Encryption laws and policies: Human rights assessment tool

December 2020

GLOBAL PARTNERS DIGITAL

Contents

Introduction

Every state has obligations under international human rights law to respect, protect and promote human rights. These obligations are often also reinforced and complemented by regional human rights frameworks – such as the European Convention on Human Rights, the American Convention on Human Rights, and the African Charter on Human and Peoples' Rights – and national constitutions and legislation.

This means that governments, legislatures and other state actors must fully consider the human rights dimensions of all areas of public policy when developing legislation and other policies that may impact upon human rights.

Encryption has strong links with human rights, and so too, therefore, do laws and policies that regulate its use. It is widely recognised as a tool which enables individuals to enjoy and exercise a number of human rights, but especially the rights to privacy and freedom of expression. Encryption offers a way for people to ensure that their communications are private and to be confident that, even if they are intercepted, they cannot be read. It also facilitates the right to freedom of expression, especially in more authoritarian or repressive states. This is because it offers users privacy in their communications, enabling them to fully exercise their right to freedom of expression without potential repercussions. When encryption is unavailable, or has restrictions, limitations or controls placed upon it, people are unable to trust that their online communications or activities are secure and private.

While international human rights law does allow for some limitations on the right to privacy and freedom of expression, and therefore on the use of encryption, these are very narrow. Despite this, many laws and policies on encryption go beyond what is permitted under international human rights law.

The standards relating to the rights most affected by encryption — to privacy and to freedom of expression — have been set out in detail by international instruments and bodies. And, the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, has published reports in 2015 and 2018 which specifically examined encryption (as

well as anonymity) from the perspective of international human rights law.[1] As such, there is now a relatively clear framework for assessing whether encryption laws and policies are human rights-respecting.

The aim of this tool is to enable the user to analyse encryption laws and policies from a human rights perspective. It outlines the key elements of encryption laws and policies and how to assess them against international human rights standards. It also includes of good and poor practice from existing encryption laws and policies. For users who are interested, the Annex outlines the methodology that was used to develop the analytical tool, i.e. the relevant international human rights law and standards, as well as relevant guidance on how they apply to encryption laws and policies.

1. UN Human Rights Council, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, UN Doc. A/HRC/29/32, 22 May 2015; Mandate of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Encryption and Anonymity follow-up report, Research Paper 1/2018, June 2018.

Assessment tool

The six key elements of encryption laws and policies

While encryption laws and policies vary in their scope, there are six elements which are particularly common and which the user should look out for when doing a human rights assessment. These are:

1. **A general right to encryption**: National legislation or policy should establish a general right for individuals to use encryption products and services.
2. **Mandatory minimum or maximum encryption strength**: National legislation or policy should not mandate maximum standards for encryption products and services. Minimum standards may be permissible if they pursue a legitimate aim, and are necessary and proportionate
3. **Licensing/registration requirements**: National legislation or policy should only require providers of encryption products or services to be licenced or registered when the requirements pursue a legitimate aim, and are necessary and proportionate. Users should never be required to have a licence, be registered or obtain permission in some other way to use encryption products or services.
4. **Import/export controls**: National legislation or policy should only set out limitations or conditions on the importation or exportation of encryption products or services when they pursue a legitimate aim, and are necessary and proportionate.
5. **Obligations on providers to assist authorities**: Ideally, national legislation or policy should not require that private entities assist state authorities to access the content of encrypted communications. If legislation does include such requirements, they should only be permitted when it is in pursuance of a legitimate aim, and is necessary and proportionate.
6. **Obligations on individuals to assist authorities**: Ideally, national legislation or policy should not provide state authorities the ability to require individuals to decrypt (or assist in the decryption) of encrypted communications. Again, if legislation does include such requirements, they should only be permitted when it is in pursuance of a legitimate aim, and is necessary and proportionate.

While we have identified these six elements of encryption laws and policies, it is important to consider that states may not have all these elements within their national laws and policies. Moreover, these elements are likely to be found across various pieces of legislation and policy as states rarely have encryption-specific laws and policies.

This rest of this section is divided into six sub-sections, corresponding to the six elements of encryption laws and policies outlined above. For each sub-section, this tool sets out what a human rights-respecting element looks like. There is a separate analytical framework for each element. To provide further support to the user, examples of good and poor practice taken from existing laws and policies which comply or do not comply with the analytical framework are included—with good marked **green**, and poor **red**.

