HUMAN RIGHTS WATCH

Comments Submitted to the UN Special Rapporteur on the Protection and Promotion of the Right to Freedom of Opinion and Expression

On the Use of Encryption and Anonymity in Digital Communications

February 2015

Introduction and Summary

Human Rights Watch welcomes the opportunity to submit comments on the use of encryption and anonymity in digital communications for the special rapporteur on freedom of opinion and expression's 2015 report to the Human Rights Council. Human Rights Watch is an independent global organization with a presence in more than 90 countries, investigating human rights abuses, publishing findings, and working with local partners to promote respect for and adherence to human rights obligations around the world.

An open Internet has been enormously beneficial for the human rights movement, which can share and make public information as never before. But it has also created new risks to human rights defenders, journalists, and other vulnerable communities. Digital technologies have enabled surveillance on an unprecedented scope and scale. If abused, digital surveillance can enable governments that fail to uphold human rights to identify journalistic sources, government critics, or members of persecuted minority groups and expose such individuals to retaliation.

The best way to protect at-risk communities and ordinary users alike is to promote broad use of strong encryption and protect anonymous expression online. Both are critical to the enjoyment of freedoms of expression, association, the press, the right to privacy, and other rights. Most Internet users rely on security practices of private companies to shield their communications from a range of online threats, including abusive surveillance, hackers, and cybercriminals. Human rights defenders and journalists increasingly use privacy and anonymity tools to encrypt their data and communications and shield their sources and contacts from harm.

In the name of security and countering terrorism, government officials in the US, the UK, and elsewhere have begun to argue for "back doors" into encrypted services or devices to enable surveillance of criminals and would-be terrorists. However, such proposals would actually undermine the security of all Internet users and expose more people to cybersecurity threats and cybercrime.

Human rights defenders, journalists, whistle-blowers, and other at-risk groups would be particularly vulnerable.

Governments have an obligation to investigate and prosecute crime and thwart terrorist attacks. But such measures cannot entail profound intrusions on rights that would essentially render them null. The issue isn't whether banning or weakening encryption would be useful to security agencies, but whether such a radical measure could justify undermining the privacy rights of everyone who uses or may use encrypted services to protect digital communications. Evidence provided to date suggests that this threshold has not been met.

1) Background

Documents released by former National Security Agency (NSA) contractor Edward Snowden allege that major US Internet companies have cooperated with the NSA's mass surveillance practices. The documents also reveal that the NSA and GCHQ have unilaterally sought to compromise the security of private systems and networks—many operated by major US-based technology companies—to gain access to user data and communications. These revelations have led to global loss of trust in the security and privacy of US-origin technology. To restore that trust, US companies have introduced a number of encryption measures to safeguard users against surveillance overreach over the past year. Google and Apple announced that data stored on their mobile devices would be encrypted by default, with even the company unable to decrypt locally stored data. WhatsApp has introduced end-to-end encryption and Facebook, Microsoft, and Yahoo are also expanding encryption across their services.[1]

Governments are becoming more aggressive in their efforts to subvert privacy. For example, officials in the US and UK have been very hostile to stronger privacy protections and have demanded "back door" access to encrypted services. In response to the *Charlie Hebdo* attacks in France, UK Prime Minister David Cameron has pledged to ensure that no communications will be unreachable by UK security services, suggesting that applications that do not comply with access requirements might be banned.[2] US and UK officials have accused Internet companies of creating "zones of lawlessness" and "dark places" where terrorists and criminals can flourish because some communications may not be

[1] Electronic Frontier Foundation, "EFF's Encrypt The Web Report," 2014, https://www.eff.org/encrypt-the-web-report (accessed February 12, 2015); Andy Greenberg, "Whatsapp Just Switched on End-to-End Encryption for Hundreds of Millions of Users," *Wired*, November 18, 2014, http://www.wired.com/2014/11/whatsapp-encrypted-messaging/ (accessed February 12, 2015).

[2] 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/?_r=0 (accessed February 12, 2015).

accessible to law enforcement.[3] At the same time, a number of governments worldwide have begun limiting use of strong encryption or introducing measures that restrict the ability to communicate anonymously online.

2) Legal Framework

The right to privacy and the right to freedom of expression entail a corollary right to communicate anonymously. Allowing people to speak anonymously has long been recognized as worthy of protection in order to encourage communication that might otherwise invite reprisal or stigmatization, from political pamphleteering, to anonymous tips for journalists, to blowing the whistle on improprieties in the workplace or government. Anonymity, of course, may also be sought by persons engaged in criminal activity, so it is not an absolute right. But neither may the freedom to communicate anonymously be subject to such restrictions as would eliminate the right *a priori*.

In the digital age, strong encryption is essential for the enjoyment of the right to communicate anonymously and privately. Online communications flow over Internet networks that are inherently vulnerable to covert and unwanted monitoring by state and non-state actors. Our digital data is also increasingly stored remotely with cloud service providers, whom we rely on to ensure data is not breached without authorization.

