Submission to the UN Special Rapporteur on freedom of expression – anonymity and encryption in digital communications, February 2015

1. Introduction

Privacy International submits this information for the Special Rapporteur's report on the use of encryption and anonymity in digital communications.

Anonymity and the use of encryption in digital communications engage both the right to freedom of expression and right to privacy very closely: anonymity and encryption protects privacy, and without effective protection of the right to privacy, the right of individuals to communicate anonymously and without fear of their communications being unlawfully detected cannot be guaranteed. As noted by the previous mandate holder, Frank LaRue, "the right to privacy is essential for individuals to express themselves freely. Indeed, throughout history, people's willingness to engage in debate on controversial subjects in the public sphere has always been linked to possibilities for doing so anonymously."[1]

Individuals' right to privacy extends to their digital communications.[2] As much as they offer new opportunities to freely communicate, the proliferation of digital communications have significantly increased the capacity of states, companies and other non-state actors to interfere with individual's privacy and free expression. Such interference ranges from mass surveillance of communications by state intelligence agencies, to systematic collection and storage of private information by internet and telecommunication companies, to cybercrime.

Anonymity and encryption are essential tools available to individuals to mitigate or avert interferences with their rights to privacy and free expression. In this way, they are means of individuals exercising to the fullest degree their rights when engaging in digital communications.

Anonymity has long been a means by which individuals could freely enjoy their right to impart and receive information, free from State control. The use of pseudonyms, nom de plumes and pen names to conceal an author's identity has been common

1 UN Doc. A/HRC/17/27, 16 May 2011.

2 Both the UN General Assembly and the UN Human Rights Council have consistently affirmed that the same rights that people have 'offline' must also be protected 'online', including the right to privacy (UN General Assembly resolution on the right to privacy in the digital age, 18 December 2014; resolution 68/167 of 18 December 2013; and Human Rights Council resolution 26/13 on the promotion, protection and enjoyment of human rights on the Internet, of 26 June 2014.)

throughout history, and essential to the publication of works that critique governments or powerful actors, or expose wrongdoings. Indeed, the name of that famous author of dystopian fiction, George Orwell, was in fact a nom de plume. Pen names have also been an effective means by which women authors have been able to have their works published and given equal and unbiased attention. Anonymity can protect whistleblowers, sources and dissidents from exposure, and thus ensure they're able to communicate freely and in private.

Encryption tools and services are a means by which individuals can protect their anonymity, as well as the security and privacy of their communications. Encryption, too, has long played a role in security the enjoyment of human rights. In fact, one of the earliest uses of encryption was by Julius Caesar, who used a "cipher" to protect the transmission of information of military significance. Today, encryption is used by every person who uses a cell phone or a computer, and protect their personal details and communications from interference by cyber criminals, identity thieves, hackers, and States. The use of encryption is the only way to ensure digital communications – ranging from online financial transactions to cell phone calls to emails - are protected from interference.

The availability of anonymity and encryption must be seen as essential preconditions to the exercise of privacy and free expression. However, the right to privacy and to freedom of expression are not absolute rights. There are legitimate grounds under which these rights can be limited. Restriction of these rights by States must be justified as a permissible limitation under international human rights legal standards, by reference to the overarching principles of legality, necessity and proportionality. This submission will address the types of measures that restrict or eradicate the availability of anonymity and encryption, and the conditions that must exist for them to constitute permissible limitations of the rights.

Underpinning our submissions and reiterated throughout is the important reality that digital communications are inherently universal, and measures which restrict their free, secure and private use will have universal impacts. Because of the way that digital communications flow across borders and around the world, measures which restrict the use of anonymity in one State cannot but impact the rights of individuals in another.

Equally, the existence of targeted powers to remove or defeat encryption in one State has implications for all individuals, and creates a chilling effect for people around the world that is far greater than the sum of isolated instances in which such powers might be deployed.

