ENCRYPTION

A MATTER OF HUMAN RIGHTS

AMNESTY INTERNATIONAL

CONTENTS

Executive summary 3

1. What is encryption? 6

Other relevant definitions 8

2. Encryption and human rights 10

Protecting the rights to privacy and freedom of expression in the digital age 13

3. Fear of "going dark": governments' efforts to weaken encryption 18

How encryption restricts governments access to data 21

Full-disk or device encryption 21

End-to-end encryption 22

Transport Encryption 23

4. Restrictions on encryption and their technical and practical feasibility 25

General measures banning or restricting encryption 25

Requiring companies to backdoor encryption 26

Mandatory disclosure of encryption keys 28

Targeted decryption orders 29

5. There can be no backdoors on rights 31

Technology companies' responsibility to respect human rights 32

Annex: Amnesty International policy on encryption 34

EXECUTIVE SUMMARY

Today, more than three billion people across the world have access to the internet. Businesses, hospitals and government agencies store our information in databases and computers connected to the internet. Devices we use every day – smartphones and computers but also increasingly cars, watches and televisions – store and transmit personal information.

This vast amount of personal data, from emails and messages, to the websites we visit, to our credit card information and health records, can all be prey to theft and spying, be it from criminals trying to steal or extort money, or governments spying on their populations.

Encryption is an essential mean of protecting our personal information. While there are different kinds of encryption, they all aim to achieve the same thing: to ensure that information can only be accessed by its owner or its intended recipient. For example, if applied to emails, encryption ensures that only the sender and the recipient can read the email; if someone is intercepting your internet connection, they will only see scrambled information.

States have obligations under international law to respect, protect and fulfil the right to privacy of their populations. In the digital age, these obligations mean that states should ensure the security of online communications, including by raising awareness of internet security issues, encouraging the identification and repair of security weaknesses in computer networks and systems, and facilitating the use of encryption tools and services.

The threats to our private data are real, and growing. Millions of people across the world have their data stolen as a result of the theft or loss of smartphones and computers, as well as large data breaches of companies and government agencies. Such data thefts are a threat to security and privacy.

At the same time, governments are increasingly threatening and violating our right to privacy through unjustified surveillance. We have learned since 2013 the vast extent of the mass surveillance programmes operated by intelligence agencies in the USA and the UK. For years, these programmes have operated in the shadows and spied on the telephone and internet communications of hundreds of millions of people around the globe.

In addition, technology for targeted electronic surveillance has become widely available and affordable. In recent years evidence has surfaced of surveillance technology being used against human rights defenders in countries such as Bahrain and Ethiopia. In 2015, countries including Pakistan, France, Poland, Switzerland and the UK have passed laws or introduced bills which aim at increasing the scope of electronic surveillance and give governments intrusive powers to spy on electronic communications.

In the digital age, access to and use of encryption is an enabler of the right to privacy. Because encryption can protect communications from spying, it can help people share their opinion with others without reprisals, access information on the web and organize with others against injustice. Encryption is therefore also an enabler of the rights to freedom of

expression, information and opinion, and also has an impact on the rights to freedom of peaceful assembly, association and other human rights. Encryption is a particularly critical tool for human rights defenders, activists and journalists, all of whom rely on it with increasing frequency to protect their security and that of others against unlawful surveillance.

However, many governments are critical of encryption and have put in place legal measures to prevent or restrict the ability of individuals to use encryption. Countries such as Pakistan, India and Cuba ban encryption, restrict the strength of lawful encryption or require individuals to seek authorization to use encryption. Government officials, including in France, the UK and the USA, have criticized encryption over fears that it will lead to intelligence "going dark", i.e. that parts of online communications cannot be accessed by law enforcement or intelligence agencies.

It is a fact that strong encryption can pose challenges to accessing information for legitimate law enforcement purposes. Governments have an obligation to protect their populations from crime, including terrorism, and electronic surveillance can be legitimately used for this purpose, if undertaken within the bounds of international law.

However, in attempting to overcome the barriers that encryption poses to them, state authorities must not violate the rights to privacy and freedom of expression, or any other rights for which the security of electronic data and communications is vital.

Amnesty International believes that, because of the critical role played by encryption in the enjoyment of these rights, restrictions on access to and use of encryption may constitute an interference with the enjoyment of human rights. As such, in order to avoid violating their human rights obligations, states must ensure that any restrictions on encryption are contained in laws that are precise and transparent, are used only when necessary to achieve a legitimate aim and do not discriminate against specific individuals or groups.

Critically, any interference with encryption must be proportionate to achieving the legitimate aim for which it is imposed, and the benefits gained must not be outweighed by the harm caused, including to individuals and network infrastructure and security.

Government officials in countries such as the USA and France are concerned about two types of encryption technologies: end-to-end encryption and full-disk or device encryption. End-to-end encryption is a technology that ensures the content of communications (emails, messages, voice and video calls) can be seen only by the parties to the communications; even the company providing the service cannot decipher the communication. In practice, this means that if a government agency makes a request for the service provider to hand over the content of the communication, they cannot comply with that request.

Device encryption is at the centre of the current Apple v FBI dispute. This type of encryption, deployed by default in some modern smartphones, means that all the data on the device is encrypted and unreadable without the correct passcode or PIN number. Even if authorities have an encrypted phone in their possession, they cannot access the information in an intelligible form without having the correct codes.

In the Apple v FBI case, if the company were to be compelled to modify its software to

unlock the phone in question, it would set a precedent that could allow the US government – and potentially other governments – to compel technology companies to weaken or otherwise circumvent their encryption by providing a ´backdoor´ to intelligence and other security agencies.

Forcing companies to provide 'backdoors' to the encryption deployed in their products or services (potentially affecting all users) constitutes a significant interference with users' rights to privacy and freedom of expression. Given that such measures indiscriminately affect all users' online privacy by undermining the security of their electronic communications and private data, Amnesty International believes they are inherently disproportionate, and thus impermissible under international human rights law

Encryption is an enabler of human rights. It provides, as the UN Special Rapporteur on Freedom of Expression stated, "individuals and groups with a zone of privacy online to hold opinions and exercise freedom of expression without arbitrary and unlawful interference or attacks".

With an ever-increasing amount of our personal information stored on internet-connected devices and transmitted across the network, governments in many countries are violating our right to privacy through unjustified surveillance. Encryption is a technology that allows us to protect ourselves, as much from violations of our right to privacy by governments as from criminals trying to steal our identity. Governments that prohibit the use of encryption or try to weaken encryption technology, are in effect preventing people from using the best available technology to protect their data and their communications. This is inherently disproportionate.

Amnesty International is calling on governments to ensure that any interference with encryption is necessary, proportionate and does not result in weakening the security of electronic communications and data for everyone. The organization is also calling on companies to incorporate an adequate level of encryption into their products and services.

1. WHAT IS ENCRYPTION?

Encryption is a technical term used to describe the manner by which communications – text messages, emails, phone calls and video chats – are secured against access by anyone who is not the intended recipient. The act of encryption is the mathematical manipulation of information to render it readable solely by the person or persons intended to receive it. Although encryption existed long before the internet – one of the earliest forms of encryption was the Caesar Cipher, developed by Julius Caesar to secure the written notes carried by messengers – the advent of digital technologies and the internet has moved encryption from the sole preserve of cryptographers, to being a concern for every internet user.

Most of us encounter one of three different types of encryption in our daily internet usage:

- **Full-disk or device encryption** is the process by which all of the information stored in our computers or smartphones is encrypted when residing on the device. If you use certain new smartphones or computers running the latest, updated operating system, device encryption will be turned on by default,[1] meaning you might be using it without even knowing about it. In other devices you need to follow a set of specified steps in order to turn on device encryption. With device encryption, the data on your device will generally not be readable or anyone who does not possess your personal identification number (PIN) or password.

- **End-to-end encryption** ensures that the communications sent between a sender and recipient cannot be decrypted or read by any intermediate actor or service provider. When end-to-end encryption is deployed, any intermediate device or service provider with access to your electronic communications, or any entity attempting to intercept the communications, is unable to read their contents. For example, at present, anyone who intercepts end-to-end encrypted iMessages and Signal[2] messages, among others, cannot read them. Another popular messaging service that uses end-to-end encryption, but only in particular cases, is WhatsApp.[3] In addition to being available users of those secure messaging applications, end-to-end encryption can also be used to secure emails, primarily through the use of an encryption technology called PGP.[4] PGP, iMessage and Signal deploy a form of encryption

[1] See for example Android 6.0 re-implements mandatory storage encryption for new devices, Ars Technica, online at:

http://arstechnica.com/gadgets/2015/10/android-6-0-re-implements-mandatory-device-encryption-for-new-devices/ and How to: Encrypt you iPhone, the Electronic Frontier Foundation, online at: https://ssd.eff.org/en/module/how-encrypt-your-iphone

[2] Signal Private Messenger is a free and open source software application for Android phones and iPhones that uses end-to-end encryption.

[3] Open Whisper Systems, the developer of Signal has partnered with WhatsApp to deploy end-to-end encryption in WhatsApp. However, it only works on some kinds of messages. See https://whispersystems.org/blog/whatsapp/

[4] For more information on PGP, see https://en.wikipedia.org/wiki/Pretty_Good_Privacy and the website of

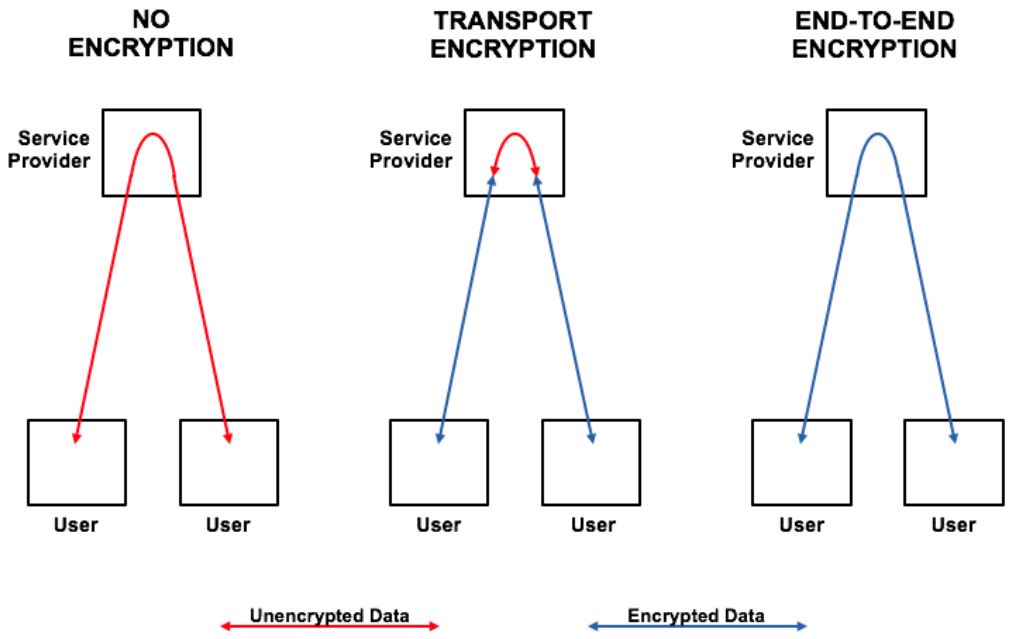
called public key cryptography, a scheme that uses a pair of keys (mathematical values that use algorithms to encrypt or decrypt data) for encryption: a public key, which encrypts data, and a corresponding private key for decryption. An individual's public key is available to the world while their private key is kept secret within their device. Anyone who has a user's public key can then encrypt information that only the recipient can read.