However, encryption is more than a mechanism to shield our communications and data. Encryption programs are both an expression of the code-creator and a language to convey further communications, and as such fully protected by the right to freedom of expression under Article 19 of the International Covenant on Civil and Political Rights (ICCPR) and Universal Declaration of Human Rights, just as Finnish or English or Navaho are, regardless of whether non-speakers can easily overhear and decode such conversations. And the content that users protect with encryption is no less protected under international human rights law if it is encoded than if it were spoken in Spanish or Swahili.

But unlike our many private, face-to-face conversations, a conversation on the Internet is at high risk of collection and monitoring by both government and private agents if it is conducted unencrypted.

[3] Delvin Barrett, Danny Yadron, and Daisuke Wakabayshi, “Apple and Others Encrypt Phones, Fueling Government Standoff,” *Wall Street Journal*, November 18, 2014, http://www.wsj.com/articles/apple-and-others-encrypt-phones-fueling-government-standoff-1416367801 (accessed February 12, 2015); 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 (accessed February 12, 2015); 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 (accessed February 12, 2015).

This is not a theoretical but an actual risk, as we now know following the cascading revelations of the extent of state signals intelligence efforts. Strong encryption is essential to safeguarding privacy online. And unfortunately, weak or partial encryption provides not just weak or partial protection, but no protection at all to well-equipped intelligence agencies and capable hackers. Privacy online in the twenty-first century hinges entirely on strong encryption.

Thus, any limits on strong encryption must be provided in law, proportionate, and necessary for a legitimate aim. The determination of necessity requires assessing whether the restriction is proportional in severity and intensity and the least restrictive means of securing the government interest. In addition, the ICCPR requires states to act positively to protect individuals from unjustified interference with privacy or correspondence by third parties such as companies and other non-state actors.

It follows that while there are legitimate law enforcement concerns that must be taken into account in particular situations, there is no justification for a blanket ban on the use of encryption or criminal sanction solely based on the use of encryption.

Further, a state mandate to require decryption of communications must also be justified as necessary and proportionate. A requirement of either decryption or assured decryptability for *all* online communications, including the billions that involve no suspicion of threat to public order or national security, could not be proportionate and has never been shown to be necessary. The law, including human rights law, does not view every member of society as a suspect when speaking online.

3) Necessity and Proportionality of US and UK Proposals

a. "Going Dark" vs. the "Golden Age of Surveillance"

To justify the need for back doors into strong encryption, law enforcement officials cite the threat of "going dark"[4]: a state where ubiquitous encryption frustrates law enforcement from accessing evidence needed to prosecute crime and prevent terrorism, even with lawful authority. This challenge can occur where the content of intercepted real-time communications (voice, email, chat) and stored data governments seek to access (files, stored emails) are encrypted. Officials warn that if strong encryption continues to be widely adopted, it will devastate their investigatory and intelligence gathering abilities.

[4] Valerie Caproni, General Counsel, Federal Bureau of Investigation, "Going Dark: Lawful Electronic Surveillance in the Face of New Technologies," Statement Before the House Judiciary Committee, Subcommittee on Crime, Terrorism, and Homeland Security, Washington, DC, February 17, 2011, http://www.fbi.gov/news/testimony/going-dark-lawful-electronic-surveillance-in-the-face-of-new-technologies (accessed February 12, 2015); James B. Comey, Speech at the Brookings Institution.

This argument elides the fact that the digital age has enabled massive surveillance capabilities that would have been unimaginable twenty years ago, a situation Peter Swire has termed the "golden age of surveillance."[5] For example, mobile phones and GPS devices allow police to track our movements over long periods of time with far fewer resources than previous forms of physical surveillance.[6] Social networking services, digitized address books, and messaging applications provide rich, detailed maps of our associates and contacts. All of our online activities leave digital traces that are difficult to erase or control, which are often enabled and amplified by commercial advertising networks that underlie popular applications and websites. More of our records are now digitized, from purchases to travel, and can be mined for connections and leads. Even the omission of directly personally identifying information can still enable analysis of large digital data sets to identify individuals with remarkable precision.[7]

Governments routinely access such data to investigate crime or possible terrorist threats. When they do, legal protections and processes are inadequate in many jurisdictions to ensure privacy is breached only when strictly necessary to address legitimate threats to security or public order. But it is undeniable that these technological shifts are creating new and fertile stores of investigatory material. For example, Snowden documents reveal that security agencies are already be exploiting Google advertising networks to identify and monitor individuals through their web and mobile data.[8] In 2012 alone, US mobile phone companies responded to 1.1 million requests from law enforcement for cell

[5] Peter Swire and Kenesa Ahmad, "Encryption and Globalization," *Columbia Science and Technology Law Review*, Vol. 23, 2012, November 16, 2011, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1960602 (accessed February 12, 2015). Peter Swire was the Chief Counselor for Privacy under President Bill Clinton's administration and a member of President Barack Obama's Review Group on Intelligence and Communications Technologies.