2. General measures that limit or eradicate anonymity

Laws that restrict anonymity of users on the internet or when communicating through mobile phones are on the rise. According to the 2014 Freedom of the Internet report by Freedom House, 19 out of the 65 countries studies passed new legislation that

increased surveillance or restricted internet anonymity in 2014.[3] State measures to restrict anonymity are both influenced by and have a flow on effect on the actions of private companies, which are also increasingly limiting the use of anonymity or pseudonymity, and requiring the use of real names as a precondition to the use of particular services. Anecdotal evidence shows that often the actions of private companies are a result of pressure from States to ensure companies are able to facilitate State surveillance of their users.

Mandatory SIM card registration

States are increasingly passing laws which require telecommunications companies to require the provision of State-issued identification as a prerequisite for the obtaining of SIM cards, and thus accessing mobile communications. SIM card registration laws are particularly prominent in Africa, where 49 of the 55 countries require the mandatory registration of SIM cards.[4]

SIM registration, in effect, eradicates the ability of mobile phone users to communicate anonymously and facilities mass surveillance, making tracking and monitoring of all users easier for law enforcement and security agencies. SIM users' information can be shared with government departments and matched with other private and public databases, enabling the State to create comprehensive profiles of individual citizens. An individual's phone number could potentially be matched with their voting preferences or health data, enabling governments to identify and target political opposition, for example, or people living with HIV/AIDs. The potential for misuse of such information, particularly in countries with traditions of ethnic conflict and in situations of political instability and unrest, is enormous.

SIM registration can also have discriminatory effects - the poorest individuals (many of whom already find themselves disadvantaged by or excluded from the spread of mobile technology) are often unable to buy or register SIM cards because they do not have identification documents. Undocumented migrants are similarly disadvantaged. This could result in exclusion from numerous public services. In addition, given the additional burdens that SIM registration places on telecommunication companies, this may result in additional costs being passed on to a customer.

Importantly, the justifications commonly given for SIM registration – that it will assist in reducing the abuse of telecommunications services for the purpose of criminal and fraudulent activity – are unfounded. SIM registration has not been effective in curbing crime, and instead has fueled it: States which have adopted SIM card registration have seen the growth of identity-related crime, and have witnessed black markets quickly pop up to service those wishing to remain anonymous (for example, in Saudi Arabia). SIMs can be illicitly cloned, or criminals can use foreign SIMs on roaming mode, or internet and satellite telephony, to circumvent SIM registration requirements.

3 https://freedomhouse.org/sites/default/files/FOTN_2014_Full_Report_compressedv2_0.pdf

4 http://firstmonday.org/ojs/index.php/fm/article/view/4351/3820

Because of its ineffectiveness and exclusionary impacts, SIM registration has been rejected after consultation in Canada, Czech Republic, Greece, Ireland, the Netherlands and Poland.

Real name registration

In some States, the ability of individuals to communicate anonymously is undermined by real name registration laws, which require internet users to register with their real name (often using a government-issued ID) when using certain internet services. Real name registration is an incredibly invasive policy as it is designed to facilitate the identification of users and the policing of content for critical, libelous, defamatory or dissenting opinions and ideas.

For example, in the last few weeks China has implemented real name registration policies that will require users of blogs, microblogs, instant-messaging services, online discussion forums and news services to register with their real name from 1 March 2015.[5] While users will be allowed to choose usernames, usernames that harm national security or unity are banned, as are those that promote pornography, gambling, violence, terror, superstition and rumour.

Blanket data retention

Use of the internet via mobile and digital devices enables the creation of certain types of personal data about communications, known as communications data or metadata. This type of data includes personal information about individuals, their locations and online activities, and logs and related information about the e-mails and messages they send or receive. Communications data are storable, accessible and searchable, and access to and analysis of the data can be hugely revelatory and highly invasive. The historical distinction between data about an individual's communications and the content of his or her communications has become insignificant.

In many States, blanket data retention regimes mandate the collection and retention of metadata by telecommunications providers for up to two years. Data retention laws are justified by the need for enforcement and intelligence agencies to have access to communications data in certain circumstances for investigation and intelligence activities.

