise themselves and report human rights abuses. However, it is also the case that some civil society organisations, such as those working with victims of domestic violence, child abuse or other victims of crime, may have concerns that encryption can be a hindrance to investigations in those areas, and thus support restrictions. Civil society also includes researchers and academics who help assure the integrity of encryption products and services by finding vulnerabilities that can later be updated and patched.

Individuals

While not a distinct stakeholder group, it is important to emphasise that all individuals are ultimately beneficiaries of encryption, being served both directly by encryption (e.g. as a means of keeping data secure, communicating privately, or avoiding fraud) but also indirectly through its use by the other stakeholders listed above, with which the individual user interacts in various forms.

THE DEBATE IN THE REAL WORLD

We've examined the premises of the current debate on encryption, and the different roles of stakeholders within it. But what does all this mean in the real world? As it is ultimately national laws, regulations and policies which have binding legal force, much of the debate has focused on efforts by states to regulate encryption in some way, usually (but not always) via some kind of limitation or restriction. In this section, we'll look at some of the ways that states have, historically and recently, attempted to limit or otherwise regulate encryption.

Top of the class!

Not all government policies relating to encryption seek to restrict, limit or control its use. There are examples where governments, through laws or policies, have recognised the benefits of strong encryption being available. For example, the German government's Digital Agenda for the years 2014-2017 included strong pro-encryption language ("[t]he use of encryption and other security mechanisms is necessary to ensuring Internet safety") and the Dutch government has also published an official policy emphasising the importance of both the right to privacy and to encryption. We will look at more examples in chapter 4.

Absolute prohibitions

Calls for an outright and absolute prohibition on the use of encryption are uncommon, but not without precedent. In 1993, for example, Colombia instituted a ban on encryption through mobile communications. And in 2011, the Pakistan Telecommunications Authority issued a directive which ordered all internet service providers and mobile phone companies in the country to prohibit users from sending encrypted information over the internet, and to report anyone who tried.

Weakening encryption standards

While not as drastic as prohibiting the use of encryption entirely, an alternative that has been seen is for a government to require, or collude in the setting of, weak technical encryption standards through law or policy. Perhaps the most notable instance of this was in in the US when, in 2013, the New York Times, the Guardian, and ProPublica revealed that the US National Security Agency (NSA) had purposefully worked to undermine encryption standards in order to preserve its own surveillance capabilities. The National Institute for Standards and Technology – an internationally recognised source for encryption standards which the NSA is required to consult – responded by establishing nine core principles to guide the establishment of future cryptographic standards.

Backdoors

Backdoors are perhaps the most widely discussed proposal of controls on encryption. In essence, a backdoor is any restriction on encryption standards which means that a user's **private key** can no longer ensure the absolute security and secrecy of the communication or data which is encrypted. As such, in certain circumstances, it would therefore be possible for the content of those communications or data to be accessed by another person.

One of the earliest proposals for a backdoor was the Clipper Chip – a chipset (a set of electronic components in an integrated circuit) – developed in the early 1990s by the NSA in the US, which, once integrated into a given item of hardware, gave law enforcement agencies access to any information stored on it. Under the proposal, the implementation of the technology was to be voluntary, but the government would have incentivised its use and there were concerns that it would eventually become mandatory. In 1994, after a technologist demonstrated a serious flaw in the Clipper Chip, the proposal was dropped.

The failure of the Clipper Chip has not killed off the idea of backdoors. In 2015, for example, Kazakhstan announced a new measure obliging all internet users to download a so-called 'National Security Certificate', which gives the government direct access to any hardware it is installed on. And in 2016, concerns were raised that the United Kingdom's Investigatory Powers Act 2016 would allow the government to require telecommunications operators to install backdoors so as to enable security and law enforcement agencies, once they had obtained a warrant, to access the content of communications.

Key escrows

Shortly after the official fall of the Clipper Chip, the US government suggested another proposal. This focused on encryption keys themselves and would have limited their length and required them to be held by one of a limited number of third-party licensed entities for access following due process. This type of system is known as mandatory key escrow because the encryption keys are viewed as being held in escrow (i.e. under the control of a third party) until law enforcement can satisfy the legal test for accessing data.

The proposal was dropped following criticism by lawmakers, international bodies, political leaders, security experts, and the European Commission, all of whom pointed out that it would damage businesses and undermine security. An important additional criticism was that the system would create 'honey pots' – highly desirous databases of information that could be targeted by ill-intentioned actors – which, if compromised, could lead to the exposure of vast amounts of personal data.

Despite this broad opposition, the idea of key escrows has resurfaced periodically, most recently in proposals, again in the US, for encryption keys to be broken up, with their constituent pieces stored in multiple locations by different certified entities. This idea, like those before it, has been criticised by security experts as weakening digital security.

Compulsory or voluntary corporate assistance

Since Edward Snowden's revelations about surveillance practices in the US and United Kingdom, large tech companies, including Apple and WhatsApp, have made moves towards strengthening encryption on their devices and services.

In response, some governments have made attempts to coerce or force companies into implementing weaker encryption practices than they would otherwise have adopted, or to undermine the security of their users by providing their information to government officials.

In the US, former FBI Director James Comey pleaded publicly with tech companies to do so in the name of public security, in response to Apple's promise to implement default device encryption on new versions of the iPhone.

Other countries have attempted to create laws or policies against the use of certain forms of encryption by companies: Russia passed a law in 2016 that could be interpreted to prohibit **end-to-end encryption** and China has put forward similar proposals.

In the United Kingdom, the Investigatory Powers Act 2016 gives the government the power to impose 'technical capability notices' on telecommunications operators. Draft regulations on what can be included in a technical capability notice include the ability "to disclose, where practicable, the content of communications or secondary data in an intelligible form and to remove electronic protection applied by or on behalf of the telecommunications operator to the communications or data".

Apple v. FBI

In early 2016, Apple refused a request from the FBI to provide access to encrypted data stored on an iPhone of one of the suspects in a terrorist attack in San Bernardino, saying that it did not possess the key. In response, the FBI obtained a court order under the All Writs Act (which dates from 1789) to attempt to force Apple into writing a new operating system that would allow the FBI to bypass the security protections, and therefore the encryption, on the phone. Apple opposed the court's order, arguing that complying would make its other products and services insecure, and vulnerable to intrusion from malicious actors.

In the end, the case was dropped after the FBI was able to gain access to the phone through a vulnerability discovered and used by a third party contractor. The exact nature of the vulnerability remains unknown and was neither disclosed to Apple nor entered into the US Vulnerabilities Equities Process (a process established to encourage the disclosure of vulnerabilities to manufacturers of software and devices so that they can be remedied to ensure that they are not discovered or exploited by a bad actor).

It is quite possible that this issue will come up again in some way before the courts, and a future case may well set a precedent that could even be followed in jurisdictions outside of the US.

Import and export controls

Historically, controls on the distribution of encryption have been a popular means of restricting its proliferation. In recent years, however, they have been seen less frequently.

The US has placed limitations on the export of **cryptography** in the form of licensing requirements since the establishment of the

US Munitions list in 1976. At the time, cryptographic tools were considered 'dual use' technologies, meaning they had both civilian and military applications. The controls on the export of such technology, among other things, helped preserve the US's surveillance capabilities: at the time, significant advances in encryption technology were being made in the US, putting it far ahead of other countries in terms of the strength of the encryption that was being produced commercially. By limiting its spread overseas, the US government was able to ensure that agencies like the NSA would be able to maintain their superior capabilities to monitor electronic communications abroad without any serious interference. But the restrictions also had impacts upon products sold within the US: in particular, they created additional costs for companies and not all could afford to produce separate products for domestic and international customers.

It was not until the 1990s that export controls would be relaxed. By then, they had become a serious financial burden on domestic businesses and were of increasingly low value for the security services, as foreign companies began catching up on encryption quality.

Encryption was first removed from the list of munitions and instead placed in the Export Administration Regulations (EAR) managed by the Department of Commerce. Then, the EAR limitations on encryption were loosened.

Import and export of cryptography has been tightly controlled in other parts of the world; notably China, where, since 1999, ownership over any encryption developed in China falls automatically to the state, and a license is required for the import of most commercial encryption products.

