THE NEED FOR DEMOCRATIZATION OF DIGITAL SECURITY SOLUTIONS TO ENSURE THE RIGHT TO FREEDOM OF EXPRESSION

Joint submission of the Citizen Lab (Munk School of Global Affairs, University of Toronto) and Collin Anderson to the United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Mr. David Kaye

February 10, 2015

MUNK SCHOOL OF GLOBAL AFFAIRS
UNIVERSITY OF TORONTO

INTRODUCTION

As demonstrated by the Edward Snowden disclosures and other research, mass Internet surveillance as well as targeted digital threats[1] present serious risks to human rights, including the right to freedom of expression and the right to privacy. While governments often justify digital surveillance and censorship efforts on the basis of national security concerns and requirements of access for law enforcement purposes, these methods disproportionately impact civil society actors—NGOs, journalists, activists, and others—that engage in work considered politically sensitive. Independent of attitudes toward the United States and its "Five Eyes" surveillance partners, methods of access to communications content (through technical and non-technical means) have proliferated to states that engage in flagrant human rights violations, as well as non-state actors interested in repression of expression. Civil society is now the target of surveillance activities by a diversity of actors in the West and elsewhere, with significant repercussions for organizations' and individuals' ability to advance their missions, as well as their physical safety. The pursuit of unfettered access to individual communications and data by states has thus resulted in a divergence between interests of individual security and those of national security, as defined by governments.[2]

This submission explores the essential role of digital security tools, particularly encryption and anonymity software, in protecting the rights to freedom of expression and privacy of civil society actors, many of which are subject to politically-motivated digital surveillance and censorship.

DIGITAL SECURITY SOLUTIONS, INCLUDING ENCRYPTION AND ANONYMITY SOFTWARE, ARE NECESSARY TO ENSURE THE RIGHTS TO FREEDOM OF EXPRESSION AND PRIVACY

Encryption and anonymity tools are an important check on the widespread and inappropriate use of information controls to undermine human rights. Standardized integration and adoption of these tools in digital communications is one of the few methods available to civil society to protect itself in an environment in which digital surveillance and espionage is ongoing and largely tolerated—if not perpetrated and mandated—by governments.

Right to freedom of expression

The confidentiality and integrity assurances provided by well-implemented cryptography are necessary to enable individuals "to seek, receive and impart information and ideas."[3]

States and malicious actors have subverted the integrity of network communications to control

1 We distinguish targeted digital threats from mass surveillance, in that this type of threat is leveraged specifically against a chosen individual or entity, often for political reasons and tailored to the particular interests, systems, and operational landscape of the target. See Citizen Lab, *Communities @ Risk: Targeted Digital Threats Against Civil Society*, November 11, 2014, https://targetedthreats.net/.

2 See Ron Deibert, "The Cyber Security Syndrome," OpenCanada.org, November 25, 2014, http://opencanada.org/features/the-cyber-security-syndrome/.

3 Universal Declaration of Human Rights, Art. 19, http://www.un.org/en/documents/udhr/index.shtml#atop; International Covenant on Civil and Political Rights, Art. 19, http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx.

and monitor Internet communications. Designed with different expectations in mind, many of the fundamental Internet protocols relied heavily on trust and did not provide native mechanisms to ensure that the answers received across the Internet were legitimate and confidential. For a government, regulatory control over telecommunications activities, and often outright ownership of incumbent operators, provide ample opportunity to control connectivity on the basis of the nature of content requested by users.

Interference with and surveillance of Internet communications is reliant on the ability of intermediaries to read the content of traffic and falsify the information exchanged over a network. The anonymous exercise of the right to seek, receive and impart information is possible only with provable assurances of confidentiality that are provided through strong encryption. For example, the protocol that drives the web, HTTP, is sent and received in the clear—without concealing content sent or received between computers over the Internet. As a result, reading unencrypted HTTP traffic is trivial, and network operators can easily log what pages an individual has requested, block individual pages or whole sites, and monitor communications sent over the connection. Countless commercial and open source products exist for managing web traffic based on the content of requests as a result. Only when HTTP is paired with encryption protocols, such as Transport Layer Security (TLS) or Secure Sockets Layer (SSL), is it more difficult for intermediaries to read or block web traffic.[4]

FIGURE 1: INTERNET TRAFFIC SURVEILLANCE

UNENCRYPTED WEB TRAFFIC (OHCHR)

```
GET /EN/Issues/FreedomOpinion/Pages/CallForSubmission.aspx
HTTP/1.1
Host: www.ohchr.org
Connection: keep-alive
Accept: text/html,application/xhtml+xml,application/
xml;q=0.9,image/webp,*/*;q=0.8
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_1)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/39.0.2171.95
Safari/537.36
DNT: 1
Accept-Encoding: gzip, deflate, sdch
Accept-Language: en-US,en;q=0.8
```