Assessing the six key elements

1. A general right to encryption

Most states do not provide a general right to use encryption, and such a provision is not strictly necessary provided that there are no restrictions on its use elsewhere which are inconsistent with international human rights law and standards. Nonetheless, guidance from the Special Rapporteur suggests that states should ensure that legislation should "recognize that individuals are free to protect the privacy of their digital communications by using encryption technology". The examples below show how some states provide for a general right to use encryption in national legislation.

Luxembourg: Article 3 of the Law of 14 August 2000 on Electronic Commerce provides that "The use of cryptographic techniques is free".

Finland: Section 6 of the Law on the Protection of Privacy in Electronic Communications (Law 516/2004) provides that subscribers and users of electronic communication services have the right to protect their communications and identification information as they wish, using any technical possibilities available, unless otherwise provided by law.

2. Mandatory minimum or maximum encryption strength

National legislation or policy sometimes, albeit rarely, mandates either minimum or maximum standards for encryption products and services, such as a minimum or maximum key length allowed.

Setting maximum standards, including a maximum key rate, is unlikely ever to be permissible under international human rights standards. By limiting the maximum standards that a person may use, state actors, companies and other third parties can more easily access the contents of that person's encrypted data. Laws and policies that set maximum standards may even be tantamount to a ban when they mandate extremely weak standards for encryption. States should therefore not establish maximum standards for encryption products and services. The examples below show how some states do, however, establish such maximum standards.

India: India's Department of Telecommunications Guidelines and General Information for Grant of Licence for Operating Internet Services provides that internet service providers may not deploy "bulk encryption" on their networks, and prohibits users from using encryption with greater than a 40-bit key length without prior permission. Anyone using stronger encryption is required to provide the government with a copy of the encryption keys.

Senegal: Article 13 of the Law on Cryptography (Law No. 2008-41) allows the National Cryptology Commission (NCC) to set down rules on the maximum size of encryption keys, and the NCC has set the maximum size at 128 bits (Article 13 of Decree No. 2010-1209, as amended by Decree No. 2012-1508). The use of encryption with a greater key length requires authorisation.

Laws and policies that set minimum standards may, however, be permissible. For example, setting minimum standards could help ensure that the encryption that is used is strong, thereby helping to protect critical infrastructure, essential services and the protection of the right to privacy. Given that

minimum standards will still amount to a restriction on the choice of encryption products and services a person uses, these minimum standards would need to be proportionate and only apply in circumstances where they are necessary. The example below show how some one state requires a minimum key size in certain circumstances, namely when government agencies are processing personal data.

The Philippines: In its NPC Circular 16-01 – Security of Personal Data in Government Agencies, the National Privacy Commission has stated that "personal data that are digitally processed must be encrypted, whether at rest or in transit" and recommends "Advanced Encryption Standard with a key size of 256 bits (AES-256) as the most appropriate encryption standard".

3. Licensing/registration requirements

In some states, national legislation or policy requires providers (and, although rarely, users) of encryption products or services to be licensed or registered in certain circumstances. As this amounts to a restriction on individuals' ability to use encryption products and services of their choice, it is important that any licensing or registration requirements pursue a legitimate aim.

For example, a government could establish a registrar for providers of encryption tools and services for the purposes of monitoring quality assurance. A licensing system might allow a regulatory body to reject certain encryption products or services when they are proven to be flawed or poorly designed. Furthermore, these requirements must be proportionate and only cover providers or users when necessary. It would be disproportionate, for instance, that every user be required to apply for a licence.

In practice, laws and policies that establish licensing or registration requirements are often used for illegitimate purposes. It is important to assess whether such requirements, particularly those within authoritarian states, are used as instruments of state control of information or restrict the market for encrypted products. This is likely to be the case when registration or licensing requirements involve the security services or military.

While best practice is not to have any licensing or registration requirements, the example below shows how one state has established a scheme that only requires encryption providers to register with a government agency, rather than to obtain any permission or authorisation.

South Africa: Section 30 of the Electronic Communications and Transactions Act of 2002 requires that all cryptography providers record their contact information and a description of their cryptography products or services with the government. The requirement only applies to companies who develop encryption products or services, and specifically states that they are not required to disclose any confidential information or trade secrets.