But even in the countries where these export limitations still exist, they are either significantly less stringent or more permissively enforced than those that were implemented in the US in the 1970s. At the same time, the easy availability of strong encryption developed in other jurisdictions – and the high cost of creating multiple products to satisfy different legal regimes – remain persuasive arguments against any expansion of import and export controls.

CHAPTER 3

WHY IS ENCRYPTION A HUMAN RIGHTS ISSUE?

Why is encryption a human rights issue?

Encryption is not just a policy question. It is now widely recognised as a tool which enables individuals to exercise a number of fundamental human rights.

When encryption is unavailable, or has restrictions, limitations or controls placed upon it, people are unable to trust that their online communications or activities are secure and private. In this chapter, we look at how this affects not only the right to privacy, but also – especially in more authoritarian or repressive states – the rights to freedom of expression, peaceful assembly and freedom of religion.

The role of international human rights law

Debates on encryption from a human rights perspective typically use international human rights law as their framework. The foundation of modern international human rights law is a document called the Universal Declaration of Human Rights (UDHR) which was adopted by the UN General Assembly in 1948. This was the first ever internationally agreed document setting out the fundamental human rights of all people. The UDHR is not a treaty and so is not binding on states as a matter of international law. However, a number of international human rights treaties developed since the UDHR (for example, the International Covenant on Civil and Political Rights (ICCPR), adopted in 1966) are binding on those states which have ratified them. In addition, many regional organisations have adopted their own human rights treaties, such as the European Convention on Human Rights, the American Declaration of the Rights and Duties of Man, and the African Charter on Human and People's Rights.

ENCRYPTION AND THE RIGHT TO PRIVACY

What is the right to privacy?

What privacy means – and what the right to it covers – is not an easy question to answer. The UN Special Rapporteur on the right to privacy, whose role, among other things, is to raise awareness about privacy issues, said in his 2016 report to the UN Human Rights Council that the concept of privacy "is known in all human societies and cultures at all stages of development and throughout all of the known history of humankind" but that "there is no binding and universally accepted definition of privacy".

UN Special Rapporteurs are independent experts, elected by the members of the UN Human Rights Council, with particular thematic mandates, such as freedom of expression, privacy, poverty or migrants. They publish annual reports on the subject matter of their mandate and receive and respond to complaints from individuals on related human rights issues.

While the UN Human Rights Committee issued a General Comment on the right to privacy in 1989, it doesn't provide a comprehensive scope of the right to privacy, simply giving some examples of what is covered – for example, information relating to an individual's private life, personal and body searches, and the holding of personal information on computers, data banks and other devices.

Established in 1977, the UN Human Rights Committee is a UN body made up of 18 independent experts on human rights, tasked with overseeing the implementation of the International Covenant on Civil and Political Rights. Among other things, the Committee issues 'General Comments' which elaborate on different rights within the ICCPR and how they should be implemented by states.

There are some issues, however, which are generally recognised as falling within the scope of the right to privacy:

- Personal autonomy, including decision-making about your identity;
- Physical and psychological integrity, i.e. decision-making relating to your body, and good physical and mental health;
- Control over private and confidential information and communications, including how such information and communications are stored and shared;
- Control over information about one's private life, including photographs and videos;
- Surveillance.

To make matters more confusing, the new forms of online communication and interaction offered by the internet, and the growing online footprints of individuals, have raised new questions about what is – and isn't – covered by the right to privacy. If photographs and videos of you are part of your private life, is it a violation if they are shared online by your friends and family? What about if they are shared by people you don't know? Can you change your mind about them being shared later? How much control should you have over personal information collected by companies which they might want to use or even sell to others for advertising purposes? These questions have not been fully answered, although data protection laws have sought to address the issues raised.

Data protection laws

Dozens of countries around the world have some form of data protection legislation. While the precise scope and enforcement mechanisms of these pieces of legislation vary, they by and large set out legal protections for individuals and the use of information or data which relates to them by others (such as public bodies, businesses and the private sector, and others).

What does this have to do with encryption?

As we've seen above, there is no single, universally agreed definition of privacy, but there are several core aspects of the concept which are generally agreed upon. Two of these aspects illustrate the relevance of encryption to human rights.

I. Relationships with others

The first is the idea that a person's privacy (or private life) includes, to an extent, their relationships and interactions with other people.

The relevance of privacy to interactions with others is also recognised in the wording of the right to privacy in many international human rights treaties: the ICCPR, for example, provides that "No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence" (Article 17) and many regional human rights instruments use similar wording. For example, the European Convention on Human Rights says that "Everyone has the right to respect for his private and family life, his home and his correspondence." (Article 8(1)) and the American Declaration of the Rights and Duties of Man says that "Every person has the right to the protection of the law against abusive attacks upon his honor, his reputation, and his private and family life." (Article V)

What the courts have said

In 1976, the European Court of Human Rights said in that the right to respect for a person's private life "comprises also, to a certain degree, the right to establish and to develop relationships with other human beings". (*X. v. Iceland*, Application No. 6825/74 (1976))

2. Privacy and correspondence

When looking at encryption, the linking of privacy and correspondence in the ICCPR and other human rights instruments is particularly important: it makes clear that privacy of communications is an aspect of the right to privacy. While online communications may not have been envisaged at the time the UDHR and the ICCPR were drafted, the term 'correspondence' is technology-neutral and the UN Human Rights Council has regularly made clear that the same rights that people have 'offline' must also be protected 'online'.

The UN Human Rights Committee has said in its General Comment on the right to privacy that the linking of these issues means that correspondence "should be delivered to the addressee without interception and without being opened or otherwise read".

Similarly, the then UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, has said that:

The UN Human Rights Council is an intergovernmental body made up of 47 UN member states and, amongst other things, is tasked with making recommendations (called resolutions) to governments on particular human rights issues. It was established in 2006.

> *"In order for individuals to exercise their right to privacy in communications, they must be able to ensure that these remain private, secure and, if they choose, anonymous. Privacy of communications infers that individuals are able to exchange information and ideas in a space that is beyond the reach of other members of society, the private sector, and ultimately the State itself."*
>
> UN Human Rights Council, Report of the Special Rapporteur on the promotion and protection of the right to freedom of expression, Frank La Rue, UN Doc. A/HRC/23/40, 17 April 2013, Para 23.

Encryption offers a way for people to ensure that their communications are private and to be confident that, even if they are intercepted, they cannot be read. To use an 'offline' analogy, since people should be free to write or speak to others in any language or code they wish, so they should also be able to use encryption to encode their online communications, a position which is also taken by international human rights law.

While international human rights law does allow for some limitations on the right to privacy, these are very narrow and we'll look at them in more detail in chapter 4.

ENCRYPTION AND THE RIGHT TO FREEDOM OF EXPRESSION

What is the right to freedom of expression?

In contrast to the right to privacy — which is not defined in any international human rights instruments — the scope of the right to freedom of expression is relatively well-understood.

Indispensable and essential

In its General Comment on freedom of opinion and expression, the UN Human Rights Committee called the right to freedom of expression an "indispensable [condition] for the full development of the person" and "essential for any society".

Article 19 of the UDHR says that the right to freedom of expression includes "the freedom to seek, receive and impart information and ideas through any media and regardless of frontiers", language mirrored in several regional human rights instruments. Article 19(2) of the ICCPR has similar wording, but instead of "through any media" uses "either orally, in writing or in print, in the form of art, or through any other media of his choice". Regional instruments use different wording:

- The European Convention on Human Rights says that "Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers." (Article 10(1))
- The American Declaration of the Rights and Duties of Man says that "Every person has the right to freedom of investigation, of opinion, and of the expression and dissemination of ideas, by any medium whatsoever." (Article IV)

- The African Charter on Human and Peoples' Rights says that "1. Every individual shall have the right to receive information. 2. Every individual shall have the right to express and disseminate his opinions within the law." (Article 9)

The term 'any other media', like the term 'correspondence' in relation to the right to privacy, is technology-neutral. As noted above, the UN Human Rights Council has made clear that the same rights that people have 'offline' must also be protected 'online', and the UN Human Rights Committee has confirmed in its General Comment on freedom of opinion and expression that "expression" includes "electronic and internet-based modes of expression".

What does this have to do with encryption?

Because it is, of course, possible to communicate in many contexts without using encryption, the link between encryption and freedom of expression may not be immediately obvious.