4 The risks faced by users from browsing the web are not limited to the specific web page the user has requested. Many websites rely upon the use of advertising trackers which send data about the user's web browsing to third parties, in many cases without encryption and generally without the user's knowledge. Documents leaked by Edward Snowden have demonstrated that the data exposed by unencrypted ad trackers is actively exploited by the NSA and its "Five Eyes" surveillance partners. See 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/; Ryan Gallagher and Glenn Greenwald, "Canada Casts Global Surveillance Dragnet over File Downloads," The Intercept, January 28, 2015, https://firstlook.org/theintercept/2015/01/28/canada-cse-levitation-mass-surveillance/. Open Effect and the Citizen Lab have developed a tool to identify the use of unencrypted ad trackers. See Citizen Lab, "TrackerSSL highlights insecure websites and their ad trackers," January 28, 2015, https://citizenlab.org/2015/01/trackerssl/.

FIGURE 1: (CONT'D)

ENCRYPTED WEB TRAFFIC (UN)

The images in Figure 1 above demonstrate what web traffic looks like to a network intermediary, such as an operator or a surveillance agency. The website of the Office of the United Nations High Commissioner for Human Rights (OHCHR) does not support HTTPS, so therefore visitors can only view the site in an unencrypted manner. In this example of HTTP traffic, we can see that a user has requested the submission page for the Call for submission of Information from the Special Rapporteur. An Internet service provider could decide to restrict access to OHCHR in a number of ways, from filtering all requests that match the 'Host' value set to 'www.ohchr.org' (thereby limiting all access to the site), to blocking all pages pertaining to the Special Rapporteur through filtering requests that contain "FreedomOpinion."[5] This is juxtaposed against the example traffic for the United Nations site, where we can find very little information within the encrypted request (HTTPS). Encryption minimizes the amount of information that is available to any other party than the visitor and the end server, increasing the difficulty of surveillance and censorship. The Internet traffic logs from Syria disclosed by the group Telecomix reinforce that unencrypted traffic poses a threat to the exercise of fundamental human rights. Syrian authorities were able to record all the requests made by Internet users and store them indefinitely, retaining a wealth of personally identifying information, including the date and time of the request down to the second, the user's IP address, browser information and the full requested web address. An example can be found based on an actual entry from a Syrian user visiting the OHCHR site in Figure 2.

5 For example in Iran and other countries, censors allow access to Wikipedia but restrict specific pages based on their ability to distinguish requests. See "Citation Filtered: Iran's Censorship of Wikipedia," Iran Media Program (11.2013), http://www.global.asc.upenn.edu/app/uploads/2014/06/citation_filtered_1-1.pdf.

FIGURE 2: SYRIAN BLUE COAT LOGS

UNENCRYPTED WEB TRAFFIC (OHCHR)

```
2011-08-03 11:19:18 2448 0.0.0.0 - - - OBSERVED "unavailable" -  200 TCP_NC_MISS GET text/html;%20charset=utf-8 http
www.ohchr.org 80 /FR/countries/MENARegion/Pages/SYIndex.aspx - aspx "Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10_6_5; fr-fr)
AppleWebKit/533.19.4 (KHTML, like Gecko) Version/5.0.3 Safari/533.19.4" 82.137.200.45 35000 402 -
```

Similar to the confidentiality assurances of encryption, protecting the integrity and accessibility of communications over the Internet requires cryptography, and even anonymity. Network providers routinely interfere with the normal operation of routing protocols to misdirect users or block connectivity for censorship purposes, and in some cases to insert intrusion software into the client's device. This may range from restricting access through blocking connections to certain addresses associated with banned sites, to reading the content of traffic in order to determine whether the requests are made for prohibited material. Users within censoring countries require circumvention or anonymization tools, which divert traffic to a third party in order to conceal the nature of a request and avoid the scrutiny of network operators. Circumvention requires cryptography for the sake of resilience, since such systems are bound to be targeted for restrictions themselves. Additionally, anonymization tools allow individuals to conceal their identity from the recipient of the communications, who may otherwise pose its own threat of information disclosure, such as a local email provider or the comments section of a news portal.

The exercise of expression itself may require encryption and anonymization tools in order to resist takedown attempts from state and non-state actors. Tools such as Tor's Hidden Services[6] provide the ability to conceal the physical location of a host, encrypt the communications between the visitor and the site, protect against denial of service attacks, and defend against seizure of domain names.

Over the past two decades, commercial interests in security and public confidence in the then-nascent digital commerce market were widely credited for the liberalization of cryptography export controls. The arguments posed during this time in favor of increasing access to cryptography internationally provide compelling evidence that the personal use of encryption is not solely defined by contention of individual interests against those of an adversarial state. Internet companies have understood that insecurities within network infrastructure provide criminal elements with the ability to access private financial information, the same ability that presents a risk to human rights. Unlawful intervention into communications poses threats to at-risk individuals, such as violence against marginalized ethnic and religious communities, blackmail of sexual minorities, or criminal reprisal against journalists.