However, blanket data retention schemes cause a grave interference with the right to privacy, and pose a significant threat to the ability of individuals to communicate anonymously. Put together, such metadata can reveal an individual's identity, relationships, location and activity, as well as a vast array of diverse information about their web browsing activities, medical conditions, political and religious viewpoints and/or affiliation, interactions and interests. Access to and analysis of such data allows deep, intrusive and comprehensive view into a person's private life. Even seemingly innocuous transactional records, when analysed and matched with other personal data,

5 http://www.wsj.com/articles/china-to-enforce-real-name-registration-for-internet-users-1423033973

can be extremely revelatory. In a country where a data retention scheme exists, the ability to remain anonymous is seriously hindered.

Banning use of anonymisation tools

Tor (The Onion Router) is an anonymisation tool that enables individuals to access the internet in a way that shields them from surveillance or censorship by the State. Another means of remaining anonymous is the use of Virtual Private Networks (VPNs). Both such services have been banned in Iran,[6] although not effectively, and are regularly blocked in other countries.

3. General measures that limit or restrict the use of encryption

Increasingly, States are seeking to limit or restrict the use of encryption in a variety of different ways. In some countries, this takes the form of prohibiting the use of encryption; in others, it involves the banning of services that use encryption. There is also an emerging debate about whether States should be entitled to have the capacity to circumvent encryption through the use of key escrow or key recovery laws.

Restrictions on the use of encryption and encrypted services

In many countries, laws exist that ban or severely restrict the use of encryption. In Pakistan[7], for example, on December 2, 2010, a notification was sent by Pakistan's telecom regulatory authority (Pakistan Telecommunication Authority, PTA) to all cellular, WLL, and Internet service providers telling them that "use of any non-standard mode of communication like VPNs and non-standard protocols including all mechanisms by means of which communication becomes hidden or modified to the extent that it cannot be monitored, is a violation of the said Regulation." and instructed them that "if such mode of communication is required to be used by service providers themselves or for their customer, prior approval of PTA shall be obtained."[8]

PTA issued a reminder to the above notification on 21 July 2011 reiterated that: "usage of all such mechanisms including encrypted VPNS (EVPNs) which conceal communication to the extent that prohibits monitoring" is prohibited and that an approval must be sought "if such mode of communication is essentially required." It further noted that "the aforementioned directive has not been followed in true letter & spirit as EVPNs are heavily used on the Licencees Network" and that the service providers should "cooperate with the Authority on the subject."[9]

These policies negate the right of individuals to protect their digital communication through encryption. Instead encryption will only be allowed "if such mode of communication is essentially required" (e.g. for business or technical reasons.)

---

6 https://blog.torproject.org/blog/iran-blocks-tor-tor-releases-same-day-fix

7 Information on Pakistan is based on the research and analysis by Digital Rights Pakistan, a partner organisation of Privacy International.

8 See http://www.ispak.pk/Downloads/PTA_VPN_Policy.pdf

9 See http://propakistani.pk/2011/07/27/pta-wants-a-watch-on-encrypted-vpns/

Key escrow and key recovery

In an increasing effort to prevent the existence of digital communications that are immune to State interception capabilities, governments have been resurrecting key escrow and key recovery policies that were initially proposed during the "crypto wars" of the 1990s.

Key escrow is an arrangement in which the keys needed to decrypt encrypted data are held in escrow so that, under certain circumstances, an authorized third party may gain access to those keys. Key escrow policies are currently in place in Turkey. Key recovery systems are characterized by the presence of some mechanism for obtaining exceptional access to the plaintext of encrypted traffic.

Both systems seriously undermine – and perhaps even defeat – the security that encryption provides, and thus their application by national laws threatens the privacy and free expression of individuals.

Policies such as key escrow and key recovery expose individuals to a significantly increased risk of violations of their human rights by state officials, who are seeking access to encryption keys for the purpose of surveillance.