On the other hand, the example below shows how another state requires those wishing to provide or use encrypted telecommunication services to obtain permission from a range of government and regulatory agencies.

Egypt: Article 64 of Law No. 10 of 2003 on Telecommunication Regulations prohibits telecommunication service operators, providers, their employees and users of such services from using any telecommunication service encryption equipment without written permission from the National Telecom Regulatory Authority, the armed forces and national security entities. There is a limited exception to this requirement when the encryption equipment used for radio and television broadcasting. Contravention of this prohibition is a criminal offence punishable by imprisonment and a fine of between 10,000 and 100,000 EGP.

4. Import/export controls

In some states, national legislation or policy sets out limitations or conditions on the importation or exportation of encryption products and services. As these controls restrict the availability of encryption products and services, they must pursue a legitimate aim, such as restricting the exportation of encrypted tools to authoritarian states. This is a common objective of many states and is reflected in the multilateral export control regime known as the Wassenaar Arrangement. The Wassenaar Arrangement establishes rules on the export of cryptography tools and other dual-use technologies to prevent them from being used to develop or enhance the military capabilities of states which pose a threat to international peace and security. Being a participating state of this agreement might be indicative of a legitimate aim when it comes to restrictions on the importation or exportation of encryption products and services.

Some states, however, control the importation or exportation of encryption products and services in order to maintain weaknesses that enable governments to access the contents of encrypted data, and to keep out of the state strong encryption products and services that they cannot decipher. It is therefore necessary to consider the system of government and potential motivations behind such controls in addition to the text of the legislation or policy itself.

While any restrictions on the import or export of encryption products and services must be a proportionate means of achieving a legitimate aim, in practice, restrictions on imports are likely to be of greater concern. It might, in theory, be proportionate to restrict imports of encryption tools from a particular state, or limit certain types of tools where there is a risk that they are flawed, poorly designed, or contain malware. However, the motivation behind restrictions on the importation of encryption tools is often to prevent the population from being able to access them at all. This is very likely to be the case where there are blanket restrictions on importation, as in the example below.

China: State Council Order No. 273 "Regulation of Commercial Encryption Codes" provides that the import and export of any encryption product requires a license by the National Commission on Encryption Code Regulations.

Restrictions on the exportation of encryption tools are less likely to be of concern. Indeed, restrictions may even beneficial where the objective is to prevent the misuse of otherwise legitimate tools by other governments and actors in ways that would harm human rights. The example below show how one state has introduced limited restrictions on the exportation of certain encryption products, focusing on potentially harmful uses, rather than products marketed to the public.

Canada: Section 3 of the Export and Import Permits Act allows the government to establish an Export Control List, setting out restrictions on the export of certain articles. Items on the list must generally be authorised by an export permit before they can be exported from Canada, which include certain forms of cryptography. A permit is not required, however, if the cryptographic item is being exported to the USA, nor if the cryptographic item is one that is marketed to the general public.

5. Obligations on providers to assist authorities

In some states, national legislation or policy requires or requests that private entities assist state authorities to access the contents of encrypted communications, whether through decryption, the development and deployment of "backdoors", or some other action. Given the significant interference that these measures constitute with individuals' human rights, national laws and policies should, ideally, not contain them at all.

If there are any measures at all which make requirements of private entities to assist state authorities in accessing the contents of encrypted communications, they must be accompanied by strict limitations, safeguards and oversight to ensure that they are only used where necessary and proportionate. This means:

- The power to require or request assistance from private entities should be clear and unambiguous;
- It should only be possible to exercise the power in order to pursue a legitimate aim, such as the prevention of serious crime, the protection of public order, or the protection of the rights of others. Even purportedly legitimate aims may be cited as a pretext for illegitimate ones so, where possible, examine how the powers are exercised in practice;
- Any exercise of the power should be overseen by an independent judicial authority;
- Any exercise of the power should only be permitted where it is proportionate, and no alternative actions would be as effective. The independent judicial authority should be entitled to make a determination of the proportionality of the power's exercise;
- Any exercise of the power should only be exercisable in relation to specific, identified individuals, rather than to an entire group of people;
- Any exercise of the power should only be exercisable for a limited, specified time period, with judicial review if the length of time is an extended one;
- Any sanction for non-compliance should be proportionate.