Right to privacy

Research on targeted digital threats against civil society organizations (CSOs) and activists has documented their ongoing targeting by advanced persistent threats (APTs)—including the same

6 "Tor: Hidden Service Protocol," Tor Project, https://www.torproject.org/docs/hidden-services.html.en.

campaigns that target the private sector and governments—and commercial spyware.[7] These operations are designed to exfiltrate sensitive data and monitor communications of the CSO, and infringe upon CSOs' right to privacy,[8] a right recognized as "an essential requirement for the realization of the right to freedom of expression."[9] CSOs, however, often lack the resources and technical expertise required to defend against or mitigate such threats.

The lack of recourse available to civil society against this form of digital compromise is largely tolerated and in some cases perpetuated by governments. For example, it has come to light that even when Western governments are aware of active digital espionage operations conducted by foreign governments against civil society, they may not attempt to intervene or notify the victims—and may seek to utilize the exfiltrated information for their own ends.[10] According to newly released Snowden documents, US, Canadian, and UK intelligence agencies discovered an ongoing hacking campaign against victims including "Chinese Human Rights Defenders," "Tibetan Pro-Democracy Personalities," and "Uighur Activists."[11] They monitored the data gleaned by the hackers for content of interest, taking no steps to prevent further compromise of the victims.[12] It is unclear why these governments took no remedial action, given that such digital intrusion and espionage activities may violate principles of international human rights law[13] and the Budapest Convention on Cybercrime,[14] as well as domestic criminal law.[15]

More action is therefore necessary to rectify imbalances in public access to digital security, enabling

7 See Citizen Lab, *Communities @ Risk: Targeted Digital Threats Against Civil Society*, November 11, 2014, https://targetedthreats.net/; Morgan Marquis-Boire, "From Bahrain with Love: FinFisher's Spy Kit Exposed?," Citizen Lab, July 25, 2012, https://citizenlab.org/2012/07/from-bahrain-with-love-finfishers-spy-kit-exposed/; Morgan Marquis-Boire, Bill Marczak, and Claudio Guarnieri, "The SmartPhone who Loved Me: FinFisher Goes Mobile?," Citizen Lab, August 29, 2012, https://citizenlab.org/2012/08/the-smartphone-who-loved-me-finfisher-goes-mobile/; Morgan Marquis-Boire, "Backdoors are Forever: Hacking Team and the Targeting of Dissent?," Citizen Lab, October 10, 2012, https://citizenlab.org/wp-content/uploads/2012/10/12-2012-backdoorsareforever.pdf; Morgan Marquis-Boire, Bill Marczak, Claudio Guarnieri, and John Scott-Railton, "You Only Click Twice: FinFisher's Global Proliferation," Citizen Lab, March 13, 2013, https://citizenlab.org/2013/03/you-only-click-twice-finfishers-global-proliferation-2/; Bill Marczak, Claudio Guarnieri, Morgan Marquis-Boire, and John Scott-Railton, "Mapping Hacking Team's Untraceable Spyware," Citizen Lab, February 17, 2014, https://citizenlab.org/2014/02/mapping-hacking-teams-untraceable-spyware/.

8 Universal Declaration of Human Rights, Art. 12, http://www.un.org/en/documents/udhr/index.shtml#atop; International Covenant on Civil and Political Rights, Art. 17, http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx.

9 U.N. 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," U.N. Doc. A/HRC/23/40, April 17, 2013, para. 24, http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf.

10 Glenn Greenwald, "Western Spy Agencies Secretly Rely on Hackers for Intel and Expertise," The Intercept, February 4, 2015, https://firstlook.org/theintercept/2015/02/04/demonize-prosecute-hackers-nsa-gchq-rely-intel-expertise/; Colin Freeze, "Canadian agencies use data stolen by foreign hackers, memo reveals," *The Globe and Mail*, February 6, 2015, http://www.theglobeandmail.com/news/national/canadian-agencies-use-data-stolen-by-foreign-hackers-memo-reveals/article22826970/.

11 Ibid.

12 Ibid.

13 Universal Declaration of Human Rights, Arts. 12 and 19, http://www.un.org/en/documents/udhr/index.shtml#atop; International Covenant on Civil and Political Rights, Arts. 17 and 19, http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx.

14 See Convention on Cybercrime, November 23, 2001, Title 1, "Offences against the confidentiality, integrity and availability of computer data and systems," http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm.

