# A joint civil society response to the Office of the High Commissioner for Human Rights call for input to a report on the right to privacy in the digital age

*This response has been jointly drafted by the civil society organisations listed in alphabetical order at the bottom of the submission.*

---

The respondents are pleased to respond jointly to this call for input for a report on "the right to privacy in the digital age".

Although there are a wide range of issues which fall within the scope of privacy in the digital age, our submission focuses specifically on the privacy and security of personal information and communications, notably via encryption. Encryption plays a critical role in enabling privacy and other human rights, particularly freedom of expression, in a range of different countries and contexts. We have seen policies and proposals put forward by different governments around the world that would restrict the availability and utility use of strong encryption, undermining – and potentially eliminating – the opportunities that encryption provides for the protection and enjoyment of human rights including, for example vulnerable and marginalised groups.

Further, considering the growing, reliance on data-driven technology, biometric data and other technologies such as the 'Internet of Things' or connected devices, we consider that it is increasingly crucial to support and recognise the role of strong encryption in helping promote and protect the right to privacy, along with the security of systems, devices and networks.

In this submission, we set out our understanding of the obligations of states on the issue of encryption, and highlight examples of concerns as well as good practice, in the hope that these will be reflected in the report.

1. **States should, as a matter of principle, ensure that relevant legislation, policies and regulation promote the use of technologies that ensure the confidentiality, integrity and security of online communications**

States have not only an obligation to *respect* the right to privacy (by refraining from undertaking actions which amount to unjustified interferences with people's privacy) but also obligations to *protect* and *fulfil* the right to privacy by ensuring that people are able to protect their privacy in practice, including through the adoption of legislative or other measures. This includes privacy of correspondence and communications as is clear from General Comment No. 16 of the Human Rights Committee.[1] Further, as has been noted by Frank LaRue, former Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, "*[i]n order for individuals to exercise their right to privacy in communications, they must be able to ensure that these remain private, secure and, if they choose, anonymous.*"[2]

Strong encryption enables all individuals to protect their right to privacy of online correspondence and communications. In addition, as was noted in the UN Human Rights Council's Resolution 34/7 on the right to privacy in the digital age , violations and abuses of the right to privacy in the digital age have particular effects on women, children and persons in vulnerable situations, and marginalised groups. As such, states have an obligation to refrain

---

[1] UN Human Rights Committee, General Comment No. 16: Article 17 (Right to Privacy), 1988, Para 8.
[2] UN 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*, UN Doc. A/HRC/23/40, 17 April 2013.

from taking steps to undermine its availability and utility, and to ensure that it is available to all individuals within their territories or subject to their jurisdiction, including through the adoption of legislative or other measures. Strong encryption provides one of the most effective means by which individuals can protect the privacy and security of their digital correspondence and communications. As such, we believe that states have an obligation – as part of their broader obligation to respect and fulfil the right to privacy – to ensure that relevant legislation, policies or regulations promote strong encryption.

Yet, there is legislation and regulation in a number of states which undermines strong encryption. These include restrictions on its use, requirements for licencing and registration of encryption products and services, or compelling communications service providers to retain decryption keys or otherwise assist in the decryption of encrypted communications. Such actions are inconsistent with the general obligation upon states to respect, protect and fulfil individuals' right to privacy of correspondence and communications.

For example, in Pakistan, Section 35(1)(g) of the Prevention of Electronic Crimes Act, 2016 provides powers to an authorised officer during search and seizure to require from an individual access to any "decryption information" of an information system, device or data under investigation that is in their possession to grant him access to such data, device or information system in an unencrypted or decrypted intelligible format for the purpose of investigating any such offence under the Act. The law further explains "decryption information" as information or technology that enables a person to readily retransform or unscramble encrypted data from its unreadable form and from ciphered data to intelligible data.

And in Brazil, the Congress is currently examining legislation which could give police officers access to the encrypted content contained within messaging services without a court order where an individual has sent or received messages and is caught in the act of committing a serious crime such as terrorism or drug trafficking. The legislation would also require platforms to decrypt the message and/or provide the technology for doing so. The Bill in question would amend, and undermine, the Marco Civil da Internet to allow law enforcement agents to have not only access to the content, but to the decryption key. The proposal makes reference to legislation in Germany under which law enforcement agencies are able to access the content of encrypted messages from WhatsApp and Skype, and use spyware on mobile phones and computers to access encrypted information.