But what if you live in a country with widespread government surveillance and censorship? Or where expressing (or receiving) information relating to a certain subject matter – for example, LGBT issues – could put you in danger? Just the perception that negative consequences might occur from sending or receiving information can restrict the right to freedom of expression.

This is where encryption comes in. By offering users privacy in their communications, encryption enables them to exercise their right to freedom of expression more fully.

Privacy as a gateway

In his 2015 report to the UN Human Rights Council, the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression has called privacy a "gateway" for freedom of expression, with encryption giving individuals and groups "a zone of privacy online to hold opinions and exercise freedom of expression without arbitrary and unlawful interference or attacks".

In a 2015 report on encryption, anonymity and the human rights framework, the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, highlighted a number of specific instances where encryption facilitates the full enjoyment of the right to freedom of expression:

- Where the government imposes censorship of certain content or criminalises certain forms of expression (such as blasphemy, certain political or religious views, or criticism of government), encryption allows people to access such content and share such expressions anonymously and without fear of persecution.
- Where governments filter certain online content or block access to certain information or data (for example by blocking searches with keywords such as 'democracy'), encryption allows individuals to overcome such filtering and blocking, better enabling information to flow both within a country and across borders.
- Encryption technology is, in and of itself, a specific medium through which information can be sent and received, so restrictions on encryption are in and of themselves interferences with the right to freedom of expression.

Just as is the case with the right to privacy, international human rights law does allow for some limitations on the right to freedom of expression, but these are similarly narrow (and will be covered in more detail in chapter 4).

ENCRYPTION AND OTHER HUMAN RIGHTS

All human rights are universal, indivisible, interdependent and interrelated. Restrictions of one right will often impact negatively upon the exercise of other rights, and the facilitation of one right will often further enable the exercise of others. As noted at the start of this chapter, this is particularly true of the rights to privacy and to freedom of expression. As well as being human rights in and of themselves, they enable the greater enjoyment of others such as:

- **Freedom of association**. The right to freedom of association is protected under Article 20 of the UDHR and Article 22 of the ICCPR, as well as in regional human rights instruments. By its very nature, the ability to associate with others, in whatever forum, requires the ability to communicate and interact with others. By enabling private communications, encryption allows people whose association with others could put them at risk (whether from state or non-state actors) both to associate online, through encrypted communications, and to organise physical association more safely. Associations which could put people at risk if discovered range from context to context, but could include political opposition groups, human rights organisations, and organisations representing or comprising minority groups where they face persecution, such as LGBT persons or ethnic minorities.
- **Right of peaceful assembly**. The right of peaceful assembly is also protected under Article 20 of the UDHR, alongside freedom of association, but has separate protection under the ICCPR through Article 21, as well as in regional human rights instruments. As with the right to freedom of association, the right of peaceful assembly, by its nature, requires those wanting to exercise that right to be able to communicate and coordinate with other people. By enabling private communications, encryption creates the conditions under which assembly can happen.

Just as there are associations which governments attempt to restrict, so there are forms of protest or assembly which governments seek to restrict (or which might even be disrupted by non-state actors). The ability to coordinate such protests and assemblies privately can therefore be crucial in enabling them to take place.

Throttling encryption and cracking down on protests in Iran

Iranian governments have, at times, placed significant restrictions on the use of encryption, including by prohibiting certain communication apps which encrypt the content of communications, and by throttling traffic that uses the encrypted SSH protocol to run at less than 20% of the network's full speed. During the presidential election in 2013, and with the authorities fearful of protest, throttling was intensified so that the speed of encrypted traffic was just 5% or less of normal speed. As a result, it became more difficult for individuals to organise and coordinate legitimate protests, and for political opposition activists to communicate and have their voices heard.

Freedom of religion. The right to freedom of religion is (alongside the right to freedom of thought and conscience) protected under Article 18 of both the UDHR and the ICCPR as well as in regional human rights instruments. Freedom of religion includes not only the right to hold a particular religious belief, but also "individually or in community with others and in public or private" to manifest that religion or belief "in worship, observance, practice and teaching". In many countries, religious minorities are persecuted by state and non-state actors, and forced to observe their faith in private. Encryption offers a way for religious groups who face risks in public manifestation to be able to exercise their freedom of religion and worship, observe, practice and teach their faiths privately with others, free from the risk of persecution.

CHAPTER 4

WHAT WOULD HUMAN RIGHTS-RESPECTING ENCRYPTION LAWS AND POLICIES LOOK LIKE?

What would human rights-respecting encryption laws and policies look like?

As we have seen in the previous chapter, human rights are highly relevant to the **encryption** debate; and restrictions on the use of encryption through laws and policies can violate fundamental human rights such as the right to privacy and freedom of expression.

Laws and policies relating to encryption therefore need to be compatible with human rights and states have obligations under international human rights law to make sure that this is the case.

The standards relating to the rights most affected by encryption — to privacy and to freedom of expression — have been set out in some detail by the bodies discussed in the previous chapter. And, in 2015, the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, published a report which specifically examined encryption (as well as anonymity) from the perspective of international human rights law. As such, there is now a clear framework for assessing whether encryption laws and policies are human rights-respecting, which we will look at in this chapter.

THE STARTING POINT: GUARANTEEING THE ABILITY TO USE ENCRYPTION

Given that encryption is an enabler of many human rights, the starting point for any lawmaker or policymaker should be to ensure that the population has the ability to use encryption and in any form (and strength) that they choose. Ideally, this should be set out in the very text of the policy or legislation.

Examples of best practice

Some states have passed legislation which specifically protects the right of the population to use encryption. In Luxembourg, for example, the Law on Electronic Commerce says that "[t]he use of cryptographic techniques is free". In Brazil, the Civil Rights Framework for the Internet guarantees the "inviolability and confidentiality of [internet users'] stored private communications". And in Zambia, the Electronic Communications and Transactions Act, 2009, explicitly states that individuals may use encryption "regardless of encryption algorithm selection, encryption key length chosen, or implementation technique or medium used".

An absolute ban on the use of encryption will therefore always be a clear breach of human rights. And a high level of state regulation of encryption, even if it falls short of an absolute ban, may amount to a ban in practice if, for example, that regulation involves the requirement of licences to use encryption, the setting of weak technical standards for encryption or significant controls on the importation and exportation of encryption tools. This is because if encryption tools are limited to those which meet government-approved standards, or if the importation and exportation of encryption tools are controlled by the state, state agencies will be able to ensure that encryption software contains weaknesses allowing them to access the content of communications. The privacy and security provided by encryption, and therefore any benefits of using encryption, disappear.

There are examples of states banning the use of encryption entirely, such as in Pakistan where, in July 2011, the Pakistan Telecommunication Authority ordered all internet service providers and mobile phone companies to implement regulations prohibiting encryption and report all users who sent encrypted information over the internet.

PERMISSIBLE RESTRICTIONS, LIMITATIONS AND CONTROLS UNDER INTERNATIONAL HUMAN RIGHTS LAW

As discussed in chapter 2, governments do have a legitimate interest in tackling terrorism, crime and public disorder, and certain limited interferences with the use of encryption are permissible. The human rights framework is clear, however, that because encryption is an enabler of human rights, any such restrictions or interferences with its use will only be permissible if a three-stage test is met:

1) Any restrictions or interferences must be 'provided for by law';
2) They must be in pursuance of a 'legitimate aim'; and
3) They must be 'necessary' to meet that aim.

1) Any restrictions should be provided for by law

The first part of the test is that any restrictions must be 'provided for by law'. This means, in the case of encryption, that there must be a clear, accessible and comprehensible legal framework in place relating to the restrictions on encryption or interferences with its use. In developing that framework, or in revising an existing framework, proposals should go out for full public comment. The framework should also ensure that:

- State authorities do not have absolute discretion in when and how they interfere with the use of encryption, but that there are clear criteria and limitations in place for when this can take place;
- There are strong procedural and judicial safeguards to guarantee the due process rights of any individual whose use of encryption is subject to restriction or who is required to decrypt communications; and
- A court, tribunal or other independent adjudicatory body supervises the application of any restriction or interference.

2) Any restrictions should be in pursuance of a legitimate aim

The second part of the test is that any restrictions must be in pursuance of a 'legitimate aim'. The international human rights framework sets out these legitimate aims as:

- Respect of the rights or reputations of others;
- The protection of national security;
- The protection of public order;
- The protection of public health; and
- The protection of public morals.