15 See, for example, the US Wiretap Act, 18 U.S.C. § 2511, available at http://www.law.cornell.edu/uscode/text/18/2511.

civil society to secure itself and prevent compromise in the first instance. The current digital threat environment requires reconsideration of the security standards applied in software and hardware used by the average person on a daily basis, to democratize security solutions such as encryption and anonymity. Encryption and anonymity may preclude the collection of meaningful data in transit that informs threat actors' targeting of these CSOs, while encryption of sensitive data at rest may also prevent threat actors that have penetrated CSO networks and devices from accessing that content. Integration of robust security as a fundamental component of all digital communications software and hardware would reduce the challenges civil society actors often encounter in improving their security posture, including resource limitations (technical expertise as well as financial constraints), spotty implementation, and user error.[16]

The appendix provides an overview of the core requirements of civil society actors when using digital mediums to engage in their work, and the utility of encryption and anonymity tools in meeting those requirements. While encryption and anonymity are not a panacea to all digital threats facing civil society, and may be overcome by particular digital attacks, they are an essential building block to enabling digital communication, increasing the resilience of civil society against digital threats, and raising the costs of attackers. Contrary to government rhetoric equating encrypted and anonymous communications with threatening activity, the use of digital security tools by civil society actors demonstrates the significant potential of such tools to advance the public interest and protect the sensitive communications of human rights activists.

STATE EFFORTS TO SUBVERT ENCRYPTION STANDARDS AND DIGITAL SECURITY TOOLS UNDERMINE THE SECURITY OF THE ONLINE ENVIRONMENT AS A WHOLE, AND WITH IT, FREE EXPRESSION AND PRIVACY

As detailed above, realization of the rights to freedom of expression and privacy is closely tied to access to digital security, particularly encryption. When digital security standards on which the public relies are undermined, freedom of expression and privacy are likewise compromised. State attempts to subvert encryption standards or other security tools constitute a direct challenge to the exercise of freedom of expression and the right to privacy online, and should be closely monitored and questioned.

Even as civil society faces an onslaught of persistent digital threats, states have used national security concerns as a basis for limiting robust digital security standards on which civil society might otherwise rely for defense. For example, in China, the draft anti-terrorism law currently under consideration includes provisions requiring telecommunications companies and Internet service providers to "report encryption plans" to relevant government departments; if "an encryption plan

16 Complicating this issue is the fact that many of the discrete encryption and anonymization tools available at present are not intuitive or user-friendly, frequently requiring training in their usage. Users are often faced with an array of different tools and methods to choose from, some proprietary and platform-specific, challenging CSOs' ability to incorporate these tools efficiently into their daily workflows.

is not reported, the relevant products or techniques must not enter use."[17] It further permits public security and state security organs investigating terrorism to "ask service providers or users to provide technical support in decryption."[18]

In North America and Europe, US President Obama and UK Prime Minister Cameron have both emphasized that encryption of communications content could stymie law enforcement and intelligence agencies investigating terrorists and criminals, and asserted that government must maintain the ability to access such data, including through cooperation from ICT companies.[19] In Prime Minister Cameron's view, "As technology develops, as the world moves on, we should try to avoid the safe havens that can otherwise be created for terrorists to talk to each other."[20] In Canada, in order to receive a license to use the wireless spectrum, mobile telecommunications companies must provide the government with the ability to monitor devices utilizing that spectrum and unscramble encrypted communications.[21] US government and other officials have also lambasted the potential of anonymity software such as Tor to shield criminals from investigation.[22] This approach significantly undervalues the utility of those same digital security tools in the protection of rights of at-risk individuals, civil society, and the public at large.

Lawful interception compliance systems introduce vulnerabilities that would otherwise be unnecessary for the provision of reliable communications. These services are not immune to their own security failures and have on occasion been used in the compromise of communications. In 2014, a backdoor and multiple vulnerabilities were found within surveillance systems provided by NICE Systems that

17 National People's Congress, Anti-Terrorism Act of the People's Republic of China (Draft), Art. 15, English translation by China Law Translate, November 8, 2014, http://chinalawtranslate.com/en/%E5%8F%8D%E6%81%90%E6%80%96%E4%B8%BB%E4%B9%89%E6%B3%95%EF%BC%88%E8%8D%89%E6%A1%88%EF%BC%89/, original Chinese text at http://www.npc.gov.cn/npc/xinwen/lfgz/flca/2014-11/03/content_1885027.htm; see also Human Rights Watch, "China: Draft Counterterrorism Law a Recipe for Abuses," January 20, 2015, http://www.hrw.org/news/2015/01/20/china-draft-counterterrorism-law-recipe-abuses.

18 Ibid., Art. 16.

19 See "Remarks by President Obama and Prime Minister Cameron of the United Kingdom in Joint Press Conference," The White House, Office of the Press Secretary, January 16, 2015, http://www.whitehouse.gov/the-press-office/2015/01/16/remarks-president-obama-and-prime-minister-cameron-united-kingdom-joint-; Danny Yadron, "Obama Sides with Cameron in Encryption Fight," *Wall Street Journal*, January 16, 2015, http://blogs.wsj.com/digits/2015/01/16/obama-sides-with-cameron-in-encryption-fight/; Rob Price, "David Cameron Wants To Ban Encryption," Business Insider, January 12, 2015, http://www.businessinsider.com/david-cameron-encryption-apple-pgp-2015-1. These remarks follow a speech by US Federal Bureau of Investigation Director James Comey in October 2014 asserting that "encryption threatens to lead all of us to a very dark place." James B. Comey, "Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?," Remarks Prepared for Delivery to the Brookings Institution, Washington, D.C., October 16, 2014, http://www.brookings.edu/~/media/events/2014/10/16%20going%20dark%20technology%20privacy%20comey%20fbi/10%2016%2014%20directors%20remarks%20for%20brookings%20institution%20as%20given.pdf.