- **Transport encryption or transport layer encryption (the most common of which includes HTTPS[5] using TLS or SSL[6])** is the means by which the communications between the websites you access (such as Google search, online shops like Amazon.com, your bank or financial institution, or a webmail service like Outlook) and your browser are encrypted. That is, when you enter a username and password in a login page, or type a query in a search engine, that information has to be transmitted to the company's servers, which are often physically located in a different country or continent. When websites use HTTPS, it ensures that, even if data is intercepted by an unauthorised party while transiting the internet, it is more secure against being read than if you were using an unencrypted connection (over plain HTTP). However, when that data arrives at its destination and becomes the possession of the website operator, it is decrypted and stored in an unencrypted format.

Phil Zimmermann, the creator of PGP, at https://www.philzimmermann.com/EN/essays/index.html

[5] "Hyper Text Transfer Protocol Secure (HTTPS) is the secure version of HTTP, the protocol over which data is sent between your browser and the website that you are connected to. The 'S' at the end of HTTPS stands for 'Secure'. It means all communications between your browser and the website are encrypted." Source: https://www.instantssl.com/ssl-certificate-products/https.html

[6] TLS stands for Transport Layer Security and SSL stands for Secure Sockets Layer. See https://www.instantssl.com/ssl-certificate-products/https.html



Essentially, encryption ensures that only the intended recipient is able to read, listen to or watch the communication that was transmitted to them. Encryption thus protects the privacy and security of the content of communications transmitted through those tools and services that use encryption.

It is important to distinguish between the privacy and security that encryption provides, and the complementary but separate condition of anonymity, which refers to successfully concealing one's identity. Encrypted communications are not anonymous communications; and achieving anonymous communications requires a difficult combination of technology and practice. Even where individuals take steps to obscure information that can identify them, such as their name and Internet Protocol (IP) addresses,[7] including by using pseudonyms or anonymizing software such as Tor,[8] the metadata generated by our use of digital technologies, such as the pattern of our locations tracked and transmitted by our mobile phones, may reveal our identities.

OTHER RELEVANT DEFINITIONS

Backdoors or "backdooring": an informal term used to refer to technical measures that weaken or undermine encryption tools, devices and services in order to facilitate access to information and communications by actors other than the service provider, and parties to, the

[7] IP addresses are numerical labels assigned to devices connected to the internet. For more information see https://en.wikipedia.org/wiki/IP_address

[8] For more information on Tor, see https://www.torproject.org/

information or communications.

Hacking: the use of vulnerabilities (flaws in computer software),[9] malware (malicious software such as viruses, worms and spyware)[10] and social engineering[11] to gain access to a device, system or network; it will often be deployed in order to circumvent encryption and enable an unauthorized party to access the unencrypted form of the data that exists on a computer or smartphone.

Metadata: refers to all information that is generated through the use of communications technology other than the actual content of the communication. While the information does not necessarily contain personal or content details, it contains information about the devices being used, the users of the devices, and the manner in which they are being used (it is also called "communications data" or "data about data", such as email recipients, call times and location records, and in the case of mobile telephones, the cell towers being used). If cross-referenced with other sources of data, an analysis of metadata can produce an accurate picture of the associations and habits of the participants to a communication.

[9] For more information on vulnerabilities see https://en.wikipedia.org/wiki/Vulnerability_(computing)

[10] For more information on malware, see https://en.wikipedia.org/wiki/Malware

[11] Social engineering in the context of information security can be defined as the psychological manipulation of people into performing actions or divulging confidential information; see https://en.wikipedia.org/wiki/Social_engineering_(security)

2. ENCRYPTION AND HUMAN RIGHTS

"Encryption tools are widely used around the world, including by human rights defenders, civil society, journalists, whistle-blowers and political dissidents facing persecution and harassment… Encryption and anonymity are needed as enablers of both freedom of expression and opinion, and the right to privacy. It is neither fanciful nor an exaggeration to say that, without encryption tools, lives may be endangered. In the worst cases, a Government's ability to break into its citizens' phones may lead to the persecution of individuals who are simply exercising their fundamental human rights."
Zeid Ra'ad Al Hussein, UN High Commissioner for Human Rights[12]

Encryption is what makes our data and communications safe online. When encryption is used, the internet can be a vehicle to which we entrust our most intimate thoughts, our medical questions, our bank details, our sexuality, and our religious beliefs. The increasing ubiquity of encryption on the internet has come about through an evolutionary process in which repeated large data breaches, hacked websites, and identity and credit card theft have been inevitably superseded by measures to extend and strengthen encryption. This evolution has been accelerated in recent years as it has become clear that the security and privacy of communications is under threat not only from online criminals and identity thieves, but from governments as well.

In the USA, there were an estimated 17.6 million victims of identity theft in 2014.[13] According to UK police data, more than 100,000 mobile phones were stolen in London alone in 2013, and of the hundreds of thousands of phones stolen in the city between 2012 and 2014, the majority were smartphones.[14] Crucially, in addition to financial loss, the theft of a smartphone also means the theft of private communications and information about the owner; this can include medical, financial and professional information.

Whereas the adoption of digital communications has revolutionized work, education, politics, relationships, culture and language across the globe, it has also dramatically lowered the barriers to, and created new opportunities for, state surveillance. What were previously

---

[12] Office of the UNH High Commissioner for Human Rights, Apple-FBI case could have serious global ramifications for human rights: Zeid, 4 March 2016, online at: http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=17138#sthash.o25R7Bqg.dpuf

[13] U.S. Department of Justice, Victims of Identity Theft, 2014, online at: http://www.bjs.gov/content/pub/pdf/vit14.pdf

[14] UK Home Office, Reducing Mobile Phone Theft and Improving Security, September 2014, online at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/390901/HO_Mobile_theft_paper_Dec_14_WEB.PDF

laborious, time and cost-intensive activities for the state to conduct – intercepting written communications, wire-tapping phone calls, tracking suspected dissidents' reading habits, monitoring the location of persons of interest – are now easily achievable through the deployment of inexpensive electronic surveillance technologies that can conduct analyses at a speed and volume that far outpaces the capacity of traditional law enforcement or intelligence services.

THE SNOWDEN REVELATIONS

On 5 June 2013, a British newspaper, *The Guardian*, published the first in a series of revelations about indiscriminate mass surveillance by the USA's National Security Agency (NSA) and the UK's Government Communications Headquarters (GCHQ). Edward Snowden, a whistleblower who had worked with the NSA, provided concrete evidence of global communications surveillance programmes that monitor the internet and phone activity of hundreds of millions of people across the world. The revelations, which have been exposed by the media based on files leaked by Edward Snowden have included evidence that:

- Companies – including Facebook, Google and Microsoft – faced legal orders to hand over their customers' data to the NSA under secret orders through the NSA's Prism programme;

- An NSA program started in 2009 allowed the agency to record, store and analyse metadata related to every single telephone call and text message transmitted in several countries, including Mexico, Kenya, and the Philippines;

- GCHQ and the NSA have co-opted some of the world's largest telecommunications companies to tap the transatlantic undersea cables and intercept the private communications they carry, under their respective TEMPORA and Upstream programmes;

- In 2010-11, GCHQ and NSA hacked into the internal computer network of Gemalto, the largest manufacturer of SIM cards in the world, possibly stealing billions of encryption keys used to protect the privacy of mobile phone communications around the world.

Were it not for encryption, states' reach into the internet could be total. Even with encryption states are still in a position to intercept communications *en masse*.

In addition to mass surveillance carried out by countries like the UK and the USA, the targeted surveillance of activist and journalists is unfortunately commonplace in countries around the world. In the UK, police have put newspaper journalists under surveillance in order to identify their sources,[15] while Bahraini activists in exile abroad have been tracked by their government using spyware,[16] and Colombian radio journalists have been subjected to

[15] Dominic Ponsford, "Surveillance court says Met grabs of Sun reports' call records 'not compatible' with human rights law," 17 December 2015, available at http://www.pressgazette.co.uk/surveillance-court-says-met-was-right-grab-sun-journalists-call-records-hunt-plebgate-sources.

[16] Amar Toor & Russell Brandom, A spy in the machine: How a brutal government used cutting-edge spyware to hijack one activist's life, online at: http://www.theverge.com/2015/1/21/7861645/finfisher-spyware-let-bahrain-government-hack-political-activist

electronic surveillance by the national police.[17] The Ethiopian government uses electronic surveillance to spy on opposition activists not only in Ethiopia, but abroad.[18]

It is only by securing communications against outside interference that ordinary internet users, human rights defenders, opposition politicians, political activists, and investigative journalists can protect themselves from cybercrime as well as from the prying eye of governments all around the world.