Because governments sometimes use these legitimate aims as a pretext for illegitimate purposes, any restrictions should be applied narrowly.

'Backdoors' and preventing terrorism and crime

Governments will often try to defend proposals to introduce 'backdoor' access into encryption products and services by arguing that security and law enforcement agencies need access to the encrypted conversations of terrorists and criminals to prevent attacks and crimes. There are two problems with this argument. First, as the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression has said, governments "have not demonstrated that criminal or terrorist use of encryption serves as an insuperable barrier to law enforcement objectives". Second, if backdoors were introduced, this would undermine the security of all online users, and would create a permanent risk of intrusion into encrypted communications by other state or non-state actors, such as hackers.

3) Any restriction should be necessary

The third part of the test is that any restrictions, as well as being in pursuance of of a legitimate aim, should be 'necessary'. This also includes an assessment of proportionality. While there is no single universal definition of 'necessary' and 'proportionate', the European Court of Human Rights has interpreted the former to mean something more than 'useful', 'reasonable' or 'desirable'. (See, for example, *Handyside v. United Kingdom*, Application No. 5493/72, (1976)).

In relation to the latter, the UN Human Rights Committee has said, in a General Comment, that:

> *"[R]estrictive measures must conform to the principle of proportionality; they must be appropriate to achieve their protective function; they must be the least intrusive instrument amongst those which might achieve their protective function; they must be proportionate to the interest to be protected (…) The principle of proportionality has to be respected not only in the law that frames the restrictions but also by the administrative and judicial authorities in applying the law."*
>
> United Nations Human Rights Committee, General Comment No. 34: Article 19: Freedoms of opinion and expression, UN Doc. CCPR/C/GC/34, 12 September 2011, Para 34.

In his 2015 report, the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression said that restrictions or limitations on encryption "must target a specific objective and not unduly intrude upon other rights of targeted persons". He also said that "a proportionality analysis must take into account the strong possibility that encroachments on encryption and anonymity will be exploited by the same criminal and terrorist networks that the limitations aim to deter".

Key disclosure orders and decryption orders

Rather than requiring 'backdoors', many states instead have legislation which, under certain circumstances, either requires an individual to provide the **key** for the **decryption** of communications ('key disclosure orders') or for decrypted versions of specified encrypted communications ('targeted disclosure orders'). Provided that there is a clear, legal framework for the use of such orders, and that they are only used when pursuing one of the legitimate aims set out above (such as to prevent crime), such orders are more likely to be proportionate, given that they are targeted on individuals and specified communications. However, to ensure that such orders are only used in a proportionate way, there are a number of further requirements:

- They should only be used when they are based on clear, publicly accessible law;
- They should be clearly limited in scope and focused upon a particular, identifiable target;
- They should be authorised and supervised by an independent and impartial judicial authority, in particularly to preserve the due process rights of the individual(s) concerned; and
- They should only be used when necessary and when less intrusive means of investigation are not possible.

CHAPTER 5

WHERE ARE ENCRYPTION STANDARDS SET?

Where are encryption standards set?

As we have seen in the earlier chapters, particularly chapter 2, there is a significant debate going on regarding the use of **encryption** and what restrictions, limitations or controls, if any, there should be on its availability and use.

However, standards and policies relating to encryption are set in a wide variety of different forums, all with different makeups and roles. The different outputs of these forums can be broadly divided into four categories:

- The encryption technology, software, services and products themselves that people use;
- Technical standards (which may be legally binding or non-binding);
- Policies, guidelines and best practice documents on the use of encryption and what restrictions are permissible (which are legally non-binding); and
- National legal and regulatory frameworks (which are legally binding).

In this chapter, we look at the major forums within these four broad categories of outputs, their roles and some detail on the specific different encryption standards or policies which they set.

The relationship between these forums and outputs is outlined on the table opposite.

	ENCRYPTION TECHNOLOGY, PRODUCTS AND SERVICES	TECHNICAL STANDARDS (BINDING)	TECHNICAL STANDARDS (NON-BINDING)	POLICIES, GUIDELINES AND BEST PRACTICE ON THE USE OF ENCRYPTION AND PERMISSIBLE RESTRICTIONS	LEGAL AND REGULATORY FRAME-WORKS
STATES: GOVERNMENTS					✓
STATES: LEGISLATURES					✓
STATES: REGULATORS					✓
STATES: OTHER STATE AGENCIES	✓				✓
INTERNATIONAL ORGANISATIONS: MULTILATERAL FORUMS				✓	
INTERNATIONAL ORGANISATIONS: STANDARDS-SETTING BODIES			✓		
NATIONAL STANDARDS-SETTING BODIES		✓	✓		
PRIVATE SECTOR	✓				

ENCRYPTION TECHNOLOGY, SOFTWARE PRODUCTS AND SERVICES

Private sector

The actual products and services which incorporate encryption are largely developed by private sector organisations:

- **Email clients which provide encrypted email services.** Some of these, such as Apple Mail (developed by Apple, and using **end-to-end encryption**) and Gmail (developed by Google, and using a protocol called Transport Layer Security to provide encryption for **data in transit**) are general email clients which do not explicitly promote themselves as providing encrypted services. There are also products and programmes such as Pretty Good Privacy (developed by Philip Zimmermann, a software engineer) and Gpg4win (developed by the Gpg4win Initiative) which are specifically designed to encrypt emails and files attached to emails.
- **Secure messaging services which provide encrypted messaging services.** There are a large number of messaging services using various encryption protocols to provide end-to-end encryption. Some of the most popular and well known include Telegram, Signal, Wickr Me, WhatsApp, Viber, Silent Phone and Facebook Messenger. Some use encryption by default whereas others require manual activation.
- **Disk encryption.** Unlike email clients and secure messaging services which encrypt data in transit, disk encryption focuses on encrypting **data at rest** while it is stored on a device. Some of the most popular include Check Point Full Disk Encryption, Dell Data Protection Encryption, McAfee Complete Data Protection, Sophos SafeGuard, Symantec Endpoint Encryption, DiskCryptor, Apple FileVault and Microsoft BitLocker.

- **File systems.** Whereas disk encryption encrypts an entire disk, filesystem level encryption encrypts individual files or directories within the disk by the file system itself. Some of the most common include Encrypting File System (for Windows), AdvFS (for OSF/1, the open source version of Unix) and ext4 (for Linux).
- **File backup and sharing.** Finally, there are also products and services which provide encrypted backup (and sharing) of files via cloud storage, such as Tresorit, TeamDrive and Wuala.

As the encryption software is developed by the companies providing the products and services themselves, there is little involvement of other actors, although the software must, of course, be permitted by the applicable national legislation and policies if they are to be provided or used in a particular country.

State agencies

Some encryption software is also developed by states themselves, almost always for the sole use of the state, particularly intelligence and security agencies. The National Security Agency (NSA), for example, is a military intelligence organisation and part of the Department of Defense in the US. The NSA undertakes research and development into encryption products and standards for use by US government agencies.

Should civil society engage?

There's arguably little benefit in human rights defenders engaging with the developers or providers of encryption technologies or software. After all, they don't have any say over the technical standards which determine the strength and availability of encryption, and that's ultimately what really matters. The standards setting and policymaking bodies which do (see below) are a more obvious target.

There are, however, exceptions. If an existing service provider – for example, an email or online communications provider – doesn't provide encryption by default in its service, advocacy to encourage them to incorporate it may be a worthwhile exercise.

A real life example of this relates to Transport Layer Security (TLS), a particular form of encryption for internet communications while they are in transit (transit encryption), developed by the Internet Engineering Task Force (see below) in 1999. Over the 2000s, a series of campaigns and advocacy efforts called for it to be adopted by all online service providers. These included a letter campaign by the American Civil Liberties Union signed by 37 law professors and security experts, and awareness raising by the Electronic Frontier Foundation, who would review companies and give credit in their gold star ratings to companies which adopted it. As a result of these campaigns, and other efforts, TLS was adopted by a number of major online service providers including Google (both as a search engine and through its email service, Gmail), Yahoo!, Microsoft, Cloudflare and Wordpress. This is an example of where direct engagement with encryption developers can prove useful.