4. General measures and the right to privacy

General measures that limit anonymity or the use of encryption enable or facilitate unlawful mass surveillance, exposing individuals to a significantly increased risk of violations of their human rights by state officials.

Furthermore, measures aimed at prohibiting or limiting the use of encryption of digital communications or requiring the use of key escrow or key recovery systems are likely to violate state's obligation to protect individuals from abuses of the right to privacy by the actions of non-state actors, such as companies and criminals. Limiting people's use of encrypted communications raises significantly the risk of criminals obtaining individuals' personal information such as bank details, etc, exposing them to crimes such as theft. From a human rights perspective, these measures fail to protect individuals from abuses of their human rights to privacy by non-state actors.

Because of their wide range and disproportionate effect, general measures such as those described above do not meet the test of necessity and proportionality.

In April 2014, the Court of Justice of the European Union (hereafter "CJEU") declared invalid the European data retention directive 2006/24, which mandated the retention of data generated or processed in the provision of communications services and networks. In the joined cases brought by *Digital Rights Ireland (C-293/12) and Seitlinger and Others* (C-594/12), the Grand Chamber of the CEJU found (in paragraph 66) that the data retention directive "entails a wide-ranging and particularly serious interference with those fundamental rights in the legal order of the EU, without such an interference being precisely circumscribed by provisions to ensure that it is actually

limited to what is strictly necessary."

Privacy International knows of at least one case where a national court, applying the principles of necessity and proportionality, has struck down a law demanding real-name registration of on-line users. On 23 August 2012, the Constitutional Court of the Republic of Korea found that real name requirement imposed on large-scale portal service providers is unconstitutional. According to reports on this ruling,[10] the Court found that while the aim of the law was legitimate (namely to prevent the posting of defamatory messages) it failed the test of necessity and proportionality required to justify measures that interfere with the rights to freedom of expression and privacy.

Further the Korean Constitutional Court found that there was no evidence that the "real name system" imposed led to a significant decrease in the posting of defamatory messages. Instead, it caused the mass-flight of local users to overseas websites, and posed difficult challenges for enforcement. As a result, the Court concluded, it was not effective to attain the intended public interest.

Similar reasoning can be applied to laws and policies that prohibit or limit the use of encryption. In particular, to pass the test of necessity the measure in question needs to be effective, i.e. able to achieve the intended, legitimate result. A frequent criticism of measures that attempt to prohibit or limit encryption of digital communications is that while they would have the (unintended) result of compromising the right to privacy of many individuals, they would not achieve the objectives for which they are introduced.[11]

Furthermore, such general measures fail the test of proportionality requiring that any interference with the right to privacy needs to be the least intrusive; to be authorised on a case-by-case basis and, most importantly, that the measure in question cannot impair the essence of the right. Laws that demands real-name registration of online or SIM users and laws that prohibit or limit the use of encryption of digital communications are not only ineffective but, by their very nature, indiscriminate and disproportionate: they apply to everyone and interfere to everyone's right to privacy.

5. Targeted measures – decryption orders and the right to privacy

Several jurisdictions provide law enforcement and/or intelligence services with powers to demand decryption as means to conduct criminal investigations or to prevent the commission of criminal acts, including terrorism. 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 demand decryption.[12]

---

10 The judgment is not available in English, here is an analysis: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2187232

11 See Nine Epic Failures of Regulating Cryptography, by Cindy Cohn (https://www.eff.org/deeplinks/2014/09/nine-epic-failures-regulating-cryptography) and What David Cameron just proposed would endanger every Briton and destroy the IT industry, by Cory Doctorow (http://boingboing.net/2015/01/13/what-david-cameron-just-propos.html)

12 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

One significant concern of the laws regulating decryption orders is the over-broad and discretionary powers vested to the relevant authorities to order or carry out decryption.

In the UK, for example, the Regulation of Investigatory Powers Act 2000 (RIPA) contains provisions to order disclosure of encrypted data. The grounds for granting such orders are very broad and vague: if decryption is necessary in the interest of national security, crime prevention or detection, or the UK's economic well-being. A person who knowingly fails to comply with the order is punishable with up to two years' imprisonment.