However, a number of governments around the world have already enacted legislation dramatically restricting access to and use of encryption tools and services. Countries such as Pakistan, India and Cuba either ban encryption,[19] restrict the strength of lawful encryption to levels set by the government,[20] or require individuals to seek regulatory authorization for their use of encryption.[21] Turkey requires encryption suppliers to provide copies of encryption keys to government regulators before offering their encryption tools to users, while the UK, France and Spain can require companies to disclose encryption keys and decrypt data.[22] China passed a Counter-Terrorism Law in December 2015 which requires telecommunications providers to "provide technical support and assistance to government investigators by, among other things, providing access to technical interfaces and decryption keys to law enforcement authorities and national security authorities to support terrorism prevention and investigation activities" (Article 18) and "implement network security, information content-monitoring systems and measures designed to prevent the dissemination of content containing terrorism and extremism, to delete such information, and to immediately report to the Chinese police"

---

[17] Committee to Protect Journalists, Claims police spied on two journalists revive surveillance fears of Colombia's press, online at: https://www.cpj.org/blog/2016/02/claims-police-spied-on-two-journalists-revive-surv.php and Committee to Protect Journalists, In the Americas, Big Brother is watching reporters, online at: https://www.cpj.org/2010/02/in-the-americas-big-brother.php

[18] Human Rights Watch, *Ethiopia: Telecom Surveillance Chills Rights*, 25 March 2014, online at: https://www.hrw.org/news/2014/03/25/ethiopia-telecom-surveillance-chills-rights

[19] Bytes for All, "Pakistan: Ban on Internet encryption a violation of freedom of expression," 9 February 2011, available at https://content.bytesforall.pk/node/40.

[20] Indian ISPs must restrict the level of encryption for individuals, groups or organizations to a key length of only 40 bits in symmetric key algorithms or equivalents. See "Digital Encryption in India," *Indian Case laws,* 10 February 2015, available at https://indiancaselaws.wordpress.com/2015/02/10/digital-encryption-laws-in-india/

[21] Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye*, A/HRC/29/32, 22 May 2015, para. 41, online at http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/Pages/ListReports.aspx

[22] United Kingdom, Regulation of Investigatory Powers Act http://www.legislation.gov.uk/ukpga/2000/23/pdfs/ukpga_20000023_en.pdf (mandatory key disclosure); France, Law No. 2001-1062 (disclosure of encryption keys on authorization by a judge); Spain, Law on Telecommunications 25/2007 (key disclosure).

(Article 19).[23]

PROTECTING THE RIGHTS TO PRIVACY AND FREEDOM OF EXPRESSION IN THE DIGITAL AGE

The two human rights most commonly associated with access to, and use of, encryption are the rights to privacy[24] and the right to freedom of expression.[25] Access to encryption, or the lack thereof, may also have an impact on other rights such as the right to peaceful assembly and association. The rights to privacy and freedom of expression are often understood as mutually reinforcing rights. When people have a secure space to seek information, expand their knowledge, develop opinions, and express ideas, the right to privacy acts as an enabler to the exercise of the right to freedom of expression. The confidence to communicate our ideas and opinions – however controversial – is underpinned by the knowledge that we are protected from any unlawful interference with those communications.

The concept of privacy and the protections offered by Article 17 (on the right to privacy) of the International Covenant on Civil and Political Rights (ICCPR) extend to issues far beyond communications and the internet. However, with the advances of modern technology, privacy rights are newly resonant with individuals, and newly meaningful for states, and have enjoyed far more attention by courts and legislatures in the past decade than in the preceding fifty years.[26] With new opportunities for expression provided by the internet, have come new and unique interferences with individuals' privacy.

While digital technologies have created new opportunities for communication and expression, they have also enabled the production, dissemination and storage of exponentially greater amounts of private data pertaining to individuals' movements, beliefs, political preferences,

---

[23] "China enacts broad counter-terrorism law," *Global Policy Watch – Covington,* 5 January 2016, available at https://www.globalpolicywatch.com/2016/01/china-enacts-broad-counter-terrorism-law/.

[24] The right to privacy, enshrined in Article 12 of the Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights, encompasses the right to be free from unlawful or arbitrary interference with one's privacy, family, home or correspondence, and from unlawful attacks on one's reputation, and the right to enjoy the protection of the law against such interference or attacks. The right to privacy is also enshrined in the Convention on the Rights of the Child (Article 16), and the International Convention on the Protection of All Migrant Workers and Members of Their Families (Article 14). At the regional level, the right to privacy is protected by the European Convention on Human Rights (Article 8), the European Union Charter of Fundamental Rights (Article 7) and the American Convention on Human Rights (Article 11). Privacy has evolved to encompass a right to protection of personal data, as specifically recognised in Article 8 of the EU Charter and Article 21 of the ASEAN Human Rights Declaration.

[25] The right to freedom of expression is protected by Article 19 of the Universal Declaration on Human Rights; Article 19 of the ICCPR; Article 10 of the ECHR; Article 11 of the European Union Charter of Fundamental Rights, and Article 13 of the American Convention on Human Rights 1969.

[26] For examples of recent pronouncements on the right to privacy, see Amnesty International and Privacy International, Two Years After Snowden: Protecting human rights in an age of mass surveillance, June 2015, pp8-9, online at: https://www.amnesty.org/en/documents/act30/1795/2015/en/

sexual orientation, health, and financial flows, among others.

In 2012, the United Nations (UN) Special Rapporteur on the situation of human rights defenders published a report on freedom of expression on the internet, noting that:

"Over the past decade, the Internet has become an indispensable tool for the work of many human rights defenders, especially as a means of imparting views, sharing information about human rights and human rights violations and connecting with other human rights defenders [...] The Special Rapporteur is [...] concerned that personal information about human rights defenders obtained through social networking and other websites might compromise their security, especially in the light of new legislative developments authorizing Governments to widely monitor websites in several countries."[27]

In 2013, the Special Rapporteur on freedom of expression published a report on state surveillance of communications and privacy. In that report, the Special Rapporteur concluded that security of communications was an essential component of the right to privacy, which is undermined by laws inhibiting the use of privacy-enhancing tools like encryption.[28]

Following the Snowden revelations, a series of other UN reports, resolutions and decisions dealt with the issue of state surveillance of communications "in the digital age". These included a report by the High Commissioner for Human Rights on *The right to privacy in the digital age*, two General Assembly resolutions, a Human Rights Council resolution establishing a new special procedures mandate dedicated to the right to privacy, and Concluding Observations by the Human Rights Committee in its reviews of the USA,[29] the UK,[30] and France[31] which addressed the use of particular digital surveillance techniques. Most recently, the current Special Rapporteur on freedom of expression published a report in

---

[27] UN General Assembly, Situation of human rights defenders, 10 August 2012, para. 61-62, online at: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N12/459/42/PDF/N1245942.pdf?OpenElement

[28] Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue*, 17 April 2013, A/HRC/23/40, para. 71, online at: http://daccess-dds-ny.un.org/doc/UNDOC/GEN/G13/133/03/PDF/G1313303.pdf?OpenElement

[29] Human Rights Committee, *Concluding observations on the fourth periodic report of the United States of America*, 23 April 2014, online at: http://tbinternet.ohchr.org/_layouts/treatybodyexternal/Download.aspx?symbolno=CCPR%2fC%2fUSA%2fCO%2f4&Lang=en

[30] Human Rights Committee, *Concluding observations on the seventh periodic report of the United Kingdom of Great Britain and Northern Ireland*, 17 August 2015, online at http://tbinternet.ohchr.org/_layouts/treatybodyexternal/Download.aspx?symbolno=CCPR/C/GBR/CO/7&Lang=En

[31] Human Rights Committee, *Concluding observations on the fifth periodic report of France*, 17 August 2015, online at http://tbinternet.ohchr.org/_layouts/treatybodyexternal/Download.aspx?symbolno=CCPR/C/FRA/CO/5&Lang=En

2015 on encryption and anonymity, and their relationship with the rights to privacy and freedom of expression.[32] The Special Rapporteur on Human Rights Defenders also touched on the question of online surveillance in his 2015 report, noting that:

"The Internet and, more broadly, new technology, which until recently provided a formidable tool for voicing opinions, accessing information, and forging networks of individuals and organizations, are today being used by States to monitor and curb the work of defenders. That is particularly worrying, given that numerous defenders use the Internet on a daily basis to promote and protect human rights, thereby exposing themselves to multiple threats [...] E-mails are also intercepted and telephone calls recorded."[33]

Alongside developments at the UN, a number of important human rights court cases at the European and American regional levels have contributed to the development of jurisprudence on privacy in the context of the internet and digital technologies. Beside landmark cases decided by the European Court of Human Rights, of particular relevance is the recent decision of the Court of Justice of the European Union in *Schrems v Data Protection Commissioner of Ireland* in which the Court concluded, in the context of mass interception of digital communications, that "legislation permitting the public authorities to have access on a generalized basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life [...]."[34]

There now exists significant legal authority to support the understanding that mass surveillance is a serious threat to the right to privacy. Amnesty International believes that encryption is a critical enabler to the realization of the right to privacy and freedom of expression on the internet, providing "individuals and groups with a zone of privacy online to hold opinions and exercise freedom of expression without arbitrary and unlawful interference or attacks".[35]

Limitations on encryption represent an interference with the enjoyment of the rights to privacy and freedom of expression, which must be justified as permissible in accordance with human rights law. The applicable framework for determining whether a restriction on encryption is permissible was articulated by the UN Special Rapporteur on freedom of

---

[32] Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye*, A/HRC/29/32, 22 May 2015, online at http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/Pages/ListReports.aspx

[33] General Assembly, Situation of human Rights defenders, A/70/217, 22 May 2015, para. 46., online at http://www.un.org/en/ga/search/view_doc.asp?symbol=A/70/217

[34] Court of Justice of the European Union, 6 October 2015, para.94, online at: http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=116845

[35] Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye*, A/HRC/29/32, 22 May 2015, para.16, online at http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/Pages/ListReports.aspx

expression in his 2015 report as follows:

> "First, for a restriction on encryption or anonymity to be "provided for by law", **it must be precise, public and transparent,** and avoid providing State authorities with unbounded discretion to apply the limitation (see Human Rights Committee, general comment No. 34 (2011)). Proposals to impose restrictions on encryption or anonymity should be subject to public comment and only be adopted, if at all, according to regular legislative process. **Strong procedural and judicial safeguards should also be applied** to guarantee the due process rights of any individual whose use of encryption or anonymity is subject to restriction. I**n particular, a court, tribunal or other independent adjudicatory body must supervise the application of the restriction."**
>
> Second, l**imitations may only be justified to protect specified interests**: rights or reputations of others; national security; public order; public health or morals [...] Moreover, because legitimate objectives are often cited as a pretext for illegitimate purposes, the restrictions themselves must be applied narrowly.
>
> Third, **the State must show that any restriction on encryption or anonymity is "necessary" to achieve the legitimate objective**. The European Court of Human Rights has concluded appropriately that the word "necessary" in article 10 of the European Convention for the Protection of Human Rights and Fundamental Freedoms means that the restriction must be something more than "useful," "reasonable" or "desirable". Once the legitimate objective has been achieved, the restriction may no longer be applied. Given the fundamental rights at issue, limitations should be subject to independent and impartial judicial authority, in particular to preserve the due process rights of individuals
>
> Necessity also implies an assessment of the proportionality of the measures limiting the use of and access to security online**.** A proportionality assessment should ensure that the restriction is "the least intrusive instrument amongst those which might achieve the desired result". **The limitation must target a specific objective and not unduly intrude upon other rights of targeted persons, and the interference with third parties' rights must be limited and justified in the light of the interest supported by the intrusion.** The restriction must also be "proportionate to the interest to be protected". A high risk of damage to a critical, legitimate State interest may justify limited intrusions on the freedom of expression. Conversely, where a restriction has a broad impact on individuals who pose no threat to a legitimate government interest, the State's burden to justify the restriction will be very high. **Moreover, 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.** In any case, "a detailed and evidence-based public justification" is critical to enable transparent public debate over restrictions that implicate and possibly undermine freedom of expression (see A/69/397, para. 12)" (*citations omitted – emphasis added).*

When applying this framework to particular restrictions on access to and use of encryption, the Special Rapporteur concludes as follows:

- **General bans on encryption**, or measures which amount to general bans (including the requirement for obtaining a licence from the government to use encryption or allowing only

the use of weak encryption) fail to meet the proportionality requirements of permissible restrictions, "because they deprive all online users in a particular jurisdiction of the right to carve out private space for opinion and expression, without any particular claim of the use of encryption for unlawful ends."[36]

- **Requiring corporate entities to weaken encryption, provide backdoors or adopt key-escrow systems** [see chapter 4 of this document] "would almost certainly fail to satisfy proportionality" when done in a manner in which restrictions are generally applicable to massive numbers of people without a case-by-case assessment.[37]

- **Targeted decryption orders** [see chapter 4 of this document] are more limited and are less likely to raise proportionality concerns than **mandatory key disclosure** laws. In both cases, however, "such orders should be based on publicly accessible law, clearly limited in scope focused on a specific target, implemented under independent and impartial judicial authority, in particular to preserve the due process rights of targets, and only adopted when necessary and when less intrusive means of investigation are not available. Such measures may only be justified if used in targeting a specific user or users, subject to judicial oversight."[38]

---

[36] Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye*, A/HRC/29/32, 22 May 2015, para. 40, online at http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/Pages/ListReports.aspx

[37] Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye*, A/HRC/29/32, 22 May 2015, para. 43, online at http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/Pages/ListReports.aspx

[38] Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye*, A/HRC/29/32, 22 May 2015, para. 45, online at http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/Pages/ListReports.aspx

3. FEAR OF "GOING DARK": GOVERNMENTS' EFFORTS TO WEAKEN ENCRYPTION

"encryption threatens to lead us all to a very, very dark place,"

FBI director James Comey in October 2014, calling for the beginning of a debate about placing obligations on corporate entities to provide access to encrypted services.[39]

Over the past few years, senior government officials in a number of countries have begun to publicly speak out against strong encryption over fears of "going dark" – a concept originally used by US law enforcement officials (and later appropriated by others) to describe the declining capabilities of law enforcement agencies to access the content of communications due to the increased use of encryption in everyday communication technologies and services.

In reality, while encryption can prevent the content of communications from being read, authorities are still able to intercept encrypted communication and access certain information (such as date, time, senders, size etc. – known as metadata) related to them.

The controversy over encryption stems from a practical component of computer security: by securing communications against illegitimate interference by criminals, encryption also secures communications against both illegitimate and *legitimate* interference by government authorities.

It is a generally accepted tenant of international law that targeted communications surveillance, provided it fulfils certain criteria, is an acceptable and effective means of pursuing legitimate objectives such as the prevention and detection of crime, and the protection of national security.[40] The prevention, detection, investigation and prosecution of such crimes may necessitate exceptional powers to read emails and text messages, track

[39] James B. Comey, 16 October 2014, online at: https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course

[40] See UN High Commissioner of Human Rights, *The right to privacy in the digital age*, A/HRC/27/37, para. 15, online at: http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf.

online purchases, and monitor financial movements, through the interception of digital communications and data flows.

Yet encryption must be unbreakable by everyone, even those with legitimate intentions, in order for it to be effective against those with illegitimate intentions.[41] It is for this reason that its deployment, promotion and use has become the focus of political debate and the target of legislative measures.

Government criticism of encryption has increased against the backdrop of a generalized fear, promoted by security agencies,[42] that the internet is proving a hospitable environment for terrorism related activities and cyber criminals. A number of key figures have come forward to condemn encryption (and its providers) for fostering "safe spaces"[43] for criminal activity. In January 2015, British Prime Minister David Cameron said that "we cannot allow modern forms of communication to be exempt from the ability… from being listened to".[44] In August 2015, three senior prosecutors and a senior law enforcement official from France, Spain, the USA and the UK, respectively, criticised disk encryption:

Full-disk encryption significantly limits our capacity to investigate these crimes and severely undermines our efficiency in the fight against terrorism. Why should we permit criminal activity to thrive in a medium unavailable to law enforcement? To investigate these cases without smartphone data is to proceed with one hand tied behind our backs."[45]

But some governments have taken the opposite stance; in January 2016, the French government rejected a proposed bill that would have required equipment manufacturers to

---

[41] Bruce Schneier, *iPhone encryption and the return of the crypto wars*, 6 October 2014, online at: https://www.schneier.com/blog/archives/2014/10/iphone_encrypti_1.html

[42] See, for example, an article by the head of British intelligence agency GCHQ Robert Hannigan that "The web is a terrorist's command and control centre of choice", *The Financial Times,* 3 November 2014, available at http://www.ft.com/cms/s/2/c89b6c58-6342-11e4-8a63-00144feabdc0.html#axzz42y5fToA0. See also the report by Europol on *Changes in Modus Operandi of Islamic State Terror Attacks,* which notes that "The internet and social media are used for communication and the acquisition of goods (weapons, fake IDs) and services, made relatively safe for terrorists with the availability of secure and inherently encrypted appliances, such as WhatsApp, Skype and Viber." Available at https://www.europol.europa.eu/content/changes-modus-operandi-islamic-state-terrorist-attacks

[43] Cameron: surveillance powers will deny terrorists 'safe space,' *BBC*, 2 November 2015, available at http://www.bbc.co.uk/news/uk-politics-34697535.

[44] *UK's Cameron won't "allow" strong encryption of communications*, BBC, 12 January 2015, online at: https://gigaom.com/2015/01/12/uks-cameron-wont-allow-strong-encryption-of-communications/

[45] Cyrus R. Vance Jr. et al, *When Phone Encryption Blocks Justice*, New York Times, 11 August 2015, online at: http://www.nytimes.com/2015/08/12/opinion/apple-google-when-phone-encryption-blocks-justice.html

consider the needs of law enforcement and intelligence authorities when designing technologies, inserting backdoors into devices.[46] In a letter published in January 2016, the Dutch Ministry of Security and Justice said that any moves to weaken or backdoor encryption "would have undesirable consequences for the security of information stored and communicated and the integrity of ICT systems, which are increasingly of importance for the functioning of society."[47]

Yet the debate rages on, fueled by the introduction in the United Kingdom of the Investigatory Powers Bill in November 2015, an expansive surveillance law which, if adopted, would place numerous obligations on communications service providers to facilitate interception. An initial draft of the bill empowered the Secretary of State for the Home Department to place obligations on companies to remove "electronic protections" on communications,[48] raising the prospect that the UK government could force technology companies to give backdoor access to encrypted data.[49] After considerable opposition by individuals, organizations and companies who participated in a public consultation on the bill, and after critique voiced by the parliamentary joint committee conducting the consultation, the government amended the bill before introducing it into Parliament in March 2015, clarifying that companies can only be asked to remove encryption that they themselves have applied, and only where it is practicable for them to do so.

THE APPLE V FBI CASE

For the past year, Apple and the FBI have been engaged in a public argument over the issue of encryption due to Apple's increasing use of strong encryption in its products. This came to head when the FBI sought to unlock an iPhone 5C used by one of the shooters in an attack in San Bernardino, California, that left 14 dead in December 2015.

On 16 February 2016, in response to a request by the US Department of Justice, a federal magistrate judge ordered Apple to create a custom version of its iOS operating system that would allow investigators on the case to get around the phone's security features. Apple's Chief Executive Officer, Tim Cook, responded in an open letter, in which he stated that the government's demands constituted a "breach of privacy" with "chilling" consequences. Cook said:

"When the FBI has requested data that's in our possession, we have provided it. Apple complies with valid subpoenas and search warrants, as we have in the San Bernardino case. We have also made Apple engineers available to advise the FBI, and we've offered our best ideas on a number of investigative options at their disposal…But now the U.S. government has asked us for something we simply do not have, and something we

[46] Jeff John Roberts, "France Rejects 'Backdoors' Law to Defeat Encryption," *Fortune,* 13 January 2016, available at http://fortune.com/2016/01/13/france-encryption/.

[47] Dutch government says no to 'encryption backdoors', *BBC News*, 7 January 2016, available at http://www.bbc.co.uk/news/technology-35251429.

[48] Section 189, Draft Investigatory Powers Bill.

[49] *Snooper's Charter: Tech companies will have to give police 'back-door' access to customers' data*, the Independent, 14 March 2016, online at: http://www.independent.co.uk/news/uk/politics/investigatory-powers-bill-tech-companies-will-have-to-give-police-back-door-access-to-private-data-a6928581.html

consider too dangerous to create. They have asked us to build a backdoor to the iPhone."[50]

Apple appealed the court order and a federal court hearing was due on 22 March 2016.[51] Numerous independent technology experts, law professors, technology companies and human rights organizations have supported Apple's stance on this matter.[52] A widely held view among those opposing the FBI's request, including Amnesty International, is that if Apple was compelled to modify its software to unlock this phone, it would set a precedent that could allow the US government – and potentially other governments – to compel technology companies to weaken or otherwise circumvent their encryption by providing a ´backdoor´ to intelligence and other security agencies.