TECHNICAL STANDARDS

Although the products and services which use encryption are developed largely by the private sector, there are a number of bodies which set common standards, some at the international level, others at the national level. These standards do not set out what national law or policies should look like, nor do they detail when encryption should be used. Instead, they provide technical standards on the development and use of encryption algorithms and protocols to ensure that encryption, when used, is universally consistent and effective. These technical standards usually aren't legally binding. But, because of the overwhelming interest in ensuring the universal usability of those products and services, they are, in practice, invariably used by those developing encryption products and services. In some countries, the standards may be legally binding if developed by a national standards-setting body or other agency which has authority to set standards which are legally enforceable. However, this is uncommon.

International organisations: standards-setting bodies

International Organization for Standardization

The International Organization for Standardization (ISO) is an independent NGO made up of 163 national standards-setting bodies and is based in Geneva, Switzerland. It is the world's largest standards-setting organisation and has developed thousands of standards on a vast range of issues, with hundreds relating to **cryptography**. The standards themselves are set in a technical committee (the technical committee on information technology), which is actually a joint committee between the ISO and the International Electrotechnical Commission (see below) with the acronym ISO/IEC JTC 1.

Within ISO/IEC JTC 1 there is a subcommittee (ISO/IEC JTC 1/SC27) with a specific mandate of developing standards on IT security techniques which includes "generic methods, techniques and guidelines to address both security and privacy aspects". This includes "cryptographic and other security mechanisms, including but not limited to mechanisms for protecting the accountability, availability, integrity and confidentiality of information". ISO/IEC JTC 1/SC27 has developed a number of standards on different **encryption** algorithms.

International Electrotechnical Commission

Like the ISO, the International Electrotechnical Commission (IEC) is an independent, international standards-setting body. However, it only develops standards relating to electrical, electronic and related technologies. Based in Geneva, it has a smaller membership of 83 'National Committees'. As noted above, the standards relating to encryption are set in a joint technical committee comprising members of the ISO and the IEC, and focus exclusively on the technical aspects of encryption.

Internet Engineering Task Force

The Internet Engineering Task Force (IETF) is an international NGO and describes itself as a "large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet". Anyone can join the IETF and it develops voluntary internet-related standards through working groups of volunteers. It has developed several important standards relating to encryption on the internet, in particular algorithms and protocols that can be used to develop encrypted email, web browsing and communication services. Pretty Good Privacy, for example, uses an open source encryption standard developed by the IETF: RFC 4880.

World Wide Web Consortium

The World Wide Web Consortium (W3C) is a consortium of over 450 governmental, non-governmental and private sector organisations, as well as individuals, and is based at the Massachusetts Institute of Technology in the US. The W3C develops standards (called 'Recommendations') specifically relating to the World Wide Web, and within this scope has developed a specific Recommendation on a Web Cryptography API as well as other Recommendations on web-related encryption such as XML and media extensions.

Institute of Electrical and Electronics Engineers

The Institute of Electrical and Electronics Engineers (IEEE) is an independent non-governmental organisation which operates as a professional association for individuals working in technical fields. It has over 420,000 members around the world. Among other activities, it develops technology-related standards via a subsection, the IEEE Standards Association. The IEEE Standards Association has developed standards on **public key c**ryptography and encryption for storage devices.

International Telecommunication Union

The International Telecommunication Union (ITU) is a specialised agency of the UN based in Geneva, Switzerland. It is a multilateral body with over 190 member states, although other organisations such as regulatory bodies and telecommunications organisations can also be (non-voting) members. The ITU is a technical body, allocating radio-frequency bands, managing the database of satellite orbits, and setting international standards on telecommunication-related issues such as the transmission of television signals and international telephone routing.

More recently, the ITU has become involved in issues related to online communications. It is divided into three sectors, one of which, the Standardization sector develops international standards. These include standards related to encryption technologies such as public key certificates, voice encryption and encryption for OTT (over the top) providers (i.e. those who provide audio, video or other media over the internet as a standalone product, such as YouTube, Skype, Netflix and WhatsApp).

National standards-setting bodies

As well as international standards-setting bodies, there are national standards-setting bodies in most, but not all, countries. These bodies may develop their own national standards or adopt standards developed by the ISO or another international organisation. There may also be national bodies which focus exclusively on technological standards.

American National Standards Institute (US)

The American National Standards Institute (ANSI) is an independent non-profit organisation in the US. ANSI does not create standards itself; its role is mostly to promote the voluntary consensus, adoption and localisation of international standards from bodies such as ISO/IEC to its membership base of over 100,000 companies and government agencies. ANSI's work focuses on ensuring local products are able to be distributed internationally. The ANSI standards on encryption are contained in what is known as the 'X9 Encryption standards package'. This is a set of encryption standards mostly focused on financial transactions in retail and the financial services industry. ANSI forms the official US representation to both the ISO and IEC, and as such is the main conduit for standards between the international bodies and to the local US context.

National Institute of Standards and Technology (US)

The National Institute of Standards and Technology (NIST) is a US government agency which forms part of the Department of Commerce. NIST's work, amongst other things, is to "[implement] practical cybersecurity and privacy through outreach and effective application of standards and best practices necessary for the U.S. to adopt cybersecurity capabilities". The primary mechanism through which NIST creates encryption standards is through the Federal Information Processing Standards (FIPS). FIPS are made available to US government agencies and government contractors for voluntary use. Many of these relate to encryption (such as 140-2 - Security Requirements for Cryptographic Modules, 186-4 - Digital Signature Standard and 197 - Advanced Encryption Standard). Many FIPS specifications are modified versions of standards from other international standards-setting bodies, such as the IEEE and the ISO.

Should civil society engage?

Most of the technical standards-setting bodies are already developing strong encryption standards, so engagement by civil society is less crucial than with the bodies which set policies, guidance, and legislative and regulatory frameworks, which are discussed below.

One exception to this general proposition is international organisations which are made up of states, rather than technical experts or representatives of national standards-setting bodies. This is because the standards set by such bodies are likely to be influenced by national policy positions, rather than pure technical considerations. In the context of encryption, this could be a government which opposes the availability of strong encryption, and so seeks weaker international technical standards. One example of an international standards-setting body which is made up of states is the International Telecommunication Union. There may be obstacles to civil society engagement in such bodies, which do not always have formal processes for involving civil society, or may require steep membership fees to engage.

POLICIES, GUIDELINES AND BEST PRACTICE ON THE USE OF ENCRYPTION AND PERMISSIBLE RESTRICTIONS

While technical standards are developed by the international and national standards-setting bodies, other international and regional bodies have developed policies and guidelines on when encryption should be used and on when it can or should be restricted, controlled or limited.

The weight of such guidelines and policies varies: some have the status of 'soft law' (and are therefore persuasive, albeit not binding, on national governments and courts), while others are merely suggestions of best practice. Three of the most important examples of such organisations are the United Nations, the Council of Europe and the Organisation for Economic Co-operation and Development. We'll also look at a couple of other international forums which have recently made statements regarding encryption.

United Nations

The main focus of the United Nations (UN) on encryption has been from a human rights perspective. As international human rights law has almost entirely developed from UN processes, it has been different bodies within the UN which have applied that legal framework to the issue of encryption. Indeed, much of chapters 3 and 4 of this guide have used UN sources in setting out how encryption is a human rights issue and what rights-respecting encryption laws and policies would look like. Out of these sources, three have provided most of the guidance: the UN Human Rights Council, the UN Human Rights Committee and the UN Special Rapporteurs.

UN Human Rights Council

As noted in chapter 3, the UN Human Rights Council is an intergovernmental body, established in 2006, made up of 47 UN member states. Among other things, it is tasked with making recommendations (called resolutions) to states on particular human rights issues. These resolutions are 'soft law', meaning that they are persuasive, but not legally binding, on governments and courts.

What has the UN Human Rights Council said about encryption?

The UN Human Rights Council has regularly made clear that the same rights that people have 'offline' must also be protected 'online'. In 2017, for the first time, it passed a resolution with explicit reference to encryption, noting that:

"[I]n the digital age, technical solutions to secure and to protect the confidentiality of digital communications, including measures for encryption and anonymity, can be important to ensure the enjoyment of human rights, in particular the rights to privacy, to freedom of expression and to freedom of peaceful assembly and association".

The resolution encouraged business enterprises "to work towards enabling technical solutions to secure and protect the confidentiality of digital communications, which may include measures for encryption and anonymity".

It also called upon states "not to interfere with the use of such technical solutions, with any restrictions thereon complying with States' obligations under international human rights law".