20 "Remarks by President Obama and Prime Minister Cameron of the United Kingdom in Joint Press Conference," The White House, Office of the Press Secretary, January 16, 2015, http://www.whitehouse.gov/the-press-office/2015/01/16/remarks-president-obama-and-prime-minister-cameron-united-kingdom-joint-.

21 Colin Freeze and Rita Trichur, "Wireless firms agree to give Ottawa ability to monitor calls, phone data," *The Globe and Mail*, September 16, 2013, http://www.theglobeandmail.com/technology/mobile/out-of-sight-officials-tell-wireless-firms-to-let-them-monitor-devices-data/article14331615/; Ron Deibert, "Shutting the Backdoor: The Perils of National Security and Digital Surveillance," Strategic Studies Working Group Papers, October 2013, http://opencanada.org/wp-content/uploads/SL13CIC018-SSWGP-Deibert-v3.pdf.

22 See, e.g., Jason Koebler, "Tor and Encryption Have Created a 'Zone of Lawlessness,' Justice Department Says," Motherboard, January 27, 2015, http://motherboard.vice.com/read/tor-and-encryption-have-created-a-zone-of-lawlessness-justice-department-says.

would enable attackers to "compromise the voice recording / surveillance solution" and "listen to recorded calls without prior authentication."[23] In Greece, exploitation and access to similar devices produced by Ericsson in the Vodafone network were used by an unidentified entity in order to eavesdrop on government communications.[24]

While the US and UK governments have asserted that they will not rely on backdoors to obtain user information,[25] the Snowden disclosures have revealed a track record of such activity,[26] undermining public confidence. Implementation of backdoors or other mechanisms to subvert the confidentiality of communications necessitates not only the involvement of governments, but also the private parties involved with the development of software and hardware. The preponderance of these technologies are consumer-oriented software that are developed by private companies with substantial economic motivations that may compete with privacy interests. This set of business incentives means that governments have the ability to leverage the market power of their population by threatening to restrict market access in order to coerce international entities into compliance with questionable local measures. Although a company may be based in a country that has rigorous protections for individual rights, other jurisdictions within which it operates—the local laws and regulations of which it is compelled to abide by—may not follow international standards on protection of human rights or adhere to rule of law. Moreover, companies may not understand the context of foreign jurisdictions sufficiently to differentiate requests that meet the standards of international law from politically-motivated wiretapping. This exposure remains the same whether the vendor has enabled direct access to encrypted content or is in control of the disclosure process.

This risk has held true in practice, notably in the case of Blackberry, as the company sought to protect its market access against governments that were increasingly concerned about the communication that occurred over its encrypted communications services.[27] With respect to the concerns of civil society, little is known about the compliance regime of Blackberry other than public reports of disputes with intelligence or law enforcement agencies across the world. In 2011, the *Wall Street Journal* reported that Blackberry had "set up a facility in Mumbai to help the Indian government carry out lawful surveillance of its BlackBerry services."[28] Two years later, leaked documents disclosed that the center was handed over to Indian authorities and allowed for the interception of all emails, chats and web

23 "Backdoor in Call Monitoring, Surveillance Gear," Krebs on Security, May 14, 2014, http://krebsonsecurity.com/2014/05/backdoor-in-call-monitoring-surveillance-gear/.

24 "The Athens Affair," *IEEE Spectrum*, June 29, 2007, http://spectrum.ieee.org/telecom/security/the-athens-affair.

25 "Remarks by President Obama and Prime Minister Cameron of the United Kingdom in Joint Press Conference," The White House, Office of the Press Secretary, January 16, 2015, http://www.whitehouse.gov/the-press-office/2015/01/16/remarks-president-obama-and-prime-minister-cameron-united-kingdom-joint-.

26 See Ron Deibert, "Shutting the Backdoor: The Perils of National Security and Digital Surveillance," Strategic Studies Working Group Papers, October 2013, http://opencanada.org/wp-content/uploads/SL13CIC018-SSWGP-Deibert-v3.pdf; James Ball, Julian Borger and Glenn Greenwald, "Revealed: How US and UK spy agencies defeat internet privacy and security," *The Guardian*, September 6, 2013, http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security.