In response to the case, the UN High Commissioner for Human Rights stated that: "A successful case against Apple in the US will set a precedent that may make it impossible for Apple or any other major international IT company to safeguard their clients' privacy anywhere in the world… It is potentially a gift to authoritarian regimes, as well as to criminal hackers. There have already been a number of concerted efforts by authorities in other States to force IT and communications companies such as Google and Blackberry to expose their customers to mass surveillance."[53]

HOW ENCRYPTION RESTRICTS GOVERNMENTS ACCESS TO DATA

While governments invoke a general concern about "going dark", the three main kinds of encryption present distinct challenges to electronic surveillance by state agencies. This section provides an overview of the protections that the three major types of encryption provide for data and how they affect governments' ability to access information.

FULL-DISK OR DEVICE ENCRYPTION

Whereas full-disk encryption has been available as a feature on many personal computers and laptops for some time, only since 2014 have technology companies such as Apple and Google begun switching full-disk encryption on by default on their smartphones. In phones where this feature is provided, devices can only be decrypted by the individual in possession of the phone's password or PIN.

Full-disk encryption plays a critical role in preventing and frustrating smartphone theft and the other potential criminal activities that may flow from access to the information contained

[50] Tim Cook, A Message to Our Customers, 16 February 2016, online at: http://www.apple.com/customer-letter/

[51] Apple, FBI to head to court March 22, USA Today, 20 February 2016, online at http://www.usatoday.com/story/tech/news/2016/02/19/apple-fbi--court-march-22-riverside-march-22/80635402/

[52] A list of amicus briefs in support of Apple for the 22 March 2016 hearing can be found here http://www.apple.com/pr/library/2016/03/03Amicus-Briefs-in-Support-of-Apple.html

[53] Office of the UN High Commissioner for Human Rights, Apple-FBI case could have serious global ramifications for human rights: Zeid, 4 March 2016, online at: http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=17138#sthash.o25R7Bqg.dpuf

in these devices.

In 2011, Symantec, a leading computer security company, conducted an experiment in several large North American cities called "The Symantec Smartphone Honey Stick Project", which involved intentionally losing 50 smartphones with simulated personal and corporate data on them – the company was able to remotely monitor what happened to the phones once they were found. The findings of the experiments included that attempts were made to access the following:[54]

- At least one of the various apps or files, on 96% of the devices;
- Personal apps or data held on 89% of devices;
- A private photos app on 72% of the devices;
- An online banking app on 43% of the devices;
- Social networking accounts and personal email, each on over 60% of the devices;
- Corporate-related apps or data on 83% of the devices.

The theft of vast amounts of personal information, whether private or professional, is a serious risk for anyone using computers, including smartphones, and it has serious privacy implications. Full-disk encryption is a reliable and practical way for individuals to protect their privacy against this risk.

For governments, full disk encryption can mean they are unable to access the contents of a device in an intelligible format, even if the device is in their possession, unless they are able to obtain the PIN or password. This issue is at the heart of the Apple v FBI case discussed in the previous section.

END-TO-END ENCRYPTION

In the last few years, several popular digital messaging services adopted end-to-end encryption technology. Some, like iMessage and Signal use end-to-end encryption between everyone using the service. Others, like WhatsApp, use end-to-end encryption between some, but not all messages, while others like Telegram provide a distinct mode that uses end-to-end encryption. When this kind of encryption is used, only the users – and not the service provider – holds the keys to decrypt the data.

Although comparatively few services actually offer end-to-end encryption by default, the considerable number of people who have access to these services – for example WhatsApp had one billion users in February 2016[55] - have catapulted this issue to the top of law

[54] Symantec, *The Symantec Smartphone Honey Stick Project*, online at: http://www.symantec.com/content/en/us/about/presskits/b-symantec-smartphone-honey-stick-project.en-us.pdf

[55] WhatsApp Blog, One Billion, 1 February 2016 online at: https://blog.whatsapp.com/616/One-billion

enforcement concerns around encryption

The provision of end-to-end encrypted messaging services has clear privacy benefits – it means that even if a message is intercepted, it cannot be accessed in an intelligible format; even when messages are stored or delivered through the company's servers, this is done in an encrypted form that the company itself is unable to read or analyze. While it is still possible for a third party, such as a government, to intercept messages sent via such services, they will not be able to read the actual content of these messages.[56]

There is a clear trade off that technology companies are making in providing end-to-end encryption: on the one hand, they are able to attract users who place a particular value on privacy; on the other, they cannot make money from selling advertising based on the contents of their users' communications. From a reputational perspective, however, companies are in a better position to refute accusations that they collaborate with governments in conducting surveillance if they offer end-to-end encryption; this is an increasingly important priority for technology companies in the aftermath of Edward Snowden's revelations about the role of corporations in the USA's PRISM surveillance programme.

The uptake of end-to-end encrypted messaging services means that government agencies can no longer access the content of some communications that, until recently, was readily accessible to them. A prime example of this, is the widespread use of internet messaging services like iMessage and WhatsApp instead of mobile Short Message Service (SMS); messages sent by SMS are not end-to-end encrypted, and are therefore potentially accessible to government agencies.

Nevertheless, the use of such end-to-end encrypted services does not preclude targeted surveillance, searches of targeted devices, or the analysis of the metadata associated with intercepted encrypted messages. What such services do defeat, however, is some kinds of mass surveillance programmes. This is possibly an unstated policy driver of efforts to frustrate the roll out of end-to-end encryption.

TRANSPORT ENCRYPTION

The encryption of data in transit is the type of encryption most people encounter on a regular basis. As more and more services, websites and applications use transport encryption, data that is transmitted to a company's services is encrypted and thus cannot be read by third parties, including internet service providers or someone intercepting internet traffic. This prevents a malicious hacker from viewing someone's internet banking details or username and password as it is entered into a web form, even if they are able to tap into their internet connection.

The move towards deployment of transport encryption, in the form of HTTPS, began long before the Snowden revelations but has gathered pace since. Deployment of HTTPS by companies ensures that customers' data is not vulnerable to acquisition by criminals and

[56] However, the metadata associated with such intercepted messages, which includes the sender, the recipient and the time a message was sent, can generally still be accessed.

malicious hackers and is widely considered to be essential to security and privacy.[57] Once data reaches the company's servers, it is decryptable – meaning it can be read by the company's computers (and operatives). The Internet Architecture Board, the committee charged by the Internet Society with the oversight of the technical and engineering development of the internet,[58] has issued a statement recommending that all "[n]ewly designed protocols [...] prefer encryption to cleartext operation" and urging "developers to include encryption in their implementations, and to make them encrypted by default."[59]

From a state surveillance perspective, deployment of HTTPS undermines the value of interception of communications while it transits a network. When a service uses HTTPS, the communications sent by that service can be intercepted, but their encrypted content is not readable. However, transport encryption does not entirely prevent authorities accessing data.

Government agencies can still issue warrants, for example to a company operating a website that uses HTTPS, ordering them to disclose the unencrypted content of communications and data they hold. Additionally, it's important to note that some forms of transport encryption may be vulnerable to decryption by the most technologically capable intelligence agencies.[60]

---

[57] See for example Mike Shema, *Web security: why you should always use HTTPS*, 31 May 2011, online at: http://mashable.com/2011/05/31/https-web-security/#suo1rb0vusqy and Scott Gilbertson, *HTTPS is more secure, so why isn't the web using it?* 20 March 2011, online at http://arstechnica.com/business/2011/03/https-is-more-secure-so-why-isnt-the-web-using-it/

[58] More information on the Internet Architecture Board can be found on its website: https://www.iab.org/about/

[59] IAB Statement on Internet Confidentiality, 14 November 2015: https://www.iab.org/2014/11/14/iab-statement-on-internet-confidentiality/

[60] See for example John Leyden, *Let's talk about that NSA Diffie-Hellman crack*, 19 October 2015, online at: http://www.theregister.co.uk/2015/10/19/nsa_crypto_breaking_theory/

4. RESTRICTIONS ON ENCRYPTION AND THEIR TECHNICAL AND PRACTICAL FEASIBILITY

There are a number of approaches that governments can use to circumvent or restrict encryption. They range from outright bans, to general restrictions, such as obligations to weaken or backdoor encryption, to targeted decryption orders. Each of these approaches, and particularly the most general restrictions, pose significant technical and practical challenges to governments and companies. This section outlines each of these types of restrictions:

- General measures banning or restricting encryption;
- Requiring companies to backdoor encryption services;
- Mandatory disclosure of encryption keys;
- Targeted decryption orders.

GENERAL MEASURES BANNING OR RESTRICTING ENCRYPTION

Generalized prohibitions on encryption already exist in countries such as Russia, Morocco, Kazakhstan, Pakistan and Colombia.[61] In these and other countries, individuals generally require a license or state-issued permission to use any encrypted services or those above a certain encryption strength.

The technical and practical obstacles to banning encryption are many, and include:

1. The nature of the internet is such that even when services are forbidden in a particular jurisdiction they will usually be technically accessible. Enforcing such restrictions would require significant technical investment on the part of internet service providers;

2. Even if software using strong encryption is banned from sale or downloading in one country, it can still be downloaded from websites or services based in other countries;

3. Adoption of an outright prohibition on encryption would not only seriously harm cybersecurity in a given country, it could also deter the technology industry from trading in or providing services to the country, with potential economic ramifications for the state in

[61] Article 1, Law No. 1738 of 2014; see http://www.digitalrightslac.net/en/la-peligrosa-ambiguedad-de-las-normas-sobre-cifrado-de-comunicaciones-en-colombia/ - For a full list of countries' domestic cryptography controls, see http://www.cryptolaw.org/.

question.

REQUIRING COMPANIES TO BACKDOOR ENCRYPTION

The US government's stance on the issue of encryption backdoors is particularly important due to the fact that many of the world's biggest technology companies are based in the USA; as such if the US government were to mandate backdoors, it would affect people across the world. In 2015, the Obama administration considered four approaches but decided against pursuing them.[62] These approaches are likely representative of the kinds of backdoors that other governments may be considering.