UN Human Rights Committee

As noted in chapter 3, the UN Human Rights Committee is made up of 18 independent experts on human rights and tasked with overseeing the implementation of the International Covenant on Civil and Political Rights (ICCPR). Among other things, the Committee develops 'General Comments' which interpret and elaborate on different rights within the ICCPR and how they should be implemented by states.

What has the UN Human Rights Committee said about encryption?

The UN Human Rights Committee has not made explicit reference to encryption in any of its General Comments. However, in its General Comment on the right to privacy, it has said that correspondence "should be delivered to the addressee without interception and without being opened or otherwise read" and that "interceptions of telephonic, telegraphic and other forms of communication, wire-tapping and recording of conversations should be prohibited".

UN Special Rapporteurs

As noted in chapter 3, UN Special Rapporteurs are independent experts, elected by the members of the UN Human Rights Council, with particular thematic mandates, such as freedom of expression, privacy, poverty or migrants. They publish annual reports on the subject-matter of their mandate and receive and respond to complaints from individuals on related human rights issues.

What have the UN Special Rapporteurs said about encryption?

In 2013, the then UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, said that:

"In order for individuals to exercise their right to privacy in communications, they must be able to ensure that these remain private, secure and, if they choose, anonymous. Privacy of communications infers that individuals are able to exchange information and ideas in a space that is beyond the reach of other members of society, the private sector, and ultimately the State itself."

He also said that:

"The security and anonymity of communications are also undermined by laws that limit the use of privacy-enhancing tools that can be used to protect communications, such as encryption", that "[i]ndividuals should be free to use whatever technology they choose to secure their communications" and that "[s]tates should not interfere with the use of encryption technologies, nor compel the provision of encryption keys".

In 2015, the current UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, published a report which looked specifically at encryption and anonymity, and summarised the position as follows:

"Encryption and anonymity, and the security concepts behind them, provide the privacy and security necessary for the exercise of the right to freedom of opinion and expression in the digital age. Such security may be essential for the exercise of other rights, including economic rights, privacy, due process, freedom of peaceful assembly and association, and the right to life and bodily integrity. Because of their importance to the rights to freedom of opinion and expression, restrictions on encryption and anonymity must be strictly limited according to principles of legality, necessity, proportionality and legitimacy in objective."

Council of Europe

The Council of Europe (CoE) is an international organisation comprising 47 member states with the aim of upholding human rights, democracy and the rule of law in Europe. One of the organs of the CoE is the Parliamentary Assembly of the Council of Europe (PACE) comprising parliamentarians from all CoE member states

and which develops recommendations, resolutions and opinions on issues relevant to the CoE. Within PACE, there are a number of committees which publish reports. These reports, along with the recommendations, resolutions and opinions passed by PACE are not legally binding on member states of the CoE , but are persuasive in setting the standards expected of them and have been referred to by courts when faced with human rights cases.

What has the Council of Europe said about encryption?

In 2015, the PACE Committee on Legal Affairs and Human Rights published a report on mass surveillance in which it said:

"[S]ome aspects of mass surveillance, such as the deliberate weakening of encryption and other Internet safety standards for the purposes of facilitating data collection, present a grave danger for national security."

PACE itself passed a Resolution based on the report in which it endorsed:

"[T]he European Parliament's call to promote the wide use of encryption and resist any attempts to weaken encryption and other Internet safety standards, not only in the interest of privacy, but also in the interest of threats against national security posed by rogue States, terrorists, cyberterrorists and ordinary criminals."

Organisation for Economic Co-operation and Development

The Organisation for Economic Co-operation and Development (OECD) is an international organisation comprising 35 states with a mission to promote policies that will improve the economic and social well-being of people around the world. The main work that the OECD does relating to encryption is through a document called the OECD Cryptography Guidelines which were published in 1997 and are reviewed every five years. The OECD body which reviews the Guidelines is called the Working Party on Security and Privacy in the Digital Economy and it is part of the OECD's Committee on the Digital Economy which meets twice a year.

What has the OECD said about encryption?

The OECD Cryptography Guidelines say:

"The fundamental rights of individuals to privacy, including secrecy of communications and protection of personal data, should be respected in national cryptography policies and in the implementation and use of cryptographic methods.

Cryptographic methods can be a valuable tool for the protection of privacy, including both the confidentiality of data and communications and the protection of the identity of individuals."

Other international forums

As well as the international and regional organisations listed above, there are a variety of more informal groupings of states where encryption has been discussed alongside other relevant issues, with positions or commitments set out upon which the states have agreed. Two examples are the G20 and the Five Eyes:

G20:

The G20 was established following the global financial crisis in 2008 as a means for the governments of 20 leading economies to discuss financial and economic policy. The G20 meets annually under a presidency which rotates among the members, and the scope of its discussions has expanded in recent years to include digital and digitalisation issues. In its 2017 Leaders' Declaration, agreed by all states at the end of the annual summit, the G20 noted that "trust in digital technologies requires (...) security in the use of ICT" and that its members therefore supported "the free flow of information while respecting applicable legal frameworks for privacy, data protection and intellectual property rights".

While this position is positive, the G20 also published a statement on countering terrorism, with a dedicated section on "countering radicalization conducive to terrorism and the use of internet for terrorist purposes", which states that "[i]n line with the expectations of our peoples we also encourage collaboration with industry to provide lawful and non-arbitrary access to available information where access is necessary for the protection of national security against terrorist threats". The G20 has a dedicated civil society engagement mechanism, 'Civil 20', which hosts its own summit prior to the G20's and publishes a Communiqué with the aim of influencing the G20's outcomes.

Five Eyes:

The Five Eyes is an intelligence alliance of five countries (the US, the UK, Canada, Australia and New Zealand) who cooperate on security and intelligence matters. The relevant government ministers from the five countries meet on occasion and, in 2017, published a 'Five Country Ministerial 2017 Joint Communiqué' with language on encryption, stating that "encryption can severely undermine public safety efforts by impeding lawful access to the content of communications during investigations into serious crimes, including terrorism" and that the governments "committed to develop our engagement with communications and technology companies to explore shared solutions while upholding cybersecurity and individual rights and freedoms".

Should civil society engage?

Yes — definitely! The forums listed above develop policies, guidelines and positions which, while not necessarily binding, are often followed by their members. Most international and regional organisations, including most of the ones listed above, have formal opportunities for civil society engagement, whether via an established forum, or opportunities for reports and submissions from civil society organisations. Even where they do not, civil society organisations can still raise awareness and campaign on **encryption**-related matters when they are discussed at these forums as a means of influencing the outcomes.

LEGISLATION AND REGULATORY FRAMEWORKS

While the technical standards for encryption are set by standards-setting bodies, and guidance is offered by international and regional organisations, ultimately states are sovereign to set their own national laws, regulations and policies on encryption, including when it can be used and whether it is subject to any restrictions, controls or limitations. Depending on the state concerned, these might be made by the legislature (or parliament), the government or by regulators or other state bodies.

Legislatures (primary legislation)

Primary legislation relating to encryption will have usually have been passed by a state's legislature (or parliament). Such legislation can either support the use of encryption or restrict it. For example, the Law on Cryptography (Law No. 2008-41) was passed by the National Assembly of Senegal and provides that "the use of cryptological [sic] means and services is free", whereas Law No. 418 of 1997 which was passed by the Congress of Colombia, prohibits the sending of messages which are encrypted or in "unintelligible language".

There is one supranational organisation with the power to pass binding legislation upon its members: the European Union (EU). As of 2017, no encryption-related legislation has been passed. However, in March 2017, the EU Commissioner for Justice, Věra Jourová, announced an intention to bring forward a range of proposals relating to the interception of encrypted communications — including both binding legislation and voluntary agreements, raising the prospect of EU legislation binding all EU member states.

Governments (secondary legislation)

Sometimes, there will also be secondary legislation that relates to encryption. Secondary legislation is usually developed by a government minister or other member of the executive rather than the legislature, and usually provides more detail on specific issues which are not covered in primary legislation. Secondary legislation can still have a significant impact on the use of encryption, however. For example, in Ethiopia, there is a government proclamation, the Proclamation on Telecom Fraud Offences (Proclamation No. 761/2012), which criminalises the manufacture, assembly or import of any telecommunications equipment without a permit. And in the United Kingdom, it is secondary legislation, rather than primary legislation, which sets out the circumstances under which the government can require telecommunication service providers to ensure they maintain the technical capability to decrypt encrypted communications.