[6] Noam Cohen, "It's Tracking Your Every Move and You May Not Even Know," *New York Times*, March 26, 2011, http://www.nytimes.com/2011/03/26/business/media/26privacy.html (accessed February 12, 2015); Robert Barnes, "Supreme Court limits police use of GPS tracking," *Washington Post*, January 23, 2012, http://www.washingtonpost.com/politics/supreme-court-warrants-needed-in-gps-tracking/2012/01/23/gIQAx7qGLQ_story.html (accessed February 12, 2015); Barton Gellman and Ashkan Soltani, "NSA tracking cellphone locations worldwide, Snowden documents show," *Washington Post*, December 4, 2013, http://www.washingtonpost.com/world/national-security/nsa-tracking-cellphone-locations-worldwide-snowden-documents-show/2013/12/04/5492873a-5cf2-11e3-bc56-c6ca94801fac_story.html (accessed February 12, 2015).

[7] See Natasha Singer, "With a Few Bits of Data, Researchers Identify 'Anonymous' People," post to Bits Blog, *New York Times*, January 29, 2015, http://bits.blogs.nytimes.com/2015/01/29/with-a-few-bits-of-data-researchers-identify-anonymous-people/?_r=1 (accessed February 13, 2015); Letter from Ilya Mironov, Researcher, Microsoft Research, to Chairman Wheeler and Commissioners of the Federal Communications Commission, "Re: WC Docket No. 13-306, Public Knowledge Petition for Declaratory Ruling," February 28, 2014, http://apps.fcc.gov/ecfs/document/view?id=7521087706 (accessed February 13, 2015).

[8] Ashkan Soltani, Andrea Peterson, and Barton Gellman, "NSA uses Google cookies to pinpoint targets for hacking," *Washington Post*, December 10, 2013, http://www.washingtonpost.com/blogs/the-switch/wp/2013/12/10/nsa-uses-google-cookies-to-pinpoint-targets-for-hacking/ (accessed February 12, 2015).

location information, text messages, and other investigatory material.[9] While encryption may limit some existing surveillance capabilities, these limitations must be weighed against surveillance capabilities of governments, their power to compel the cooperation of private entities or regulate them, and their own enormous and growing prowess in analyzing digital data. Seen against these burgeoning powers, the necessity and proportionality of measures that weaken encrypted services must be questioned.

Swire poses thought experiment to help evaluate the competing narrative of "going dark" against the "golden age of surveillance":[10]

> A simple test can help the reader decide between the "going dark" and "golden age of surveillance" hypotheses. Suppose the agencies had a choice of a 1990-era package or a 2011-era package. The first package would include the wiretap authorities as they existed pre-encryption, but would lack the new techniques for location tracking, confederate identification, access to multiple databases, and data mining. The second package would match current capabilities: some encryption-related obstacles, but increased use of wiretaps, as well as the capabilities for location tracking, confederate tracking and data mining. The second package is clearly superior – the new surveillance tools assist a vast range of investigations, whereas wiretaps apply only to a small subset of key investigations. The new tools are used far more frequently and provide granular data to assist investigators.

Far from ushering in an apocalyptic "Dark Age" of security threats, the increasing use of cryptography will still leave intelligence and law enforcement with more data to work with than ever existed before online communications became ubiquitous. The Golden Age of Surveillance may lose a bit of luster, but it will hardly be ended.

b. Lessons Learned from the "Crypto Wars"

Demands from US officials for a backdoor into encrypted services are not new, but rather a re-emergence of the so-called "crypto wars": a policy debate that took place in the US in the 1990s over whether strong encryption should be broadly available. In the early days of the commercial Internet, US law enforcement agencies proposed a system where strong encryption would be allowed, but

[9] Brian X. Chen, "A Senator Plans Legislation to Narrow Authorities' Cellphone Data Requests," *New York Times*, December 9, 2013, http://www.nytimes.com/2013/12/09/technology/a-senator-plans-legislation-to-narrow-authorities-cellphone-data-requests.html (accessed February 12, 2015).

[10] Center for Democracy and Technology (CDT), "'Going Dark' Versus a 'Golden Age for Surveillance,'" November 28, 2011, https://cdt.org/blog/%E2%80%98going-dark%E2%80%99-versus-a-%E2%80%98golden-age-for-surveillance%E2%80%99/ (accessed February 12, 2015).

copies of keys used to decrypt communications would be held by the government so they could access communications with lawful process (also known as key escrow). Any secure systems would have to be technologically designed to allow such third party access.[11]

The exact contours of the crypto wars are beyond the scope of these comments and have been extensively documented elsewhere.[12] But the outcome of that debate was clear: proposals to weaken encryption through back doors or other limitations were rejected early in the Internet's history because they would have threatened security, not enhanced it. Limits on encryption were neither necessary nor proportionate to address legitimate threats and investigate crime.

No development in the intervening years has changed this conclusion. Instead, the fundamental insecurity of Internet networks has driven the demand for and adoption of strong encryption worldwide. This, in turn, enabled the Internet to flourish: without encryption, it is unlikely that the Internet would have succeeded as a global platform for commerce, finance, and a myriad of cloud-based services. It facilitated the dramatic growth of e-commerce since it allowed secure financial transactions online. Without always realizing it, individuals and even governments rely on strong encryption to protect them in many everyday activities online.

Requiring companies to design their products with a "backdoor" into secure services would be deeply regressive and threatening to security. As the security community has established, this approach would mean deliberately introducing vulnerabilities into applications and devices that could be exploited by a range of malicious actors—from abusive governments to hackers, identity thieves, and other cybercriminals. It is impossible to create a backdoor that can be guaranteed to be used only by governments acting under lawful authorization.