2. **States should allow individuals to use whatever technology they choose in order to secure their communications. Relevant legislation, policies and regulations should recognise that individuals are free to protect the privacy of their digital communications by using encryption technology of their choice**

As part of their general obligation to ensure that relevant legislation, policies and regulation promote strong encryption, we believe that best practice dictates that this should be explicitly guaranteed in legislation, policies or regulation as appropriate. While general guarantees of privacy in constitutions or national human rights legislation are welcome, we believe that more specific recognition of an individual's right to use whatever encryption technology they wish, and of whatever strength provides clearer and stronger protection. A number of states have such legislation, for example Barbados,[3] Finland,[4] Luxembourg[5] and Malawi.[6] In a number of

[3] Section 21(2) of the Electronic Transactions Act, 2001.
[4] Section 5 of the Act on the Protection of Privacy in Electronic Communications.
[5] Article 3 of the Law of 14 August 2000 on Electronic Commerce.
[6] Section 52(4) of the Electronic Transactions and Cyber Security Act, 2016.

other states, governments have publicly recognised the benefits of strong encryption and committed themselves to supporting its use, such as Netherlands[7] and Germany.[8]

In other states, however, we have seen attempts made to restrict either certain forms of communications technologies that are encrypted (such as WhatsApp in Brazil, Telegram in Pakistan) or maximum encryption key sizes (such as in Senegal and India). Such actions, while not amounting to prohibitions on the use of encryption *per se*, significantly undermine the ability of individuals to use strong encryption of their choice, and, we believe, are inconsistent with the state's general obligation as set out above.

For example, the use of Telegram has been banned in Pakistan since November 2017, when the Pakistan Telecommunication Company Limited, PTCL tweeted for its customers confirming the block on Telegram services at ISP level in Pakistan.

In addition to the above, states should also ensure the integrity of communications against interferences as well as uninhibited communications as a precondition for the full enjoyment of the right to freedom of expression given that such freedom of expression is undermined by the possibility of surveillance.

3. **States should refrain from interfering with the use of encryption technologies and should avoid all measures that weaken or undermine the security or effectiveness of that encryption. These include backdoors, mandated weak encryption standards, key escrows, requiring or promoting the installation of technical vulnerabilities in encryption products or the banning of devices, platforms and software which employ encryption by default or by design**

The benefits of encryption in protecting the right to privacy, and in facilitating the enjoyment of other human rights, is also undermined by interferences with encryption technology which weaken or undermine its security and effectiveness. While the right to privacy is not an absolute right, and can be restricted in certain circumstances, one of the requirements – which we set out below – is that restrictions be proportionate. We believe that blanket measures which apply to certain particular forms of encryption or all users of a particular service or product, however, amount to disproportionate restrictions that cannot be justified, a conclusion also reached by David Kaye, Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression.[9] We are particularly concerned by continued calls in some states for backdoors or some other means offering the potential for any encrypted message to be decrypted within certain products and services that provide end-to-end encryption.

4. **States should ensure that there are no legal barriers or restrictions that prevent or limit the use or effectiveness of encryption. Interference with specific encrypted communications should only be permitted exceptionally, on a case-by-case basis, after the act of communication, and only where the requirements of legality, legitimate aim, necessity and proportionality are met. Any such interferences should require a court order, follow due process and ensure the protection of procedural rights of individuals concerned**

---

[7] Ministry of Security and Justice, Cabinet's view on encryption, 4 January 2016, available: https://www.enisa.europa.eu/about-enisa/structure-organization/national-liaison-office/news-from-the-member-states/nl-cabinet-position-on-encryption.

[8] Federal Ministry of the Interior, Cyber Security Strategy for Germany, 2016.

[9] See, for example, 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, Paras 40, 41 and 43.

As we note above, we recognise that the right to privacy is not an absolute right, and that there are certain situations whereby interferences with the right can be justified. For an interference to be justified, it will need to meet the tests of (i) lawfulness, (ii) pursuance of a legitimate aim, and (iii) necessity and proportionality. Any restrictions on the use or effectiveness of strong encryption, or interferences with specific encrypted communications, would need to meet all elements of this three part test so as not to be in breach of international human rights law.