Regulators and other state agencies (regulation)

Finally, in some states, it may be a regulator or other agency which sets binding rules on encryption, either in addition to, or instead of, the legislature and the government. For example, in Nigeria, the Nigerian Communications Commission is empowered to make binding rules on communications and, in 2013, published the draft Lawful Interception of Communications Regulations. Regulation 13 would provide that where there is a warrant for communications to be intercepted, and those communications are encrypted, the relevant communications provider must provide the National Security Adviser and the State Security Service with the key, code or access to the communication, or request a person who has the key or code so provide it, or provide the communication in an intelligible format.

Should civil society engage?

Yes - definitely! The legal and regulatory frameworks in states are legally binding and the most significant determinant of the availability of (and restrictions, limitations and controls on) encryption. The precise mechanisms by which civil society can engage and influence that legal and regulatory framework will vary considerably from state to state. In more open states, there may be public consultations on proposed legislation and policies when being considered by the government or the legislature. In more closed states, it may be almost impossible for civil society to input into the legislative process. Given the variation, national civil society organisations are generally best placed to determine what opportunities for engagement exist and how best to use them.

CHAPTER 6

HOW CAN HUMAN RIGHTS DEFENDERS AND CIVIL SOCIETY ORGANISATIONS ENGAGE?

How can human rights defenders and civil society organisations engage?

As we saw in the previous chapter, the technologies, standards, laws and policies relating to **encryption** are set in a wide range of forums and are constantly being reviewed and developed, meaning there are almost always chances for civil society to get involved in their development.

And in chapter 4, we set out what human rights-respecting encryption standards, laws and policies look like. Human rights defenders and civil society organisations can (and do) play a critical role in ensuring that those forums and bodies develop and decide upon encryption-related standards, laws and policies which are consistent with human rights. In this final chapter, we set out some of the messages that can be used in those forums to persuade decisionmakers, put forward some general tips on advocacy at different levels, and showcase some recent examples of effective encryption-related engagement from civil society.

KEY MESSAGES FOR ENCRYPTION ADVOCATES

In advocacy, success often depends on finding the right argument to your audience – whether that's a state, a business or a regulator. The ultimate goal is to ensure that the standards, laws and policies on encryption that are being developed in different forums respect, and are consistent with, human rights. In some forums, talking about human rights will be an effective line of argument.

In other forums, other messages may carry more weight or be more persuasive. Below are some different angles on encryption that human rights defenders might want to try out.

Message 1: Encryption is essential to the protection of human rights

Unlike concepts of privacy and freedom of expression, encryption in and of itself doesn't have a traditional place in the human rights conversation. However, as we saw in chapter 3, encryption is essential in order to ensure the protection and enjoyment of a number of human rights, including the rights to privacy and to freedom of expression. The importance of encryption to these rights is set out in more detail in chapter 3.

Message 2: Encrypted devices are less likely to be stolen

As a key component of cybersecurity, encryption helps protect people against a number of crimes, including data breaches and other forms of unauthorised access to personal information. However, encryption can also protect against other crimes, such as device theft. Kevin Bankston, the Director of New America's Open Technology Institute, has argued that if all smartphones used encryption by default, this would act as a serious deterrent to the theft of smartphones (and the violence that often accompanies it), as smartphone thieves increasingly go after the data on stolen phones in addition to (or instead of) solely trying to profit from sale of the hardware itself. If the data is encrypted and the smartphone password-protected, it would be virtually impossible for the thief to access the data.

Open Rights Group and the UK's Investigatory Powers Act 2016

Open Rights Group (ORG) is a digital campaigning organisation in the United Kingdom, focusing on the rights to privacy and freedom of expression online. As well as its public awareness-raising activities around these rights, it has been seeking to influence decision-makers in relation to the Investigatory Powers Act 2016, a piece of legislation which, among other things, could allow the UK government to weaken encryption standards.

In March 2017, ORG published a set of simple messages on the importance of encryption to human rights, the economy and cybersecurity, explaining in plain English the arguments in favour of strong encryption. A few months later, it followed this up by publicly revealing that the government was secretly consulting on the scope of a set of planned regulations which would enable the Home Secretary to impose 'technical capability notices'. These notices could lead to companies being forced to weaken the security of their products (including by weakening their encryption standards), so that intelligence and law enforcement agencies could more easily obtain communications and data.

At the same time, ORG launched an email campaign calling on its members, supporters, and members of the public to lobby the Home Office not to weaken encryption standards.

Message 3: Strong encryption supports strong local economies

One of the great benefits of the internet is that it is a truly global medium. This means that, subject to a few exceptions, internet-based companies tend to compete globally to attract users and gain market share. For example, a tech company based in Brazil may compete with similar companies in India, France, and Kenya to serve the same global user base. If Brazil's government were to suddenly restrict strong forms of encryption, that business might become less appealing to customers and potential customers, and may suffer criminal hacks and data breaches, which could trigger expensive notices to impacted users and other mitigation expenses. In the US, the Federal Trade Commission has even levied fines against companies for failure to implement appropriate data security practices.

Aside from the avoidance of fines, businesses who build in strong encryption might also find that they gain a competitive edge over rivals. By this measure, laws and policies that not only allow but incentivise the use of strong encryption will allow companies to provide the features that entice users.

Message 4: Restrictions on encryption hurt ordinary people – not terrorists or criminals

As we saw in chapter 2, arguments in favour of limits on encryption usually invoke the need for law and order. Restrictions are needed, these arguments go, so that the state can catch terrorists and criminals.

The problem is that there's no evidence that limitations on encryption will do anything to stop these actors. Actors seeking to plot or scheme using encrypted technologies will always find ways to circumvent restrictions — whether by creating their own ultra-strong encryption tools using open source technologies, or by seeking out encryption tools developed by companies outside the jurisdiction of the country which is imposing the restrictions.

In fact, the real victim of restrictions on encryption is always the general population, and especially the most disadvantaged people within it, who likely rely on cheap or free encryption services (now compromised), and lack the technical knowledge and money to procure alternatives.

Message 5: Limitations on strong encryption are market barriers

Another consequence of the global nature of the internet is that companies often operate across many jurisdictions with different legal requirements. This often means that companies have to possess significant knowledge about compliance in different countries to ensure that they are not inadvertently breaking any laws.

This means that, as a company offering a service which relies on encryption, you essentially face three choices:

- Create different products to be sold or distributed, to the extent possible, in jurisdictions with different rules;
- Create a single product that incorporates each of the different mandated limitations on encryption and use that across all markets; or
- Ignore the different requirements and put out a single product for all jurisdictions and hope that officials in the countries where limitations exist don't notice.

This list of choices demonstrates how encryption restrictions preference the status quo of large companies but can harm the overall economy. While large companies may be able to afford the first option and continue creating products that are at least as secure as legally

possible, the expense of creating, distributing, and maintaining several different versions of a single product may be prohibitively expensive for small or emerging companies. These companies instead face a choice between the second or third options, neither of which is scalable or sustainable.

Unfortunately, the second option all but guarantees that the offered device or service will be considerably more vulnerable than its counterparts, will face more data breaches, and will be less appealing to users. On the other hand, the third option may work well for a period of time — even a long period of time — but if and when the law catches up, the results may be disastrous. In China, for instance, the potential monetary penalty for a serious violation of its limitation on encryption has no upper limit, meaning companies could face fines large enough to send them into bankruptcy. Consequently, encryption bans act as a market barrier to new, innovative companies, ultimately harming users.

UN Special Rapporteur report on encryption

In March 2015, the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, issued a call for submissions for a report he was preparing on encryption, anonymity and the human rights framework. The call was open to civil society organisations (as well as governments) and requested information on encryption-related laws and policies in different countries and their impacts on human rights. Civil society organisations from a range of countries were able to feed into the report, providing examples of good and bad practice (such as legislation which enabled encryption or restricted it) and the consequences of this in practice. These examples were then highlighted in his report and influenced his conclusions on what a human rights-respecting legal framework for encryption should look like.