Security researchers have documented several case studies that illustrate this point:

- *Vodafone, Ericsson, and Greece*: In 2005, Greece discovered that an unknown third party had gained access to lawful intercept capabilities built into cell phone networks. This third party was able to monitor the prime minister's cell phone, along with a hundred other high-level officials.[13]

[11] A requirement that telecom companies build in "lawful intercept" capability into equipment already exists for traditional telecommunications networks around the world, but has not yet been extended to online applications in the US. This mandate requires telecom companies to design their equipment to be wiretappable by law enforcement agencies. See Leslie Harris and John B. Morris, Jr., "Dealing with the Devil," *Index on Censorship*, July 17, 2009, http://www.indexoncensorship.org/2009/07/dealing-with-the-devil-2/.

[12] Peter Swire and Kenesa Ahmad, "Encryption and Globalization"; Ben Adida et. al., "CALEA II: Risks of Wiretap Modifications to Endpoints," May 17, 2013, https://www.cdt.org/files/pdfs/CALEAII-techreport.pdf (accessed February 12, 2015).

[13] Vassilis Prevelakis and Diomidis Spinellis, "The Athens Affair," *IEEE Spectrum*, June 29, 2007, http://spectrum.ieee.org/telecom/security/the-athens-affair (accessed February 12, 2015).

- *Cisco*: In 2010, a security researcher documented how lawful intercept back doors built into Cisco systems contained security holes that could allow unauthorized third parties to eavesdrop on communications.[14]

- *Google and China*: In 2010, Google disclosed that it was a victim of a sophisticated cyberattack, allegedly sponsored by the Chinese government.[15] The attack targeted email accounts of Chinese human rights activists. Notably, the hackers exploited Google's lawful intercept compliance systems to gain access to information about the accounts.[16]

Hackers sell security vulnerabilities they uncover on private markets to customers seeking to exploit them, so hackers have ample financial motivation to seek out such vulnerabilities.[17] These security holes can be used by criminals to steal data for identity theft and credit card fraud.[18] Other actors, including governments or state-sponsored hackers, may seek the same access, but with the goal of targeting human rights activists or political dissidents. These security risks must be weighed against any concrete gains for law enforcement of limiting use of encryption online. Weakening encryption for any one purpose may have serious and widespread consequences that weaken the security of the Internet overall.

c. Little Evidence that Encryption has Significantly Thwarted Investigations

Officials in the US have failed to identify any significant number of cases where investigations were thwarted because of encryption to support their arguments for back doors into Internet services.

[14] Susan Landau "Moving Rapidly Backwards on Security," *Huffington Post*, October 13, 2010, http://www.huffingtonpost.com/susan-landau/moving-rapidly-backwards-_b_760667.html (accessed February 12, 2015); William Jackson, "Lawful wiretap interfaces are vulnerable to unlawful exploits," *GCN*, February 10, 2010, http://gcn.com/Articles/2010/02/15/Black-Hat-Sidebar-wiretap-interfaces.aspx (accessed February 12, 2015).

[15] Google, "A new approach to China," January 12, 2010, http://googleblog.blogspot.com/2010/01/new-approach-to-china.html (accessed February 12, 2015).

[16] Robert McMillan, "China: Google attack part of widespread spying effort," *IDG News Service*, January 13, 2010, http://www.macworld.co.uk/news/apple/china-google-attack-part-widespread-spying-effort-28293/ (accessed February 12, 2015); Julian Sanchez, "Surveillance, Security, and the Google Breach," Cato Institute, January 13, 2010, http://www.cato.org/blog/surveillance-security-google-breach (accessed February 12, 2015); Bruce Schneier, "US enables Chinese hacking of Google," *CNN*, January 23, 2010, http://www.cnn.com/2010/OPINION/01/23/schneier.google.hacking/index.html (accessed February 12, 2015).

[17] Kelly Jackson Higgins, "Hacking The Zero-Day Vulnerability Market," *Information Week – Dark Reading*, December, 9, 2013, http://www.darkreading.com/vulnerabilities---threats/hacking-the-zero-day-vulnerability-market/d/d-id/1141026 (accessed February 12, 2015).

[18] See, e.g., Nelson D. Schwartz and Eric Dash, "Thieves Found Citigroup Site an Easy Entry," *New York Times*, June 13, 2011, http://www.nytimes.com/2011/06/14/technology/14security.html?pagewanted=all (accessed February 12, 2015); Laura Shin, "What's behind the dramatic rise in medical identity theft?" *Fortune*, October 19, 2014, http://fortune.com/2014/10/19/medical-identity-theft/ (accessed February 12, 2015).

Lessons learned from earlier debates on telecom backdoor mandates are also instructive here:[19] In 1992, the FBI's Advanced Telephony Unit warned that without back door requirements for modern telecommunications infrastructure, the agency would have access to only 60 percent of wiretapped communications within 3 years (posed as a best case scenario) because of encryption.[20]

This scenario did not come to pass. Instead, the number of authorized law enforcement wiretaps in the US more than doubled in the last decade between 2003 and 2013.[21] Notably, these increases also coincide with a steady increase in the adoption and use of encryption over the last fifteen years.