Data on numbers of decryption requests are provided by the Chief Surveillance Commissioner's Annual Reports. During the 2013-2014 period covered in the last annual report, the National Technical Assistance Centre (NTAC) granted 76 approvals from 76 applications. The punishments meted out in cases where people were convicted for not complying with the decryption order, are not mentioned in the Commissioner's reports.[13]

Scope of and limits to decryption orders

The scope of decryption orders has a bearing on the extent of the interference with the right to privacy. In some jurisdictions, the relevant authorities have power to order decryption *or* the handing over of decryption keys.

In South Africa, the Regulation of Interception of Communications and Provision of Communication-Related Information Act establishes that a designated judge may issue a decryption order. The order may include requiring the decryption key or providing decryption assistance (defined as the assistance which is necessary to obtain access to the encrypted information specified in that decryption direction or to put that encrypted information in an intelligible form.) In the UK, under RIPA, a decryption order may require the person believed to be in possession of the decryption key to decrypt, or, in special circumstances, to provide the decryption key.

From a right to privacy perspective, an order to decrypt may potentially be less interfering than an order to disclose the encryption key. The latter would allow the authorities to review any encrypted information, as opposed to some specific (e.g. within a given time span or in between only certain individuals) communications.

Some jurisdictions contain provisions to prohibit demanding disclosure of encryption keys from criminal suspect to guarantee their right against self-incrimination.[14] This, however, does not apply to telecommunications or internet service providers, which may be ordered to decrypt communications and/or disclose encryption keys, including

---

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.

13 See 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

14 See, for example, Zimbabwe bill mentioned above. According to http://www.cryptolaw.org other countries that have similar limitations are Belgium and Netherlands.

pertaining to suspects. Other states do not make such distinction allowing a decryption order to be served to individuals suspected of having committed a crime.[15]

Decryption orders are particularly invasive of the privacy of individual's digital communications. Their potential for misuse is extremely high. This is particularly so in light of the fact that failure to comply with such orders is often considered a criminal offence.

6. Conclusions

The issues of anonymity of internet and mobile phone users and of encryption of digital communications are of significant relevance to the protection of the right to privacy and the right to freedom of expression. Recent months have seen a resurgence in governments' announcements proposing to limit the use of encryption or to impose specifications that make encryption vulnerable to state surveillance (and in consequence to non-state actors, including criminals) as a response to perceived terrorist threats.

The international human rights framework applicable to assess whether these measures violate the right to privacy and freedom of expression is well established. The International Principles on the Application of Human Rights to Communications Surveillance seek to clarify how international human rights standards apply to digital communications. They reflect, inter alia, the requirement that states respect the integrity of digital communications and systems, including by not unduly limit the security and anonymity of communications.[16]

Privacy International encourages the Special Rapporteur to develop recommendations and guidance for states, including by pointing at practices of states that do not impose restrictions on anonymity and on the use of encryption.

Building on previous recommendations by independent experts, states could be required to:

- Ensure that individuals can express themselves anonymously online and refrain from compelling the identification of users as a conditions for access to digital communications, online services or mobile use.
- Recognize that individuals should be free to protect the privacy of their digital communications by using encryption technology and refrain from adopting laws or policies that prohibit or limit the use of encryption for digital communications or compel the provision of encryption keys.
- Ensure that any targeted measures envisaged for the purposes of criminal

15 See, for example, case in the UK of one suspect convicted for failing to comply with decryption order reported here: http://www.bbc.co.uk/news/uk-25745989

16 See International Principles on the Application of Human Rights to Communications Surveillance, https://necessaryandproportionate.org

investigation or the prevention of crimes are in full compliance with the international human rights framework, respecting the principles of legality, necessity and proportionality.

Contact: Tomaso Falchetta, Legal officer, Privacy International, tomasof@privacyinternational.org