27 "Security that makes spies feel insecure," *Financial Times*, August 2, 2010, http://www.ft.com/intl/cms/s/0/7ad48c10-9e5d-11df-a5a4-00144feab49a.html#axzz3R5nCIW6I.

28 "RIM Facility Helps India in Surveillance Efforts," *Wall Street Journal*, October 28, 2011, http://www.wsj.com/articles/SB10001424052970204505304577001592335138870.

browsing for non-enterprise clients.[29] Since Blackberry has refused to issue transparency reports on requests for user information,[30] it is unclear how much access authorities have in countries such as the United Arab Emirates, Saudi Arabia, Indonesia, Russia and China, who have made similar threats and reportedly received cooperation from Blackberry.[31] It is essential that individuals are allowed to access end-to-end encryption with features such as forward secrecy and strong cryptography, without mandates for key escrow or cleartext retention. By designing a system with unnecessary access to the content of communications, Blackberry left itself vulnerable to coercion by governments with abysmal track records on human rights. This history portends the future of any communications technology that offers backdoor functionality.

THE OPPORTUNISTIC RESPONSE OF THE COMMERCIAL SPYWARE MARKET TO ENHANCED DIGITAL SECURITY STANDARDS PRESENTS ADDITIONAL RISK TO THE PROTECTION OF RIGHTS ONLINE

It is important to simultaneously consider the threat that wider deployment of encryption and anonymity software will feed the growth of the commercial market for exploitation and intrusion software. Recent conferences of ISS World, which brings together government agencies and private sector providers of "lawful intercept" and intelligence tools, have included seminars devoted to defeating the use of anonymity and encryption tools online.[32] The president of TeleStrategies, organizer of the ISS World conferences, opined in 2013 on what he viewed as the options for obtaining digital information despite widespread use of encryption:

29 "Government, BlackBerry dispute ends," *Times of India*, July 10, 2013, http://timesofindia.indiatimes.com/tech/tech-news/telecom/Government-BlackBerry-dispute-ends/articleshow/20998679.cms.

30 "BlackBerry has 'no plans' to issue transparency reports on gov't data requests," ZDNet, April 10, 2014, http://www.zdnet.com/article/blackberry-has-no-plans-to-issue-transparency-reports-on-govt-data-requests/.

31 "Use your Blackberry to map global surveillance," Committee to Protect Journalists, October 21, 2010, http://cpj.org/blog/2010/10/use-your-blackberry-to-map-global-surveillance.php.

32 See, e.g., ISS World Americas 2014 Conference Agenda, http://www.issworldtraining.com/ISS_WASH/index.htm. Seminar #7, titled "Understanding Encryption Technologies, Services Used by Criminals and Covert IT Intrusion Techniques," addressed "the encryption protocols, techniques and standards that the Internet community is adopting, and consider[ed] the implications to traditional intercept and content decoding systems - including application fingerprinting, exploitation approaches and practical considerations for law enforcement." That seminar included segments on "Special Encryptions and Anonymous Communications Services Frequently used by Criminals" ("Commercial Offerings, TOR, Proxy Servers and VPN Services, P2P Option") and "Defeating Encryption and Covert IT Intrusion Techniques" ("How Does Spyware and IT Intrusion Work, Cooperation with Certificate Authorities, Defeating GSM Encryption, Man-in-the-Middle Attack Techniques, Device Fingerprinting"). Other sessions on the conference agenda included "Off The Grid: New Technologies That Are Going Dark And How To Address Them," "Current and Future Standardization Challenges: Encryption, Network Function Virtualization, Cloud Computing and More," "Today's interception in an encrypted, social and clouded world," "Monitoring encrypted and secure communication - Extract actionable intelligence securely and efficiently to stay ahead of security threats," and "Cyber Warfare Weapons for Mobile & Desktop devices, Internet backbone, Wireless networks and SSL Decryption. Security solutions for a Non-traceable mobile and Point-to-Point Uncrackable Encryption."

> "[W]ith the proliferations of smartphones comes the proliferation of free or nearly free software to provide mobile caller privacy. Features found very attractive by criminals and terrorists. Example, TIGER TEXT: pick a message time to live in storage and kill the message after it's read and Wickr all messages (voice, text, video) are sent encrypted, set to self destruct after a given time and it's completely anonymous. Wickr promotes this service as an iPhone encryption app a three-year-old can use. An Android version is in development.
>
> Three ways come to mind. First, **use IT Intrusion** to remotely infect the criminals terminal so you can extract the content before its encrypted. Sessions given by Gamma Group, Hacking Team, VUPEN Systems and others are very popular at ISS World Programs, but these sessions are only open to LEA and IC attendees.
>
> If this is not an option, **have the telecom collect metadata** where possible. No content but you can determine who called whom, where and when because call set up data is sent unencrypted.
>
> Finally, be patient and **wait for targets to make mistakes**. Libya's Col. Muammar Gaddafi certainly knew mobile satellite phone calls can be intercepted with precise location of caller identified. He was captured and killed after he made a call from a vehicle in a caravan leaving Tripoli. He called, NATO intercepted the call with location ID and a French fighter jet attacked and stopped the caravan on route out of Tripoli. The rest is history."[33]