There is no state which has placed legal obligations on providers to assist authorities in a way which fully meets all of the above criteria, however some states have stronger limitations, safeguards and oversight than others.

China: Article 18 of the Anti-Terrorism Law simply provides that telecommunications operators and internet service providers "shall provide technical interfaces, decryption and other technical support assistance to public security organs and state security organs conducting prevention and investigation of terrorist activities in accordance with law".

There are no limitations, safeguards and oversight save that the provisions only apply in relation to the "prevention and investigation of terrorist activities".

India: Section 69 of the Information Technology Act 2000 gives the central and state governments the power to direct any government agency to intercept, monitor or decrypt, or cause to be intercepted, monitored or decrypted any information transmitted, received or stored through any computer resources. The government must be satisfied that "it is necessary or expedient to do so in the interest of the sovereignty or integrity of India, defense of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence". In consequence, the agency may require any "subscriber or intermediary or any person in charge of the computer resource" to "extend all facilities and technical assistance" necessary to intercept, monitor or decrypt the information. Failure to do so is a criminal offence punishable by up to seven years' imprisonment, a fine, or both.

The limitations and safeguards here are minimal, limited solely to the government being satisfied that such measures are "necessary or expedient" in relation to a list of objectives.

Australia: The Telecommunications Act 1997 provides for three types of requests and notices that the government and certain security and law enforcement agencies can issue to communications providers.

Technical assistance requests (sections 317G to 317K) which can be issued by a security or law enforcement agency, and ask, but do not require, the provider to take specified steps which would ensure that the provider is capable of giving certain types of help to the agency for purposes such as safeguarding national security or to enforce criminal law.

Technical assistance notices (sections 317L to 317RA) which can also be issued by a security or law enforcement agency, and require the provider to take specified steps which would help the agency in relation to its functions relating to national security or enforcing the criminal law.

Technical capability notices (sections 317S to 317ZAA) which can only be issued by the Attorney-General, and require the provider to do certain specified acts or things, related to technical capability, which ensure that the provider is capable of giving certain types of help to the security agencies, again, in relation to its functions relating to national security or enforcing the criminal law.

Failure to comply with a technical assistance notice or a technical capability notice is a criminal offence, punishable by up to 47,619 penalty units (AUD 9,999,990) if the provider is a body corporate and 238 penalty units (AUD 49,980) if it is not.

All of the requests and notices are made by the government, and not subject to judicial oversight. However, there are some safeguards:

- Any request or notice must be reasonable and proportionate, and compliance must be practicable and technically feasible. The assessment of reasonableness and proportionality includes consideration of a number of specified factors, including whether the request or notice is "necessary" as well as "the legitimate expectations of the Australian community relating to privacy".
- Where a request or notice relates to encryption, it must not have the effect of "requesting or requiring a designated communications provider to implement or build a systemic weakness, or a systemic vulnerability, into a form of electronic protection" or "preventing a designated communications provider from rectifying a systemic weakness, or a systemic vulnerability, in a form of electronic protection".
- The Act explicitly states that such requests cannot require implementing or building new decryption capabilities in relation to a form of electronic protection as well as anything that would render systemic methods of authentication or encryption less effective. Weaknesses and vulnerabilities are systemic if they affect "a whole class of technology" but are not if they are "selectively introduced to one or more target technologies that are connected with a particular person".

6. Obligations on individuals to assist authorities

In addition to provider assistance provisions, national legislation or policy may also provide for state authorities to be able to require individuals to decrypt (or assist in the decryption) of encrypted communications. Again, ideally, states should not require any individual to assist in the decryption of encrypted communications. However, if powers to require individuals to do so do exist, they must be accompanied by strict limitations, safeguards and oversight to ensure that they are only used where necessary and proportionate. This means:

- The power to require individuals to decrypt or assist in the decryption of communications should be clear and unambiguous;
- It should only be possible to exercise the power in order to pursue a legitimate aim, such as the prevention of crime, the protection of public order, or the protection of the rights of others. Even purportedly legitimate aims may be cited as a pretext for illegitimate ones so, where possible, examine how the powers are exercised in practice;
- Any exercise of the power should be overseen by an independent judicial authority;
- Any exercise of the power should only be permitted where it is proportionate, and no alternative actions would be as effective. This should include a determination of whether other tools, such as traditional policing and intelligence and transnational cooperation, would enable relevant evidence to be obtained;
- The independent judicial authority should be entitled to make a determination of the proportionality of the power's exercise;
- Any exercise of the power should only be exercisable in relation to specific, identified individuals', rather than to an entire group of people;
- Any sanction for non-compliance should be proportionate.

