Promote Strong Encryption and Anonymity in the Digital Age
Joint Civil Society Statement

Submitted to the 29th Session of the UN Human Rights Council

June 17, 2015

The undersigned civil society organizations and independent experts work to promote human rights and press freedom online. We welcome the report of the Special Rapporteur on freedom of opinion and expression on the use of encryption and anonymity in digital communication (A/HRC/29/32), which was presented at the UN Human Rights Council on June 17.

We urge all governments to promote the use of strong encryption technologies and to protect the right to seek, receive, and impart information anonymously online. Any laws or regulations that restrict the use of encryption or anonymity online should be revised to comply with the strict three-part test the Special Rapporteur sets out in the report. We also urge information and communications technology (ICT) companies to broadly adopt encryption and other privacy-enhancing measures to safeguard the security of users.

The Internet has been enormously beneficial for the human rights movement and the work of journalists and independent civil society worldwide. Yet it has also created new risks for all users. As described in the 2014 report of the UN High Commissioner for Human Rights (A/HRC/27/37) on privacy in the digital age, digital technologies have enabled intrusive surveillance on an unprecedented scope and scale. Such surveillance can enable governments to violate professional confidentiality and identify journalistic sources, government critics, whistleblowers, or members of persecuted minority groups (such as LGBT people) and expose such individuals to retaliation. Ordinary users also face a range of online threats from overbroad state surveillance, identity thieves, and malicious actors.

As the Special Rapporteur's report recognizes, strong encryption and anonymity are fundamental for the protection of cybersecurity and human rights in the digital age. Encryption and anonymity, separately or together, "create a zone of privacy to protect opinion and belief" (para. 12). Both are critical to the enjoyment of freedoms of opinion, expression, and association, the press, the right to privacy, and other rights.

Often without knowing it, Internet users rely on the security practices of ICT companies, including support for encryption, to shield their data from online threats. Human rights defenders, lawyers, and journalists use tools to encrypt their data and communications and protect their sources and contacts from reprisals. Indeed, many of the undersigned organizations and individuals rely on encryption in their daily work to ensure the safety of staff and associates. States have a duty to protect the right to privacy, and all Internet users should be able to experiment with and adopt client-to-client encryption and anonymity tools without obstruction by government regulation or corporate policies.

Governments also have an obligation to investigate and prosecute crimes and prevent terrorist attacks. In recent years, however, some governments have sought to restrict access to strong encryption or limit anonymity online in the name of national security or public order. The Special Rapporteur's report

reiterated that any "restrictions on encryption and anonymity must be strictly limited according to principles of legality, necessity, proportionality, and legitimacy in objective" (para. 56). Any public debate on the legitimacy of specific, individualized restrictions on encryption must consider the critical role that encryption and anonymity play to protect and promote human rights, press freedom, and online security. The Special Rapporteur further states that "blanket prohibitions" on encryption and anonymity "fail to be necessary and proportionate." States should also "avoid all measures that weaken the security that individuals may enjoy online, such as backdoors, weak encryption standards and key escrows" (para 60).

Broad restrictions on the use of encryption and anonymity will not meet these criteria. For example, politicians and government officials in the US and UK have expressed concern that increased use of encryption in social media services or on mobile devices will make it more difficult to investigate terrorist threats. Some have urged companies to insert "back doors" or other vulnerabilities that would allow law enforcement to circumvent these protections.[1]

Yet as the Special Rapporteur confirms, "In the contemporary technological environment, intentionally compromising encryption, even for arguably legitimate purposes, weakens everyone's security online" (para. 8). Introducing weaknesses into digital architecture for the purposes of surveillance weakens the security of the Internet as a whole, undermining security rather than enhancing it, and conflicts with the state duty to protect the right to privacy.

We urge states to adopt and implement the report's core recommendations:

1. **States should promote and comprehensively protect strong encryption and anonymity.** National laws should recognize that individuals are free to protect the privacy of their digital communications by using encryption technology and tools that enable anonymity online (paras 57-59).

2. **States should avoid all measures that weaken the security that individuals may enjoy online.** Such measures include mandated "backdoors," weak encryption standards, key escrow arrangements, or generally forcing developers to design systems so they retain the capability to decrypt communications. Requiring companies to build vulnerabilities into secured products unavoidably and disproportionately undermines the security of all users of that product (paras 42, 60).