Additional methods for defeating digital security protocols are in continual development, rendering transparency and accountability measures in this sector essential. As encryption and other forms of secure technologies become more ubiquitous, society must also address the market for advanced spyware and other "work-arounds" that will spring up to undermine such digital security solutions—such as the intrusion software flagged by TeleStrategies. As TeleStrategies notes, however, successful law enforcement investigations may not require complete access to the content of digital communications or compromise of personal devices; other options enumerated include the lawful and limited collection of metadata and elementary investigative practices. The private sector and law enforcement, in consultation with civil society, should also explore alternative investigative tools specifically designed with safeguards in place for human rights, such as incorporating open source data analysis or technical mechanisms facilitating judicial review and oversight.

ISSUES FOR FURTHER DIALOGUE

Further dialogue between governments, civil society, and the private sector is required to bring individual security and national security interests into closer alignment. Such dialogue must consider the legitimate needs of civil society as well as the law enforcement and intelligence communities, to craft solutions that protect both individual and national security and map out an appropriate role for encryption and anonymity. Such discussions must be predicated on principles of international law, which require states to demonstrate any interference with the rights to freedom of expression and

33 Stephen E. Arnold, "Telestrategies: An Interview with Dr. Jerry Lucas," January 15, 2013, http://www.arnoldit.com/search-wizards-speak/telestrategies-2.html (emphasis added).

privacy is necessary and proportionate.[34]

Important issues to address include:

- **Government Mandates and Effect of Encryption:** What evidence supports the position of governments that they must maintain the ability to decrypt or prevent the encryption of digital communications? For example, what percentage of encrypted traffic online is considered pertinent to active law enforcement investigations? What percentage of decrypted communications have in the past actually proven useful to investigations? What methods, aside from blanket access to digital communications, are available to law enforcement in pursuing an investigation that do not rely on the compromise of online security protocols?
- **Coordination of Security Policies and Information:** What measures are in place to ensure inter-agency coordination and accountability regarding digital threats? Do government agencies responsible for intelligence, law enforcement, and diplomacy maintain consistency in their responses to known advanced persistent threats and other digital security risks affecting civil society? Can individuals and CSOs engaging with government agencies that purport to work on their behalf have confidence their concerns will be addressed across the board?
- **Principles on Limitations to Surveillance:** Can governments agree to clear principles of self-restraint concerning digital surveillance and espionage conducted against civil society?
- **Data and Encryption Key Safeguards:** Under what conditions can cryptographic keys be compelled by authorities? What safeguards exist to mediate the entrustment of data between users, private companies, and government agencies?
- **Government and Commercial Intrusion Software:** How will governments control the largely unregulated market for commercial spyware, which has been implicated in rights abuses and seeks to undermine trusted methods of digital defense? On what legal grounds are government agencies, including intelligence and law enforcement, authorized to use intrusion software?
- **Export Controls on Cryptography:** Export controls covering cryptography may inappropriately impede the provision of information security tools, especially for organizations in countries that have poor diplomatic relations with the West. Such controls may reduce the strength of encryption by necessitating a smaller key length or inclusion of backdoors, thus exposing users to harm. What regulations do governments have in place regarding the foreign availability and export of encryption software?
- **Technical Restrictions on Expression and Anonymization:** What technical restrictions on the use of circumvention or anonymization tools are mandated by governments, including through formal regulation or informal pressure on telecommunications and content companies? This would include examples such as requirements for real name registration on website comments sections or the filtering of VPNs and Tor. Conversely, does the government provide for the right of anonymity and unfettered access to information online?

34 See U.N. Human Rights Committee, General Comment No. 34, U.N. Doc. CCPR/C/GC/34, http://www.un.org/Docs/journal/asp/ws.asp?m=CCPR/C/GC/34; Johannesburg Principles on National Security, Freedom of Expression and Access to Information, http://www.article19.org/data/files/pdfs/standards/joburgprinciples.pdf; U.N. General Assembly, "Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism," U.N. Doc. A/69/397, September 23, 2014, paras. 11-12, http://www.un.org/Docs/journal/asp/ws.asp?m=A/69/397 ("Article 17 of the Covenant [ICCPR, on the right to privacy] provides that any interference with private communications must be prescribed by law, and must be a necessary and proportionate means of achieving a legitimate public policy objective. . . Merely to assert—without particularization—that mass surveillance technology can contribute to the suppression and prosecution of acts of terrorism does not provide an adequate human rights law justification for its use. The fact that something is technically feasible, and that it may sometimes yield useful intelligence, does not by itself mean that it is either reasonable or lawful (in terms of international or domestic law). . . International human rights law requires States to provide an articulable and evidence-based justification for any interference with the right to privacy, whether on an individual or mass scale.").