In 2000, annual US government wiretap reports also began describing whether law enforcement officials encountered encryption in the course of wiretaps, and whether encryption prevented them from obtaining unencrypted text of intercepted communications. Until 2012, encryption had never thwarted law enforcement officials from accessing the plain text of communications. In 2012, out of 15 instances of encryption, they were unable to decipher only 4 cases. In 2013, 9 intercepts were not deciphered out of 41 instances of encryption. While the number of cases increased from 2012 to 2013, these numbers represent a tiny fraction of the thousands of wiretaps authorized by US courts each year (3576 authorized in 2013).[22]

Wiretap orders are seldom used to gain access to email so we cannot accurately extrapolate from this example the full picture of how encryption is affecting investigatory powers.[23] But the dire predictions, contrasted with the minimal impact of strong encryption in this context, firmly suggests caution in accepting broad-brush claims by governments of "going dark" again. Today, given the known risks of deliberately compromising encryption, governments bear the burden of providing real evidence of necessity and proportionality for any proposal to limit strong encryption.

[19] For a summary of the CALEA debates, see Laura K. Donohue, "Anglo-American Privacy and Surveillance," *Journal of Criminal Law and Criminology*, Vol. 96, Issue 3 (2006).

[20] Whitfield Diffie & Susan Landau, *Privacy on the Line: The Politics of Wiretapping and Encryption, Updated and Expanded Edition*, (London: The MIT Press, 2007) http://mitpress.mit.edu/books/privacy-line (accessed February 12, 2015) pp. 183, 205.

[21] According to government reports, increased from 1442 to 3576. United States Courts, "Wiretap Reports Archive," 1997-2012, http://www.uscourts.gov/Statistics/WiretapReports/WiretapReports_Archive.aspx (accessed February 12, 2015). There was a decrease in the number of wiretaps between 201 and 2012, but the overall trend has been upward. See also Andy Greenberg, "Rising Use of Encryption Foiled the Cops a Record 9 Times in 2013," *Wired*, January 2, 2014, http://www.wired.com/2014/07/rising-use-of-encryption-foiled-the-cops-a-record-9-times-in-2013/ (accessed February 12, 2015). This trend may be due, in part, to the declining costs of surveillance. The US's wiretap reports also underestimate government surveillance activities since they do not capture increases in use of other tools like access to stored records and location information and do not include the NSA's signals intelligence activities.

[22] Administrative Office of the US Courts, "Wiretap Report," 2013, http://www.uscourts.gov/Statistics/WiretapReports/wiretap-report-2013.aspx (accessed February 13, 2015).

[23] In addition, the wiretap report does not cover intelligence activities conducted under the Foreign Intelligence Act of 1978.

The evidence put forward by the US and UK so far has not met this burden. In a major speech in October 2014, FBI Director James Comey cited four cases to illustrate why unencrypted access to data on cell phones is critical to investigations. Yet upon closer scrutiny, cell phone data was not essential to solving or preventing the crimes in question and undecipherable encryption was not a factor.[24] Instead, these crimes were solved using more traditional investigatory techniques, with cell phone data supplementing evidence used to convict or identify the wrongdoer.

Similarly, there has been no public suggestion that encryption was a barrier to preventing the horrific *Charlie Hebdo* attack. Though not all details are known yet in the *Charlie Hebdo* attack, the perpetrators' counter-surveillance tactic apparently was not encryption, but using their wives' mobile phones.[25] Authorities had already identified the perpetrators as potential security threats, but agencies stopped monitoring them due to perceived higher priorities and resource limitations.[26]

After the murder of Fusilier Lee Rigby in Woolwich, a number of prominent UK figures expressed concern about the potential of the Internet to facilitate terrorism. However, factors other than strong encryption seemed to be at issue in that case as well. Authorities had also already identified the perpetrators as persons of interest: either Michael Adebolajo or Michael Adebowale appeared in seven different agency investigations and both had previously been under surveillance. However, agencies ceased some monitoring of them due to perceived higher priorities. Adebowale was later identified as a more serious potential threat, but delays meant that MI5's application for more intrusive surveillance was not approved in time for measures to have been in place before the attack.[27]

These facts suggest that more resources should be invested in targeted surveillance (offline and online) and sheer capacity to analyze and follow through with identified leads.

There is no doubt that more sophisticated terrorist elements will find a way to shield their communications through lawful or unlawful means—this has always been true for individuals engaged

[24] Jack Gillum and Eric Tucker, "Do cases FBI cites support encryption worries?", *Associated Press*, Oct. 17, 2014, http://bigstory.ap.org/article/e03177df2c9a4e0ebe5b584c909218bf/do-cases-fbi-cites-support-encryption-worries (accessed February 12, 2015); Dan Froomkin and Natasha Vargas-Cooper, "The FBI Director's Evidence Against Encryption Is Pathetic," *The Intercept*, October 17, 2014, https://firstlook.org/theintercept/2014/10/17/draft-two-cases-cited-fbi-dude-dumb-dumb/ (accessed February 12, 2015).