4. **Requiring companies to modify devices to include an independent, physical encrypted port** for which the government would maintain a separate set of encryption keys that it could use if it had physical access to the device. Such a system would only provide access to the (potentially limited) data stored on the device. Furthermore, such a system could be defeated if individuals used other forms of encryption on their devices.

5. **Requiring companies to send fake security updates to a user** through which malware from law enforcement authorities could be deployed, giving the government remote access to the device. This would have serious consequences for secure communications as it would call into question the trustworthiness of security updates, dissuading users from downloading them.

6. **Requiring companies to implement a one-off forced backup of data** to an alternative, accessible location, with or without notifying the user. The approach would require the service provider to have the technical ability to back up information that is originally stored in an encrypted location to a different location that is not encrypted, to which law enforcement agencies would have access. It would therefore require many service providers to modify their existing systems or develop new ones.

7. **Develop a key escrow system**: this refers to an arrangement in which the keys needed to decrypt encrypted data are split, with the different parts held by several parties so that, under certain circumstances, the keys are combined to gain access to the data. The US government, while maintaining the technical feasibility of a key escrow system, accepts that it "would be complex to implement and maintain, as it would require a network of independent recovery parties which could then be validated by trusted third parties."[63]

---

[62] *Obama administration explored ways to bypass smartphone encryption*, Washington Post, 24 September 2015, online at: https://www.washingtonpost.com/world/national-security/obama-administration-ponders-how-to-seek-access-to-encrypted-data/2015/09/23/107a811c-5b22-11e5-b38e-06883aacba64_story.html; the Obama administration's draft paper on technical options for the encryption debate can be found here http://apps.washingtonpost.com/g/documents/world/read-the-obama-administrations-draft-paper-on-technical-options-for-the-encryption-debate/1753/

[63] From the Obama administration's draft paper on technical options for the encryption debate, online at: http://apps.washingtonpost.com/g/documents/world/read-the-obama-administrations-draft-paper-on-technical-options-for-the-encryption-debate/1753/

The Obama administration concluded that it should not pursue any of these proposals. There is reportedly division within the administration, with some senior officials voicing support for robust encryption.[64]

Proposals to backdoor encryption have been heavily criticized by numerous computer security experts, who believe that they would create grave security risks and post serious human rights challenges. One of the most authoritative papers on the issues, *Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications,* was published in 2015 by fifteen of the world's most respected cryptographers and computer engineers. In the paper, they argued against "exceptional access" arrangements. They contend:

> "There are three general problems. First, providing exceptional access to communications would force a U-turn from the best practices now being deployed to make the Internet more secure. These practices include forward secrecy — where decryption keys are deleted immediately after use, so that stealing the encryption key used by a communications server would not compromise earlier or later communications[...]
>
> Second, building in exceptional access would substantially increase system complexity. Security researchers inside and outside government agree that complexity is the enemy of security — every new feature can interact with others to create vulnerabilities. To achieve widespread exceptional access, new technology features would have to be deployed and tested with literally hundreds of thousands of developers all around the world.
>
> Third, exceptional access would create concentrated targets that could attract bad actors. Security credentials that unlock the data would have to be retained by the platform provider, law enforcement agencies, or some other trusted third party. If law enforcement's keys guaranteed access to everything, an attacker who gained access to these keys would enjoy the same privilege. Moreover, law enforcement's stated need for rapid access to data would make it impractical to store keys offline or split keys among multiple keyholders, as security engineers would normally do with extremely high-value credentials[...] If service providers implement exceptional access requirements incorrectly, the security of all of their users will be at risk."[65]

The current approach of the US government appears to be focused on engagement with

---

[64] See for example: "Defense secretary favors strong encryption, not 'back doors,'" Associated Press, 2 March 2016, online at: http://bigstory.ap.org/article/01cc8a109f934081b341a573e382a5f3/defense-secretary-favors-strong-encryption-not-back-doors; "Obama, at South by Southwest, Calls for Law Enforcement Access in Encryption Fight," 11 March 2016, online at: http://www.nytimes.com/2016/03/12/us/politics/obama-heads-to-south-by-southwest-festival-to-talk-about-technology.html

[65] Harold Abelson et al, *Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications*, Massachusetts Institute of Technology, 6 July 2015, online at: http://www.crypto.com/papers/Keys_Under_Doormats_FINAL.pdf

communications services providers. The internal US White House memo that scoped the four possible approaches discussed above, took the view that "attempts to build cooperation with the industry [...] will offer the most successful option for making progress on this issue."[66] Such "cooperation" could entail encouraging technology companies to weaken, roll-back or restrain their deployment of strong encryption by default.

THE CRYPTO WARS

The present controversy around restricting encryption has been labelled the second 'Crypto Wars',[67] an unsettling reference to what is widely referred to as the 'Crypto Wars', which pitted the US government against the technology sector in the 1990s. Its origins trace back to the 1970s, when the US government classified encryption algorithms as a munition for the purpose of export controls.[68] In the 1990s, the US government sought to enforce the controls on those seeking to disseminate free, mass market encryption products for non-military applications, and even attempted to prosecute the developer of PGP, Phil Zimmerman.[69] Technologists and activists reacted by printing encryption ciphers and keys on t-shirts and in hard copy when travelling abroad as a protest against the USA's draconian application of the controls. [70]

At the same time, the administration of former US president Bill Clinton attempted to get the technology industry to adopt an encryption backdoor scheme called the 'Clipper Chip', a physical encryption device that network operators would place on their networks, for which the government would possess a decryption key.[71] When that scheme was rejected by the industry, the US government pressed for other forms of key escrow, and encouraged other countries, including the UK, to propose similar schemes. However, industry opposition, including from the banking industry, civil society outrage, and a change of administration following the 2000 US elections, saw attempts at key escrow to be ultimately abandoned.

MANDATORY DISCLOSURE OF ENCRYPTION KEYS

Where law enforcement agencies are able to intercept but not decrypt communications, they may seek the power to compel corporate entities to disclose encryption keys. Mandatory disclosure of encryption keys is provided for in legislation in a number of European countries,

---

[66] From the Obama administration's draft paper on technical options for the encryption debate, online at: http://apps.washingtonpost.com/g/documents/world/read-the-obama-administrations-draft-paper-on-technical-options-for-the-encryption-debate/1753/

[67] See for example: The Economist, *Spooks v tech firms: Crypto wars 2.0*, 8 November 2014, online at: http://www.economist.com/news/business/21631055-intelligence-agencies-and-tech-firms-have-little-choice-compromise-crypto-wars-20 and Matthew Prince, The Second Crypto War and the Future of the Internet, Huffington Post, 21 January, 2015, online at: http://www.huffingtonpost.com/matthew-prince/the-second-crypto-war-and_b_6517528.html

[68] See for example Electronic Frontier Foundation, *EFF sues to overturn cryptography restrictions*, 21 February 1995, online at: https://www.eff.org/press/archives/2008/04/21-42

[69] Philip Zimmermann, *Frequently Asked Questions*, online at: https://www.philzimmermann.com/EN/faq/index.html

[70] *The latest weapon in encryption war: a t-shirt*, GCN, 5 February 1996, online at: https://gcn.com/articles/1996/02/05/the-latest-weapon-in-encryption-war-a-tshirt.aspx

[71] Electronic Privacy Information Center, *The Clipper Chip*, online at: https://www.epic.org/crypto/clipper/

including the UK, Spain and France. It is different from the mandatory disclosure of stored data, for example pursuant to a court order or warrant, and the requirement to decrypt information (see targeted decryption orders, below), as it involves the service provider disclosing the actual encryption keys to the government agencies, and thus surrendering control over the type and scope of data which is decrypted.

The technical feasibility of this approach is being increasingly challenged by a feature that can be added to transport encryption, known as perfect forward secrecy.[72] The implementation of forward secrecy protocols means that if a server's private encryption keys are compromised, they cannot be used to decrypt past communications.[73] Google and Facebook are two of the major web services that support perfect forward secrecy; [74] as do as instant messaging application using the OTR protocol.[75] Companies providing products using end-to-end encryption such as iMessage and Whatsapp[76] do not hold the encryption keys for messages sent through their services, which means they cannot comply with key disclosure orders.

TARGETED DECRYPTION ORDERS

Several jurisdictions provide law enforcement and/or intelligence services with powers to demand decryption as a means to conduct criminal investigations or to prevent the commission of criminal acts, including terrorism. Part III of the UK's Regulation of Investigatory Powers Act (RIPA), for example, imposes an obligation of any person in possession of an encryption key to decrypt specified information when presented with an order to do so. 76 authorizations for decryption orders were granted by the UK's National Technical Assistance Centre in the year 2013-2014, the latest period for which statistics are available.[77] Even in cases where the law does not provide specifically for decryption orders, general provisions regulating/requiring assistance in searches of computers may be invoked to

[72] For more information, see https://en.wikipedia.org/wiki/Forward_secrecy

[73] For more information see Electronic Frontier Foundation, *Why the web needs perfect forward secrecy more than ever*, 8 April 2014, online at https://www.eff.org/deeplinks/2014/04/why-web-needs-perfect-forward-secrecy

[74] *Pushing for Perfect Forward Secrecy, an Important Web Privacy Protection*, Electronic Frontier Foundation, 28 August 2013, online at

https://www.eff.org/deeplinks/2013/08/pushing-perfect-forward-secrecy-important-web-privacy-protection

[75] OTR is short for Off-the-Record Messaging, a cryptographic protocol that provides encryption in instant messaging applications. See https://en.wikipedia.org/wiki/Off-the-Record_Messaging

[76] There are limitations on the applicability of end-to-end encryption for both iMessage and WhatsApp. For more details, see Kurt Wagner, *Is Your Messaging App Encrypted?*, 21 December 2015, online at: http://recode.net/2015/12/21/is-your-messaging-app-encrypted/

[77] Office of Surveillance Commissioners, *Annual Report 2013-2014,* HC 343 SG/2014/92, online at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/350857/Annual-Report-of-the-Chief-Surveillance-Commissioner-for-2013-2014-laid-4-September-2014.pdf

demand decryption.[78]

[78] For example, according to Article 30 of the Draft Zimbabwe Cyber-crime bill, a person (who is not a suspect of a crime) with knowledge of a computer system subject to a search may be ordered to assist by providing information that enables obtaining an intelligible output from such a computer system in such a format that is admissible for the purpose of legal proceedings.