This means that, first, any general legal barriers or restrictions which prevent the use or effectiveness of encryption cannot be justified. As we note above, any such barriers or restrictions are blanket measures since they would impact upon all users and potential users of encryption. For an interference to be justified, it must be proportionate, meaning it must be narrowly tailored to meet the legitimate aim pursued. We do not believe that blanket measures can ever meet this test, even where it applies only to a particular product or service. Further, regardless of any legal safeguards, restrictions should not involve attempts to break encryption on the technical side, such that its effectiveness for other users would be effective. Again, such measures would be disproportionate.

Second, interferences with the encrypted communications of a specific individual – such as by requiring their decryption from the individual concerned or a third party, including the communication service provider – may in exceptional circumstances and on a case-by-case basis meet the test of proportionality. Given that such interferences amount to a significant invasion of a person's privacy of communications, strict scrutiny is required that they can be justified.

First and foremost, the requirements relating to justified interferences with the right to privacy (as set out in General Comment No. 16 of the Human Rights Committee) must be met. The interference must be provided for by law (which is accessible, clear and precise); interferences will only be permissible if they are in pursuance of an objective, legitimate aim (such as to prevent serious crime or to protect national security); and they will only be permissible if they are necessary and proportionate (i.e. that no alternative, less restrictive means, would achieve the same result). Further, we believe that any interferences should only be permitted where the following institutional and procedural safeguards apply: a court order has been obtained, that due process is followed in the obtaining and enforcement of that order, and that the procedural rights of the individuals concerned be protected.

5. **States should ensure that policies regarding encryption are subject to public debate and adopted through public, informed and transparent processes. States should ensure the effective participation of a wide variety of all stakeholders, including civil society actors and minority groups in such debates and processes.**

Given their significant impact upon human rights, particularly as noted above under heading 1, to women and those who are vulnerable or marginalised, we believe that the development and adoption of laws, policies and regulations relating to encryption should be undertaken following a public, informed, transparent and multistakeholder process. This means, for example, that the following principles should be considered:

**Open and accountable**: Participation in the process should open and accessible to relevant stakeholders. This may take the form of active measures to enable participation (e.g. notice given well in advance and distributed via relevant channels), as well as efforts made to address obstacles that may prevent or discourage it.

**Inclusive**: Assessing the degree to which a process is inclusive means looking at both the extent to which the different views and interests of the relevant stakeholders are heard and considered, and the extent to which deliberations are informed and evidence-based.

**Consensus-driven**: In a consensus-driven process, the participants act with common purpose, in a collaborative manner and, as far as is possible, take decisions by general agreement. Compromise also plays an important role in multistakeholder processes; the willingness of stakeholders to cede ground is often a necessity to achieving consensus.

**Transparent and accountable**: Clearly defined and transparent procedures and mechanisms are essential to the success of a multistakeholder policy development process. These can include disclosure of stakeholder interests, systems of records management, clear and functioning lines of accountability internally between the leadership and group, as well as externally between stakeholders and their wider communities.

6. **States should promote and encourage the use of encryption, better digital literacy and the proliferation of open source encryption software, including by supporting its regular and independent maintenance and auditing for vulnerabilities.**

As we note above, states have an obligation to ensure that the right to privacy is fulfilled in practice. With respect to encryption, we believe that this means that states should create the conditions in which individual are able to ensure the privacy of their correspondence and communications, and that this can be achieved with measures going beyond legislation and regulation. In particular, we believe that there are three broader steps that states could take to help meet this obligation:

- By promoting the use of strong encryption in relevant policies and statements, for example in national cybersecurity strategies and policies, or through public statements;
- By supporting better digital literacy within countries, at all levels and for all age groups, with a particular focus on vulnerable and marginalised. As part of this, states should ensure that education on security measures is provided or available to individuals, including on how to take effective measures to protect the confidentiality, integrity and security of their communication; and
- By supporting the development, use and adoption of open source encryption software, through financial support or supporting the regular and independent maintenance and auditing of such software for vulnerabilities.

## Respondents

Bytes for All
Coding Rights
Derechos Digitales
Global Partners Digital
KICTANet
ICT Watch
Media Rights Agenda
Media Foundation for West Africa
SUARAM