[25] Rukmini Callimachi and Jim Yardley, "From Amateur to Ruthless Jihadist in France," *New York Times*, January 17, 2015, http://www.nytimes.com/2015/01/18/world/europe/paris-terrorism-brothers-said-cherif-kouachi-charlie-hebdo.html?_r=0 (accessed February 13, 2015).

[26] Stacy Meichtry, Margaret Coker, and Julian E. Barnes, "Overburdened French Dropped Surveillance of Brothers," *Wall Street Journal*, January 9, 2015, http://www.wsj.com/articles/kouachis-links-to-yemen-overlooked-by-french-intelligence-1420837677 (accessed February 13, 2015).

[27] Intelligence and Security Committee of Parliament, "Report on the intelligence relating to the murder of Fusilier Lee Rigby (Woolwich report)," November 25, 2014, http://isc.independent.gov.uk/files/20141125_ISC_Woolwich_Report(website).pdf (accessed February 12, 2015). The Intelligence and Security Committee report concludes that the attack was likely unpreventable, even in light of delays by security and law enforcement agencies to act.

in illicit activity, whether online or offline. The issue is not whether banning or weakening encryption would be useful to security agencies, but whether it is proportional to the cost to the privacy rights of every single person who may use the Internet to communicate—among them many millions of individuals who right now use encrypted services every day. Evidence provided to date suggests that this threshold has not been met.

4) Encryption in the Service of Human Rights

Strong encryption and the ability to speak anonymously are especially important for the protection of human rights defenders, journalists, and other at-risk communities.[28]

The global Internet has been a boon for the human rights movement. Increasingly affordable, global communications tools allow human rights defenders to document abuses and disseminate their findings quickly and on a worldwide scale. Local organizations can more easily connect with international partners and policymakers through a range of digital tools to amplify the impact of their work. Social media gives independent voices a platform in places where legacy media is heavily controlled. It is not accidental that the rise in global communications has coincided with some of the strongest global efforts to end impunity for abuses.

It is no surprise that some governments see the Internet as a threat and have tried to censor and control it. Governments are building their technical capacity to use the Internet as a powerful tool for abusive surveillance and enacting new laws to expand spying powers and limit anonymity online.

For example, in December 2010, Facebook began receiving reports that Tunisian Facebook accounts had been compromised or deleted in the midst of the popular uprising in Tunisia. Facebook was a crucial platform for organizing demonstrations and disseminating videos and information that documented the violent crackdown. Facebook discovered that the government had launched a “man-in-the-middle” attack to steal Facebook passwords of Tunisian users and access their accounts. This attack was possible because Internet traffic flowing from inside Tunisia to Facebook servers abroad through the country’s centralized Internet gateways was unencrypted, allowing the ISPs to intercept passwords.[29]

[28] Dinah Pokempner, “Briefing Paper: Encryption in the Service of Human Rights,” Human Rights Watch, August 1, 1997, http://library.law.columbia.edu/urlmirror/CHRLR/32CHRLR477/dinah.htm (accessed February 13, 2015).

[29] Alexis C. Madrigal, “The Inside Story of How Facebook Responded to Tunisian Hacks,” *The Atlantic*, January 24, 2011, http://www.theatlantic.com/technology/archive/2011/01/the-inside-story-of-how-facebook-responded-to-tunisian-hacks/70044/ (accessed February 12, 2015).

Journalists are also increasingly under threat. A joint Human Rights Watch and American Civil Liberties Union (ACLU) report in July 2014 documented the insidious effects of large-scale surveillance on journalism and law in the United States. Interviews with dozens of leading journalists showed that increased surveillance is stifling reporting, especially when government tightens controls to prevent sources from leaking government information, or even talking to journalists about unclassified topics of clear public interest. Many journalists are taking extraordinary measures to protect their sources and shield them from retribution—including by using disposable burner phones or very high levels of encryption, or avoiding phones and the Internet altogether. The Guardian has also reported that the GCHQ has also intercepted emails of journalists from major media organizations in the US and UK.[30]

Strong encryption offers fundamental protection to those who seek to bring abuses to light in these circumstances. It can help protect against covert monitoring of email or web traffic. In the Tunisia example, using encrypted connections (like HTTPS) could have helped guard against such attacks, and Facebook now uses HTTPS by default for all users.[31] Tools like PGP (Pretty Good Privacy) encryption and OTR (Off-the-Record) messaging enable activists to shield email and chat. Encryption is also a means of authentication. Digital signatures use encryption to allow the recipient of an email to verify that the message was not altered by someone else on its way to their inbox. Tor, which helps Internet users browse the web anonymously, is built on encryption.

Finally, encryption for data on mobile phones and laptops can protect sensitive information—such as information that can reveal the identities of victims and sources—if a human rights researcher or journalist's equipment is seized. Because activists and defenders often use global services like Facebook, Skype, WhatsApp, and Gmail, along with mobile phones, in their daily work, pressing for robust security practices by these private companies becomes paramount to their protection.

Human Rights Watch and our partners in the field grapple with how to keep our communications secure and our contacts and associates safe every day. To serve any of these functions, the encryption tools we rely on must be effective and strong, without built-in vulnerabilities that can be exploited by abusive actors.