Message 6: Restrictions on encryption are a threat to cybersecurity

Digital products and services are inherently insecure. Even companies with large, well-resourced teams of expert developers and technologists send products to the market that are rife with vulnerabilities. Numerous government agencies around the world, including the US Department of Defense, consistently identify cybersecurity as a top concern. The WannaCry ransomware attack in 2017, for example, targeted computer systems in over 150 countries, causing harm to businesses and public bodies alike, encrypting data on their computers and demanding ransom payments in the Bitcoin cryptocurrency for it to be decrypted. In 2016, a single product, Google's Android OS, was found to have more than 500 vulnerabilities.

In spite of this, tech companies around the world are still facing pressure from governments to weaken or compromise the encryption technologies they use. If these companies comply, it means they are, in effect, deliberately making their products and services – which, in some cases, store the sensitive personal information of hundreds of millions of users – more vulnerable, more unstable, and more prone to intrusion.

Such measures don't just threaten the rights and security of individual users – they also diminish the security of cyberspace in a more general sense. And if a government really cares about cybersecurity, it should, logically, oppose them.

TIPS ON ADVOCACY AND ENGAGING AT DIFFERENT LEVELS

Advocacy on encryption happens at a number of levels, with strategies targeting the grassroots (i.e. the general public), the grass tops (i.e. the ultimate decisionmakers) and everyone in between. Groups should choose an advocacy strategy that best utilises their strengths and respects their audience.

Grassroots

People are at the heart of conversations about encryption. People, after all, aren't just the users of encryption products – they are also the beneficiaries, indirectly or directly, of wider developments and applications of encryption, whether by companies and governments.

They're also a key constituency for advocacy. In countries with representative democracies, individual voters carry the most weight with the decisionmakers who will ultimately develop and implement laws and policies that either encourage or restrict encryption.

While it is good to focus direct advocacy on these decisionmakers, and provide expert advice and testimony, there is also value in presenting the personal stories of people in their countries. How are people using encryption in a given country? What do they want from their policymakers? In this sense, advocacy organisations can serve as a powerful intermediary.

"Secure the Internet"

On January 12, 2016, Access Now launched securetheinternet.org. The website contained the text of a letter in support of encryption, referencing the rights-based, technical, and economic arguments in its favour. The website specifically and emphatically highlighted five things that governments should not do in order to limit the development of encryption or interfere with its use:

- Governments should not ban or otherwise limit user access to encryption in any form or otherwise prohibit the implementation or use of encryption by grade or type;
- Governments should not mandate the design or implementation of 'backdoors' or vulnerabilities into tools, technologies, or services;
- Governments should not require that tools, technologies, or services are designed or developed to allow for third-party access to unencrypted data or encryption keys;

- Governments should not seek to weaken or undermine encryption standards or intentionally influence the establishment of encryption standards except to promote a higher level of information security. No government should mandate insecure encryption algorithms, standards, tools, or technologies; and
- Governments should not, either by private or public agreement, compel or pressure an entity to engage in activity that is inconsistent with the above tenets.

The letter and website are available in fifteen different languages. The letter – which came to attract over 300 signatories from organisations, businesses, and prominent individuals and experts in over 50 countries – was sent to governments around the world. It also served as a crucial resource and tool for local civil society organisations advocating on encryption, giving them a louder voice than they would have otherwise had, and removing the necessity of 'reinventing the wheel' every time a government put forward a new proposal.

Building support for – and usage of – stronger encryption among a general population is also a hugely valuable activity. It increases the market demand for even more encryption, creating a positive reinforcement loop that incentivises companies to adopt encryption or expand its use, which then provides greater protections for users.

Grass tops and direct advocacy

Decisionmakers and policymakers, both in elected and appointed positions (as well as those with direct connections to those individuals), benefit from hearing from organisations and well-informed individuals on the subjects within their mandates. Leaders and influencers will certainly have heard from law enforcement agencies and those representing their interests, as

well as those in the national security community, so advocates should be prepared not only to present facts and information about the benefits of encryption and how it is used, but also should be educated about common myths and misinformation regarding encryption.

These decisionmakers should be approached with a clear idea of desired steps and a clear sense of what is possible for them to do. While some decisionmakers will be happy leading the charge on legislation or regulation about encryption, others may be more comfortable in a supporting role, and still others will want to stay informed but may remain inactive unless necessary. Having a clear ask in mind, and providing space for different levels of commitment, will help ensure that leaders have a comfortable place to sit on the issue.

In addition, grass top advocates should engage honestly, recognising the arguments on the other side. For example, law enforcement agencies may face legitimate hurdles due to encryption that they would not have otherwise faced. Not acknowledging that will open the door to greater challenge and pushback. Instead, advocates should recognise that there are points to be made on the other side, while communicating clearly the case for strong, available and accessible encryption.

Coalition engagement

Advocacy is rarely a solo effort, and advocacy around encryption is no exception. On the topic of encryption, partnerships can be particularly powerful and should be used strategically. Non-profit organisations, academics, technical and legal experts, and both large and small businesses, all have stood together in favour of measures to protect encryption. While these groups are not all natural bedfellows, they can and should join together to amplify one another's voices.

GLOSSARY

Asymmetric encryption: encryption using asymmetric keys, i.e. a different key to encrypt and decrypt the communication or data.

Brute force attack: an attempt to decrypt encrypted communications or data by trying all possible key combinations.

Cipher: an algorithm, process, or method for encryption or decryption.

Ciphertext: communications or data while it is encrypted and unreadable.

Cryptography: the study and practice of techniques for secure communication.

Data at rest: data while it is not being used, for example while it is on a storage device such as a computer, a laptop or a mobile phone.

Data in process (or data in use): data while it is being viewed, processed or manipulated, for example, data on a storage device while it is being accessed, or, in the case of communications, being written or edited.

Data in transit: data while it is being sent over data networks.

Decryption: the means by which encrypted communications are decoded so that they can be read and understood.

Digital signature: a mechanism by which the recipient of a communication or data can be sure that it was sent by a particular person. It usually involves decrypting communications or data successfully with a public key when the sender used their private key to encrypt it. If the decryption is successful, then the recipient can be sure that it was encrypted with the sender's private key, which only the sender knows, thus authenticating that it was he or she that sent the communication or data.

End-to-end encryption: the continual encryption of data throughout its journey, with no point at which it is unencrypted.

Encryption: the means of encoding communications (or information or data) so that they cannot be read by anyone other than the intended recipient.

Key: a parameter, usually a string of binary bits of a fixed length, which is used as part of the algorithm (cipher) to encrypt or decrypt communication or data. The addition of the key in encryption and decryption means that communications and data cannot be decrypted by knowledge of the algorithm alone.

Key length: the length of the string of binary bits in a key. The longer the key length, the stronger the encryption.

Key space: the total number of possible combinations of ones and zeros given the key length. The longer the key length, the greater the key spaces, and therefore the stronger the encryption.

Plaintext: communication or data in its original, readable form.

Private key: a key which is known only to the person encrypting or decrypting communications or data, rather than everyone in the process. It is commonly used in asymmetric encryption, with the public key publicly available.

Public key: a key which is publicly available or known to people other than the person who encrypts the communication or data. It is commonly used in asymmetric encryption, with the private key known only to the second party.

Symmetric encryption: encryption using symmetric keys, i.e. the same key to encrypt and decrypt the communication or data.

ACKNOWLEDGEMENTS

This guide was produced by Global Partners Digital with input from Amie Stepanovich, Gustaf Björksten and Richard Wingfield. Comments and feedback on were gratefully received from Carly Nyst and Gisela Perez de Acha.

Produced by The Kitchen agency
Designed by Miriam Hempel | Illustrations by Valentina Cavallini

GLOBAL PARTNERS DIGITAL

Everyone who uses the internet depends on encryption. It makes online banking and shopping possible, allows us to communicate securely, and facilitates the exercise of many human rights.

Despite these obvious benefits, encryption has always had its opponents – and they are becoming more active. In legislatures and policymaking forums around the world, attempts are being made, often under the guise of fighting crime or terrorism, to weaken, compromise or restrict access to encryption. This is a threat to the security and rights of everyone, and it must be resisted.

That's where this guide comes in. Designed specifically for human rights defenders, it offers a comprehensive and accessible introduction to the world of encryption policy – explaining the technology behind encryption, the key debates, why it relates to human rights, and where – and how – you can engage.

Encryption Policy for Human Rights Defenders is the fourth entry in the Travel Guide to the Digital World series. Find the rest of the series on www.gp-digital.org

ISBN 978-0-9929147-2-1