5. THERE CAN BE NO BACKDOORS ON RIGHTS

In the digital age, access to and use of encryption is an enabler of the rights to privacy and freedom of expression, information and opinion, and also has an impact on the rights to freedom of peaceful assembly, association and other human rights.

Encryption is a particularly critical tool for human rights defenders, activists and journalists, all of whom rely on it with increasing frequency to protect their security and that of others. Without encryption, and with the ubiquity of surveillance technology and its widespread use by states, the work of those who stand up for their rights and the rights of their communities is at great risk.

Amnesty International believes that states should facilitate the use of encryption and must not interfere with encryption, or permit interferences by others, in an unjustified manner.

Because of the critical role played by encryption in enabling the enjoyment of, among others, the rights to privacy and freedom of expression, restrictions on access to and use of encryption, constitute an interference with the enjoyment of human rights. As such, any restrictions on encryption must be contained in laws that are precise and transparent, must be used only when necessary to achieve a legitimate aim and must not discriminate against specific individuals or groups. Critically, any measure interfering with encryption must be proportionate to achieving the legitimate aim for which it is imposed, and the benefits gained through the adoption of such measure must not be outweighed by the harm caused, including to individuals and network infrastructure and security.

Amnesty International believes that laws and policies that prohibit the use of particular encryption services or tools as such, prohibit the deployment of encryption outside of government-sanctioned specifications, or which require individuals to seek government licences prior to using encryption, amount to a disproportionate interference with the enjoyment of the rights to privacy and freedom of expression. Such measures not only deprive all individuals in a particular jurisdiction of the ability to effectively secure their communications, they also prevent individuals from freely and confidently accessing the internet and other digital technologies, and can have a "chilling effect" on freedom of expression and access to information.

Measures to oblige corporations to backdoor the encryption used in their products or services (affecting all users) constitute a significant interference with users' rights to privacy and freedom of expression. Given that such measures indiscriminately affect all users' online privacy by undermining the security of their electronic communications and private data, Amnesty International believes they are inherently disproportionate, and thus impermissible under international human rights law

States have obligations to respect, protect and fulfil the rights to privacy and freedom of expression. This includes protecting individuals against abuses by third parties, including foreign states, international organisations, corporations or private individuals. States should therefore actively promote, facilitate and otherwise ensure the security of online communications. This may include, for example, raising awareness about internet security issues, and encouraging the identification and repair of vulnerabilities in networks and systems, as well as facilitating the use of encryption tools and services.

TECHNOLOGY COMPANIES' RESPONSIBILITY TO RESPECT HUMAN RIGHTS

Companies have a responsibility to respect all human rights wherever they operate in the world.[79] This responsibility exists independently of a state's ability or willingness to fulfil its own human rights obligations.[80] As part of fulfilling this responsibility, companies need to put in place adequate measures to identify, prevent and address human rights abuses within their global operations (known as human rights due diligence).[81]

Because of the critical role that encryption plays in enabling the enjoyment of, among others, the rights to privacy and freedom of expression, technology companies and service providers could contribute to human rights abuses by governments or other third parties if they have weak encryption in their products or fulfil government requests to restrict access to, or use of, encryption. As such technology companies and service providers should be taking steps – on an ongoing, proactive and reactive basis – to assess and mitigate against such risks in each jurisdiction in which they operate or plan to operate.

At a minimum, companies have a responsibility to provide an adequate level of encryption, where their products or services involve the storage, processing or transmission of personal data. Companies should deploy encryption at a level that is effective against and commensurate to identified risks. Companies should also explicitly and clearly communicate to their users the level of security deployed in their tool or service as well as whether they can be compelled under relevant national law to make user information accessible to the law enforcement or intelligence agencies.

Companies may come under significant legal and political pressure to agree to government requests to provider user information or to restrict access to or use of encryption, including

---

[79] UN Guiding Principles on Business and Human Rights (UNGPs), endorsed by the UN Human Rights Council in 2011. UN Office of the High Commissioner for Human Rights, Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework (2011) UN Doc HR/PUB/11/04, available at www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf. These principles have also been reflected in the Human Rights Chapter of the revised OECD Guidelines for Multinational Enterprises. As of 2011, this contains a human rights chapter detailing the due diligence steps companies must take to ensure they respect human rights in their global operations. OECD Guidelines for Multinational Enterprises (2011), available at: http://mneguidelines.oecd.org/text/.

[80] UNGPs, Commentary to Principle 11

[81] UNGPs, Principles 15(b) and 17.

by weakening the encryption in their products or inserting "backdoors". If a company receives a demand from a government which is illegal under local law, or which complies with local law but would risk breaching international human rights standards, the company should challenge such requests and do everything that they can to respect human rights to the greatest extent possible in the circumstances. Companies must be able to demonstrate their efforts in this regard (i.e., their human rights due diligence measures). They should notify affected users and publicly disclose such requests and how they were dealt with.

Encryption is, today, an important enabler of human rights and a critical requirement for individual, national and international security. In the words of the UN High Commissioner for Human Rights: "The debate around encryption is too focused on one side of the security coin, in particular its potential use for criminal purposes in times of terrorism. The other side of the security coin, is that weakening encryption protections may bring even bigger dangers to national and international security."[82] Encryption must not only be protected against unjustified interference by states, which would violate their obligations under international law, but governments also have a positive obligation to facilitate its use, while corporations have a responsibility to incorporate an adequate level of encryption into their products and services.

---

[82] Office of the UNH High Commissioner for Human Rights, *Apple-FBI* case could have serious global ramifications for human rights: Zeid, 4 March 2016, online at: http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=17138#sthash.o25R7Bqg.dpuf

ANNEX: AMNESTY INTERNATIONAL POLICY ON ENCRYPTION

This policy represents the position of Amnesty International with respect to the international human rights law and standards applicable to the use of encryption tools and services in digital technologies by rights holders, and potential restrictions on such use by the state. Through this policy and associated materials, Amnesty International aims to contribute to international discussions on this issue. The policy will be reviewed and revised as needed on an ongoing basis.

1. Definitions

Encryption – a mathematical process of converting messages, information, or data into a form unreadable by anyone except the intended recipient. Most common are three different types of encryption in ordinary internet usage:

- **End-to-end encryption** exists when the keys to decrypt communications are held exclusively by the sender and recipient of the communication. When end-to-end encryption is deployed, any intermediate device or service provider with access to the electronic communications, or any entity attempting to intercept the communications, is unable to read their contents. For example, at the time of drafting of this policy in early 2016, anyone who intercepts end-to-end encrypted iMessages (used on Apple devices) or Signal messages cannot read them.
- **Disk or device encryption** is the process by which all of the information stored in computers or smartphones is encrypted when residing on the device. With some forms of device encryption, the data on a device will not be able to be read or accessed by anyone who does not possess the PIN or password to the device, including the company which manufactured the device or its software.
- **Transport encryption or transport layer encryption (the most common of which includes HTTPS, TLS or SSL)** is the practice of encrypting information and data as it traverses a computer network, for example when accessing a website or sending email. Types of transport layer encryption include Secure Socket Layer (SSL) and Transport Layer Security (TLS). These types of encryption, in effect, encrypt individuals' interactions with particular websites accessed through their web browser. When the data is in the possession of the service operator, it is in an unencrypted format, meaning that it can be disclosed to law enforcement or otherwise accessed in intelligible form once it reaches the target company/website.

Anonymity – the condition of avoiding identification. Encryption does not provide anonymity: whereas encryption tools ensure that the content of a communication is decipherable only to those holding a decryption key, they provide neither the recipient nor the sender with anonymity. The identity of the parties to a communication remains ascertainable when parties use encryption, because the metadata associated with a communication are not encrypted. Should an individual wish to remain anonymous, they need to employ anonymization tools and methods, such as using pseudonyms or anonymization tools such as

the special web-browser "Tor".[83]

Backdoors or "backdooring" – an informal term used to refer to technical measures that weaken or undermine encryption tools, devices and services in order to facilitate access to information and communications by actors other than the service provider, and parties to, the information or communications. Some of the measures that states can take to compel service providers to create backdoors include:

- Generate and retain encryption keys to accommodate the eventuality of government access to information and communications;
- Place encryption keys with a trusted, neutral outside party **"**in escrow" (meaning in custody) so that, under certain circumstances, an authorized third party, usually a state authority, may gain access to those keys to perform decryption (known as "key escrow");
- Diminish the strength of encryption used in encryption tools, devices and services; or
- Deploy only approved forms of encryption or specific state-approved random number generators used for generating encryption keys.

Another approach that gained attention in early 2016 are measures to compel companies to generate and deploy software updates that would defeat the encryption protections from a particular device, tool or service. Although this is being called a backdoor, it can also be described as an attempt to circumvent encryption in order to gain access to information and communications, which might generally be called hacking (also referred to as computer network exploitation or equipment interference). Hacking is effected through the use of vulnerabilities, malware and social engineering[84] to gain access to a device, system or network, and will often be deployed in order to circumvent the encryption which might frustrate the effectiveness of other interception capabilities. However, for the purpose of this policy, we consider the use of "forced updates" to be another "backdooring" tool.

"Going dark" – A phrase used by US law enforcement (and appropriated by others) to describe the allegedly declining capabilities of law enforcement agencies to access the content (but not the metadata) of communications due to the increased use of encryption in everyday communication technologies and services. However, in reality, encryption generally will not prevent interception of communications, nor does it render communications completely void of any intelligence information; intercepting authorities will still be able to derive some information (such as a date, time, senders, size etc. – known as metadata) from the intercepted encrypted communication.

Metadata: refers to all information that is generated through the use of communications technology other than the actual content of the communication. While the information does not necessarily contain personal or content details, it contains information about the devices being used, the users of the devices, and the manner in which they are being used (hence

[83] For more information about Tor, see https://www.torproject.org/about/overview.html.en

[84] Social engineering in the context of information security can be defined as the "psychological manipulation of people into performing actions or divulging confidential information".

also called "communications data" or "data about data", such as email recipients, call times and location records, and in the case of mobile telephones, the cell towers being used). If cross-referenced with other sources of data, an analysis of metadata can produce an accurate picture of the associations and habits of the participants to a communication. The inspection, storage, use and communication of people's metadata is a significant interference with their rights to privacy and other rights.