[30] James Ball, "GCHQ captured emails of journalists from top international media," *The Guardian*, January 19, 2015, http://www.theguardian.com/uk-news/2015/jan/19/gchq-intercepted-emails-journalists-ny-times-bbc-guardian-le-monde-reuters-nbc-washington-post (accessed February 12, 2015).

[31] Eva Galperin, "EFF Calls for Immediate Action to Defend Tunisian Activists Against Government Cyberattacks," EFF, January 11, 2012, https://www.eff.org/deeplinks/2011/01/eff-calls-immediate-action-defend-tunisian (accessed February 12, 2015).

5) Global Trends

The US and UK are not the only governments who have sought to limit availability of encryption online. Restrictions on encryption and anonymity have emerged in many forms and we provide a few examples below. We urge the special rapporteur to document and raise the human rights implications of these practices as they emerge worldwide.

- *Ethiopia*: The Ethiopian government is one of the world's largest jailer of journalists and has sought to systematically repress access to independent sources of information and the media. In 2014, six bloggers from Zone 9, a blogging collective that provides commentary on current events in Ethiopia, were charged under the abusive anti-terrorism law and the criminal code. Among the evidence the prosecution cited was digital security training the bloggers took through Tactical Technology Collective, an international nongovernmental organization (NGO) that provides activists with tools like encryption to protect their privacy and avoid reprisals. The arrest and prosecutions of the Zone 9 bloggers has had a wider chilling effect on freedom of expression in the country, elevating the level of fear among bloggers and online activists who increasingly fear posting critical commentary on Facebook or other social media platforms.[32] The government has also previously tried to block encrypted Tor traffic, which is used to communicate privately online.[33]

- *SIM card registration*: Nearly fifty countries in Africa now require real-name registration to acquire a SIM card, though enforcement may vary widely.[34]

- *Turkey*: Regulations passed in 2010 in Turkey require encryption suppliers to provide copies of encryption keys to government regulators before offering products and services to individuals or companies.

- *Voice and Chat Applications*: Over the last few years, several countries, including Saudi Arabia, the United Arab Emirates, and Pakistan, have threatened to ban voice and chat applications (Skype, WhatsApp, and Viber) unless the companies provide a back door into their encrypted services so they can be more easily intercepted.[35]

[32] Human Rights Watch, *"Journalism Is Not a Crime": Violations of Media Freedoms in Ethiopia*, January 22, 2015, http://www.hrw.org/reports/2015/01/21/journalism-not-crime (accessed February 12, 2015).

[33] "Ethiopia Introduces Deep Packet Inspection," post to Tor (Blog), May 31, 2012, https://blog.torproject.org/blog/ethiopia-introduces-deep-packet-inspection (accessed February 12, 2015).

[34] Kevin P. Donovan and Aaron K. Martin, "The Rise of African SIM Registration: The Emerging Dynamics of Regulatory Change," *First Monday*, Vol. 19, No. 2, February 3, 2014, http://firstmonday.org/ojs/index.php/fm/article/view/4351/3820 (accessed February 12, 2015).

[35] Nandagopal J. Nair, "Saudi Arabia bans messaging app Viber. WhatsApp and Skype could be next," *Quartz*, June 5, 2013, http://qz.com/91292/saudi-arabia-bans-messaging-app-viber-whatsapp-and-skype-could-be-next/ (accessed February 12, 2015); Faisal Kapadia, "Pakistani Web Rallies Against Proposed Ban on Whatsapp, Viber, and Skype," *Global Voices*, October

- *India*: India currently limits use of strong encryption by users and service providers through telecom licenses. Telecom service providers must ensure that "bulk encryption" is not deployed on their networks. Licenses also restrict individuals or service providers from using encryption with greater than a 40-bit key length (trivial to break with current computing power) without prior permission. Anyone using stronger encryption must provide the government copies of encryption keys that would allow the government to decipher communications.[36] The practical effect is that many mobile networks use no encryption, enabling anyone to intercept mobile calls.[37]

- *China*: The Chinese government is considering new regulations to require technology companies to turn over source code, build back doors into hardware and software, and use government-approved encryption algorithms that have not been peer reviewed for security (unlike other widely used encryption).[38] Over the years, the government has also sought to enforce real-name registration requirements to more easily identify social media users.[39] In February 2015, the government renewed calls to enforce these requirements, as well as shut down parody accounts by regulating online pseudonyms.[40] The government has also tried to block or interfere with Tor and encrypted web traffic and has recently stepped up blocks of Virtual Private Networks.[41] These tools use encryption to shield web traffic from third-party monitoring and to circumvent the Great Firewall.

20, 2013, http://globalvoicesonline.org/2013/10/20/pakistani-web-rallies-against-proposed-ban-on-whatsapp-viber-and-skype/ (accessed February 12, 2015).

[36] Government of India, Ministry of Communications & IT, Department of Telecommunications, "Licence Agreement for Provision of Internet Services," 2007, http://dot.gov.in/sites/default/files/internet-licence-dated%2016-10-2007_0.pdf (accessed February 12, 2015).