3. **Restrictions should be targeted on a case-specific basis and should be limited to only what is necessary and proportionate for a legitimate aim.** Court-ordered decryption may only be

[1] See James B. Comey, Director, Federal Bureau of Investigation, "Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course," Speech at the Brookings Institution, Washington, DC, October 16, 2014, http://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course; Mark Scott, "British Prime Minister Suggests Banning Some Online Messaging Apps," *New York Times*, January 12, 2015, http://bits.blogs.nytimes.com/2015/01/12/british-prime-minister-suggests-banning-some-online-messaging-apps; Robert Hannigan, "The web is a terrorist's command-and-control network of choice," *Financial Times*, November 3, 2014, http://www.ft.com/intl/cms/s/2/c89b6c58-6342-11e4-8a63-00144feabdc0.html.

permissible when it results from transparent and publicly accessible laws applied solely on a targeted case-by-case basis to individuals (i.e., not to a mass of people) and subject to judicial warrant and the protection of due process rights (paras 57, 60).

4. **States should not impose blanket prohibitions on encryption and anonymity, as they are neither necessary nor proportionate.** Such bans deprive all online users in the jurisdiction of the right to create private space for opinion and expression, without establishing that the encryption is used for unlawful ends. Some forms of regulation may, in practice, amount to a blanket prohibition—for example, requiring licenses for encryption, mandating weak technical standards for encryption, or controlling the import or export of encryption tools (paras 40-41).

5. **States should refrain from making identification of users a condition for access to online services or SIM card registration for mobile users (real-name registration). States should also refrain from limiting access to anonymity tools.** Anonymity facilitates the rights to privacy, opinion, and expression in significant ways online and states should protect it and generally not restrict the technologies that provide it. In some cases, anonymity tools may be the only mechanism for individuals to exercise a range of rights securely (paras 47-52).

The Special Rapporteur also called on the private sector to review the adequacy of their practices with regard to the responsibility of business to respect human rights. Adequate human rights due diligence for ICT companies should involve assessing threats to the security of Internet users, including from overbroad state surveillance, and developing strategies to mitigate human rights harm. The security practices of ICT companies can significantly promote or compromise encryption and anonymity (along with human rights) online. In particular, the integration of encryption into everyday Internet services and products, such that it is ubiquitous and automatic, would dramatically improve the communications security of anyone who uses the Internet.

Accordingly, we also call on ICT companies to:

1. Refrain from blocking or limiting the transmission of encrypted communications;
2. Permit anonymous communications and use of online services and refrain from imposing real-name registration requirements;
3. Deploy end-to-end encryption by default in every online service and product;
4. Support the development of other secure technologies for websites based on strong and open protocols;
5. Resist efforts by governments to require them to compromise anonymity and encryption. Also resist requests from governments to decrypt specific communications or data except in accordance with a court-order resulting from transparent and publicly accessible laws applied on a targeted case-by-case basis;
6. Effectively secure user data stored at rest through verifiable practices including encryption;
7. Maintain the security of credentials and provide robust authentication safeguards;
8. Initiate a breach notification and patching system for known, exploitable vulnerabilities; and
9. Provide user education tools on the importance of digital security best practices.

Submitted by: Human Rights Watch

Signatories:
Access
Amnesty International
Article 19
Association for Progressive Communications (APC)
Australian Privacy Foundation
Bytes for All, Pakistan
Center for Democracy & Technology (CDT)
Chaos Computer Club (CCC) e.V.
Digital Rights Foundation
Electronic Frontier Foundation
FIDH
Foundation for Internet and Civic Culture, Thailand
Global Voices Advocacy
Human Rights Watch
International Modern Media Institute (Iceland)
La Quadrature du Net
Media Matters for Democracy, Pakistan
OpenMedia.org
Panoptykon
PEN International
Privacy International
Reporters sans frontières (RSF)
SFLC.in
WITNESS
World Wide Web Foundation

Additional signatories added after submission:
American Civil Liberties Union
Bolo Bhi
Coding Rights, Brazil
Committee to Protect Journalists
Electronic Frontiers Australia