2. General principles

In the digital age, access to and use of encryption is an enabler of the rights to privacy and freedom of expression, information and opinion, and also has an impact on the rights to freedom of peaceful assembly, association and other human rights. Encryption is a particularly critical tool for human rights defenders, activists and journalists, all of whom rely on it with increasing frequency to protect their security and that of others. Amnesty International believes that states should facilitate the use of encryption and must not interfere, or permit interferences by others, in an unjustified manner.

Because of the critical role played by encryption in enabling the enjoyment of, among others, the rights to privacy and freedom of expression, restrictions on access to and use of encryption, therefore, constitute an interference with the enjoyment of human rights, which must be provided for by law and be necessary and proportionate to achieving a legitimate objective.[85] In particular:[86]

- Proposals for restricting access to or use of encryption must be supported by a detailed and evidence-based public justification; the onus is on the state to demonstrate that any interference is justified (not unlawful or arbitrary and is necessary and proportionate).
- Measures interfering with access to or use of encryption must be contained in laws that are precise, public, transparent and non-discriminatory, provide for effective safeguards against abuse, and avoid providing state authorities with unbounded discretion;
- Measures seeking to overcome the protection offered by encryption must be subject to prior judicial authorization;
- Measures interfering with encryption must be narrowly applied and only resorted to when necessary[87] to achieve an enumerated legitimate aim, and applied in a manner proportionate to this legitimate aim;
- Measures interfering with encryption must be the least intrusive measures available to achieve the desired result, and must not make the essence of the right interfered with meaningless;

[85] The UN Human Rights Committee has confirmed that non-arbitrariness (the term used in Article 17 of the ICCPR) requires reasonableness, which means necessity and proportionality, and has reiterated that Article 17 enshrines the same three part test as Article 19 (in its Concluding Observations to the United States of America, 2014).

[86] See also the Report of the UN Special Rapporteur on Freedom of Expression, David Kaye, on encryption and anonymity, 2015, available at http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/29/32

[87] A higher threshold than being 'useful', 'reasonable' or 'desirable').

- Measures interfering with encryption must not be discriminatory against specific individuals or groups on the basis of race, sex/gender, sexual orientation, gender identity, religion or belief, political or other opinion, ethnicity, national or social origin, disability, or other status;
- The benefits gained through the adoption of the measure interfering with encryption must not be outweighed by the harm caused, including to third parties and to network infrastructure and security; and
- Restrictions to access to or use of encryption, and measures taken to interfere with use of encryption, should be overseen by an effective impartial and independent civilian oversight authority.

3. Positive obligations

States have obligations to respect, protect and fulfil the rights to privacy and freedom of expression. This includes protecting individuals against abuses by third parties, including foreign states, international organisations, corporations or private individuals. States should therefore actively promote, facilitate and otherwise ensure the security of online communications. This may include, for example, raising awareness about internet security issues, and encouraging the identification and repair of vulnerabilities in networks and systems as well as facilitating the use of encryption tools and services.

4. The private sector

Companies have a responsibility to respect all human rights wherever they operate in the world.[88] This responsibility exists independently of a state's ability or willingness to fulfil its own human rights obligations.[89] As part of fulfilling this responsibility, companies need to take ongoing, pro-active and reactive steps to ensure they do not cause or contribute to human rights abuses. This requires companies to put in place adequate measures to identify, prevent and address human rights abuses within their global operations (known as human rights due diligence).[90]

Because of the critical role that encryption plays in enabling the enjoyment of, among others, the rights to privacy and freedom of expression, technology companies and service providers could contribute to human rights abuses by governments or other third parties if they have weak encryption in their products or fulfil government requests to restrict access to, or use of, encryption. As such technology companies and service providers should be taking steps – on

[88] UN Guiding Principles on Business and Human Rights (UNGPs), endorsed by the UN Human Rights Council in 2011. UN Office of the High Commissioner for Human Rights, Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework (2011) UN Doc HR/PUB/11/04, available at www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf. These principles have also been reflected in the Human Rights Chapter of the revised OECD Guidelines for Multinational Enterprises. As of 2011, this contains a human rights chapter detailing the due diligence steps companies must take to ensure they respect human rights in their global operations. OECD Guidelines for Multinational Enterprises (2011), available at: http://mneguidelines.oecd.org/text/.

[89] UNGPs, Commentary to Principle 11.

[90] UNGPs, Principles 15(b) and 17.

an ongoing, proactive and reactive basis – to assess and mitigate against such risks in each jurisdiction in which they operate or plan to operate.

At a minimum, companies have a responsibility to provide an adequate level of encryption, where their products or services involve the storage, processing or transmission of personal data. Companies should deploy encryption at a level that is effective against and commensurate to identified risks; ranging from common forms of transport encryption, to disk/device encryption, and end-to-end encryption. Therefore, where there is a likely or serious risk of causing or contributing to human rights abuses – for example because of the situation or context in which the company operates – the strongest encryption will need to be put in place. In any event, companies should explicitly and clearly communicate to their users the level of security deployed in their product or service as well as whether they can be compelled under relevant national law to make user information accessible to law enforcement or intelligence agencies.

Companies may come under significant legal and political pressure to agree to government requests to provide user information or to restrict access to or use of encryption, including by weakening the encryption in their products or inserting "backdoors". If a company is subjected to a demand from a government which is illegal under local law, or complies with local law but would risk breaching international human rights standards, they should challenge such requests and do everything that they can to respect human rights to the greatest extent possible in the circumstances, and must be able to demonstrate their efforts in this regard (i.e., their human rights due diligence measures). They should notify affected users and publicly disclose such requests and how they were dealt with. They should also disclose the due diligence steps they take to identify and address human rights abuses in their operations.

These measures will reduce the risk of technology companies and service providers contributing to human rights abuses, not only by governments but also by other third parties. However, a robust and thorough human rights due diligence process may result in a company not operating in a jurisdiction if it cannot identify any effective means of mitigating the risk of human rights abuse.

5. General bans on encryption

Laws and policies that prohibit the use of particular encryption services or tools as such, prohibit the deployment of encryption outside of government-sanctioned specifications, or which require individuals to seek government licences prior to using encryption, amount to a disproportionate interference with the enjoyment of the rights to privacy and freedom of expression. Such measures not only deprive all individuals in a particular jurisdiction of the ability to effectively secure their communications, they also prevent individuals from freely and confidently accessing the internet and other digital technologies, and can lead to a "chilling effect" on freedom of expression and access to information.

6. State attempts to oblige corporations to backdoor encryption

Measures to oblige corporate entities to backdoor the encryption deployed in their products or services (affecting all users), in order to ensure that communications can be decrypted by themselves or state authorities on demand, constitute a significant interference with users' rights to privacy and freedom of expression. Given that such measures indiscriminately affect

all users' online privacy by undermining the security of their electronic communications and private data, Amnesty International believes they are inherently disproportionate, and thus impermissible under international human rights law. This is particularly the case given the availability of other less intrusive measures (such as targeted decryption orders), as well as the harmful consequences of such measures, including the chilling effect on the exercise of freedom of expression and the exposure of online communications and individuals' data to vulnerabilities and other security threats. Even if it were possible to design a backdoor that could allow a state to access only a particular individual's communications and did not undermine the security of the communications of other individuals, it would raise a range of concerns similar to those relating to mandatory key disclosures (see 8 below).

7. End-to-end encryption

End-to-end encryption provides individuals with the ability to effectively secure their communications against interferences by third parties, and is therefore an important means by which individuals can protect and enjoy their rights to privacy and freedom of expression. While the use of end-to-end encryption may in specific circumstances complicate legitimate state surveillance measures, such challenges should be considered insufficient to justify broad, sweeping measures to ban, weaken or "backdoor" end-to-end encryption.

8. Mandatory key disclosure

Judicial orders requiring the disclosure of encryption keys would enable state access to an individual's entire set of communications, not just specific parts thereof.[91] Although such orders may be an effective means of pursuing a legitimate objective, they amount to a serious interference with an individual's right to privacy, among other rights. They enable an accessing authority to scrutinize private data that may go well beyond the scope of a particular investigation or legitimate objective. Such orders also often create correlative obligations on corporate entities to retain encryption keys in order to facilitate key disclosure once ordered, incurring the proportionality concerns raised above.

Moreover, the very existence of mandatory key disclosure powers in a particular jurisdiction may have the effect of deterring the use of particular tools or services for the exercise of freedom of expression and access to information, amounting to excessive state interference with private communications and leading to a "chilling effect".

As such, Amnesty International believes that mandatory key disclosure orders will fail to satisfy human rights requirements unless, among other things:

- They are used on a case-by-case basis against specified individuals based on reasonable suspicion;
- They are narrow in scope, i.e. limited to a person's communications that are sufficiently directly related to conduct which it is necessary to prevent or investigate in order to achieve a legitimate aim;

[91] This is because in many applications of encryption, a single set of keys is used to encrypt all of an individual's communications. If the keys are disclosed, all past and future communications can be decrypted.

- The time period for which they enable decryption must be no longer than strictly necessary to achieve the legitimate aim for which it has been obtained;
- They must not create obligations on corporate entities to retain keys;
- They must be used only when less intrusive means, including targeted decryption orders, are not available;
- They must not be discriminatory against specific individuals or groups on the basis of race, sex/gender, sexual orientation, gender identity, religion or belief, political or other opinion, ethnicity, national or social origin, disability, or other status;
- They must be authorized in advance by a judicial authority; and
- They must be open to a judicial challenge during and after their use.

Legislation must require that communications acquired through the use of mandatory key disclosures must be deleted at the earliest possible moment, and at the latest when it is no longer strictly necessary to achieve the legitimate aim for which it has been obtained.

9. Targeted decryption orders

While still amounting to an interference that must be justified under international human rights laws and standards, targeted decryption orders are, on their face, a more proportionate limitation of the rights to privacy and freedom of expression, as they pertain only to specified and particular communications and do not require the disclosure of the encryption key. Nevertheless, such orders must only be used in exceptional circumstances to achieve a legitimate aim, based on publicly accessible law, clearly limited in scope, focused on a specific target and based on reasonable suspicion, authorized by a judicial authority and implemented under effective independent and impartial civilian oversight. They can be resorted to only when less intrusive means are not available.

AMNESTY
INTERNATIONAL

www.amnesty.org