[37] Pranesh Prakash, "How Surveillance Works in India," post to India Ink (Blog), *New York Times*, July 10, 2013, http://india.blogs.nytimes.com/2013/07/10/how-surveillance-works-in-india/ (accessed February 12, 2015).

[38] "China: Draft Counterterrorism Law a Recipe for Abuses," Human Rights Watch news release, January 20, 2015, http://www.hrw.org/news/2015/01/20/china-draft-counterterrorism-law-recipe-abuses; See also, recently adopted banking regulations, Paul Mozur, "New Rules in China Upset Western Tech Companies," *New York Times*, January, 28, 2015, http://www.nytimes.com/2015/01/29/technology/in-china-new-cybersecurity-rules-perturb-western-tech-companies.html (accessed February 12, 2015).

[39] "China: Renewed Restrictions Send Online Chill," Human Rights Watch news release, January 4, 2013, http://www.hrw.org/news/2013/01/04/china-renewed-restrictions-send-online-chill.

[40] Josh Chin, "China Is Requiring People to Register Real Names for Some Internet Services," *Wall Street Journal*, February 4, 2015, http://www.wsj.com/articles/china-to-enforce-real-name-registration-for-internet-users-1423033973 (accessed February 12, 2015).

[41] Craig Timberg and Jla Lynn Yang, "Google is encrypting search globally. That's bad for the NSA and China's censors, " *Washington Post*, March 12, 2014, http://www.washingtonpost.com/blogs/the-switch/wp/2014/03/12/google-is-encrypting-search-worldwide-thats-bad-for-the-nsa-and-china/ (accessed February 12, 2015); Emerging Technology From the arXiv, "How China Blocks the Tor Anonymity Network," *MIT Technology Review*, April 4, 2012, http://www.technologyreview.com/view/427413/how-china-blocks-the-tor-anonymity-network/ (accessed February 12, 2015); Andrew Jacobs, "China Further Tightens Grip on the Internet," *New York Times*, January 29, 2015,

- *Russia*: In Russia, new regulations went into effect in August 2014 that would require bloggers with 3,000 or more daily readers to register with the media regulator and identify themselves publicly.[42] Also in August, separate regulations were published that would require users to provide identification to connect to public Wi-Fi networks.[43] Finally, in July 2014, media outlets reported that government officials were offering more than US $100,000 for techniques to identify anonymous users of Tor.[44]

- *Brazil*: Brazil's constitution guarantees freedom of expression, but prohibits anonymity.[45]

Conclusion

We respectfully recommend the special rapporteur:

- Reaffirm that everyone has the right to freedom of expression, which includes the right to seek, receive, and impart information anonymously, and establish that the freedom to communicate anonymously should not be restricted in a way that would limit the right *a priori*.

- Recognize that in the digital age, strong encryption and other privacy-protecting code and technology is essential for the enjoyment of the right to communicate anonymously and privately. Thus, use of strong encryption or programs such as Tor should not subject an individual to criminal sanction, nor should it be banned outright.

- Emphasize that compelled disclosure of an anonymous speaker or an individual's encrypted communications must be justified to appropriate and independent state authorities as necessary and proportionate for the protection of a legitimate state interest, on the basis of individualized suspicion of wrongdoing. Those whose communications are stripped of anonymity or decrypted must eventually be notified at the earliest moment that protection of public safety or national security allows, which is critical for access to redress and remedy where rights have been violated.

http://www.nytimes.com/2015/01/30/world/asia/china-clamps-down-still-harder-on-internet-access.html?_r=0 (accessed February 12, 2015).

[42] "Russia: Veto Law to Restrict Online Freedom," Human Rights Watch news release, April 24, 2014, http://www.hrw.org/news/2014/04/24/russia-veto-law-restrict-online-freedom.

[43] "Russia demands Internet users show ID to access public Wifi," *Reuters*, August 8, 2014, http://www.reuters.com/article/2014/08/08/us-russia-internet-idUSKBN0G81RV20140808 (accessed February 12, 2015).

[44] Alec Luhn, "Russia offers 3.9m roubles for 'research to identify users of Tor,'" *The Guardian*, July 25, 2014, http://www.theguardian.com/world/2014/jul/25/russia-research-identify-users-tor (accessed February 12, 2015). Tor is an encrypted anonymizing network used to cloak online activities.

[45] Constituicao Federal art. 5.

- Recognize that any requirement to weaken secure software or equipment, or build in back door access, interferes with freedom of expression, including the right to communicate anonymously, as well as the right to privacy. Thus, any limits on encryption must be provided in law, proportionate, and necessary for a legitimate aim.

- Emphasize that the weakening or limitation of private or anonymous communications—whether through legal restraint or technical "back doors"—can cause irreparable harm to human rights, placing at risk life, security, free expression, privacy, and other rights.

- Recognize that broad use of encryption and the ability to speak anonymously are especially important for the protection of human rights defenders, journalists, and vulnerable minority groups, all of which have been the focus of special concern of the international community in reviewing human rights protections.

- Recommend that online service providers and device and equipment makers be encouraged to design privacy and security into their products from the outset and adopt strong encryption where possible.

- Recommend that Internet service providers refrain from blocking or intercepting encrypted or anonymous Internet communications.