The examples below show how some states' legislative and policy framework either do not include any obligations on individuals to decrypt (or assist in the decryption) of encrypted communications, or subject such requirements to significant limitations, safeguards and means of oversight.

Canada: There is no legislative power which can be used to require individuals to decrypt encrypted communications and in R v. Boudreau-Fontaine (2010 QCCA 1108), the Quebec Court of Appeal found that an order compelling an individual to provide a password violated his constitutional rights, including his rights to silence and against self-incrimination.

Ireland: Section 7 of the Criminal Justice (Offences Relating to Information Systems) Act 2017 provides that a judge may issue a warrant for the search of a particular place and any persons found at that place. A person executing the warrant may operate computers at that place, and require persons at the place to give them any password or encryption key necessary to unencrypt any information on that computers. Failure to comply with such a requirement is a criminal offence punishable with a class A fine or imprisonment for a term not exceeding twelve months, or both.

While this power does require individual to provide decryption keys, there are a number of safeguards in place:

- The power can only be exercised after a judge has issued a warrant, and can only be exercised at the specific place set out in the warrant;
- Before issuing a warrant, the judge must have reasonable grounds for suspecting that evidence of (or relating to) the commission of an offence can be found in that place;
- The offence must be one of a limited number of computer-related offences set out in the law (such as accessing information or intercepting communications without lawful authority);
- As an alternative to producing the password or encryption key, the person can produce the required information in a form in which it can be removed and in which it is, or can be made, visible and legible;
- The maximum penalty for non-compliance is a fine or twelve months' imprisonment.

Uganda: Section 10(1) of Regulation of Interception of Communications Act, 2010 allows the security and law enforcement agencies to impose "disclosure requirements" to persons in respect of encrypted information where they believe that a key to encrypted information is in the possession of that person, and that a disclosure requirement is necessary for in the interests of national security, to prevent or detect a criminal offence which puts a person's life at risk, to prevent or detect an offence of drug trafficking or human trafficking, or in the interests of the country's economic wellbeing.

A person subject to a disclosure requirement must use any key in their possession to get access to the information and disclosure it in an intelligible form (s. 10(4)). If the person no longer possess the key but has information that will facilitate the obtaining or discovery of the key, they must disclose that information to the agency (s. 10(5)).

Failure to comply with a disclosure requirement is a criminal offence, punishable with up to five years' imprisonment, a fine, or both.

There are no meaningful safeguards, such the need for a warrant or some other form of judicial oversight, and the range of circumstances where the power can be exercises is broad, extending beyond cases involving immediate harm, to cases involving the "economic wellbeing" of the country.

Methodology

The methodology used to undertake the analysis is based on international human rights law, primarily the International Covenant on Civil and Political Rights (ICCPR). As noted in the introduction, the most relevant human rights impacted by laws and policies on encryption are the rights to privacy and freedom of expression. Article 17 of the ICCPR guarantees the right to privacy and provides that "no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence". The right to privacy includes control over one's personal property and the ability to communicate with others privately. Article 19 of the ICCPR guarantees the right to freedom of expression, including the right to receive and impart information and ideas of all kinds regardless of frontiers. This right applies to communications of all kinds, through any media (and therefore online as well as offline).

As is well-established under international human rights law, any measure which interferes with either the right to privacy or the right to freedom of expression will amount to a breach of those rights unless it can be justified. In order to be justified, any restriction must meet a three-part test, namely that (i) there is a clear legal basis for the restriction, (ii) it pursues a legitimate aim, and (iii) it is necessary and proportionate to achieve that aim.

These international human rights laws and standards form the basis of the methodology, but it is also informed by relevant guidance from the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, and in particular the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression's report on encryption and anonymity in 2015,[2] and the follow up report on the same issues in 2018.[3] .

2. UN Human Rights Council, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, UN Doc. A/HRC/29/32, 22 May 2015.

3. Mandate of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Encryption and Anonymity follow-up report, Research Paper 1/2018, June 2018.

Registered address:
Second Home
68 Hanbury St
London E1 5JL

info@gp-digital.org