APPENDIX

Civil Society Requirements for Security and Availability in Digital Communications

CIVIL SOCIETY REQUIREMENT	APPLICATIONS AND ACTIVITIES	DIGITAL THREATS	UTILITY OF ENCRYPTION OR ANONYMITY IN MITIGATING RISK
Availability and integrity in access to information over the Internet	Retrieval of Content Web Browsing Information Resources and Databases	Network Interference • Restrictions of sites, content or services imposed by network intermediaries[1] • Insertion of malware into content retrieved over the Internet[2] • Misdirection and impersonation of sites or applications through manipulation of Internet routing protocols or interception of traffic[3] Network Surveillance • Monitoring of communications in transit, whether targeted or mass surveillance • Monitoring by communications platform or service provider • Local networks and intermediaries may be compromised by third parties for monitoring or interference with communications • Metadata on communications activities can be used to correlate individuals and reveal hidden behaviors Legal and Regulatory Measures • Access to particular categories of content restricted according to local requirements; restrictions enforced by content companies	Transport Encryption and Cryptographic Protocols: Security protocols that in order to conceal the content of communications either offer a layer of encryption to other types of traffic streams sent over a network or carry the content themselves. (Examples:[4] SSL, L2TP) Internet Circumvention Tools and Virtual Private Networks: Software that allows a user to bypass local restrictions, or attempts to insert malicious content into a device, by routing the traffic through an encrypted tunnel to other networks. (Examples: Psiphon,[5] VPNs, Hotspot Shield) Anonymization Services: Software that conceals the destination of traffic to network operators and masks the original source to the end destination through the use of encryption and routing the connection across other computers. (Examples: Tor, JonDo) Certificate Authorities (CAs): Certificate Authorities manage the trust relationships required to validate security credentials across the Internet. A user's operating system or browser relies on the statements of a limited number of CAs on what certificates are valid for what resource or site, in order to ensure that a client is actually communicating with who it expects. In this capacity, CAs make credible impersonation of sites more difficult even if misdirection is easy.

CIVIL SOCIETY REQUIREMENT	APPLICATIONS AND ACTIVITIES	DIGITAL THREATS	UTILITY OF ENCRYPTION OR ANONYMITY IN MITIGATING RISK
Secure communications over the Internet	Email Instant Messaging and Chat Voice over IP Telephony and Video Conferencing File Sharing Services Social Media and Networking	Compromise of Devices[6] Compromise of Account Credentials or Communications Platform Network Interference • Misdirection and impersonation of sites or applications through manipulation of Internet routing protocols or interception of traffic ("man-in-the-middle" attacks) • Local networks and intermediaries may be compromised by third parties for interference with communications Network Surveillance • Monitoring of communications in transit, whether targeted or mass surveillance • Monitoring by communications platform or service provider • Metadata on communications activities can be used to correlate individuals and reveal hidden behaviors • Local networks and intermediaries may be compromised by third parties for monitoring of communications Legal and Regulatory Measures • Compelled disclosure of information by communications platform or service providers Social Engineering[7] and Deception • Preliminary reconnaissance against targets relying on open source information or existing compromises • Impersonation of individuals of interest to target[8]	Cryptographic Software: Security software conceals the content or validates the identity of other parties in communications through encryption, not only to protect against surveillance in transit but also when data is at rest with third parties. Cryptographic Software is used in order to add an additional encryption layer on top of normal email and instant messaging communications services. (Examples: PGP/GPG, OTR) Transport Encryption and Cryptographic Protocols: Security protocols that, in order to conceal the content of communications in transit and validate end parties, either offer a layer of encryption to other types of traffic streams sent over a network or carry the content themselves. (Example: SSL) Anonymization Services: Software that conceals the destination of traffic to network operators and masks the original source to the end destination through the use of encryption and routing the connection across other computers. Anonymization services can reduce the amount of metadata available to service providers and intermediaries. (Examples: Tor, JonDo)

CIVIL SOCIETY REQUIREMENT	APPLICATIONS AND ACTIVITIES	DIGITAL THREATS	UTILITY OF ENCRYPTION OR ANONYMITY IN MITIGATING RISK
Secure communications over mobile networks	Voice Telephony SMS/Text Messaging Assorted Applications of Interest	Compromise of Devices[9] Improper Application Permissions and Data Leakage Application-Specific Keyword Censorship[10] Telecommunications Surveillance • Telephone and SMS messages are unencrypted to the telecommunications network • Impersonation of telecommunications networks or passive interception of communication by third parties, such as monitoring mobile phone broadcasts • Metadata on communications activities can be used to correlate individuals and reveal hidden behaviors Legal and Regulatory Measures • Compelled disclosure of information by communications platform or service providers Geolocation Tracking • Geolocation information, based on identifiers such as GPS and base station triangulation, can potentially be accessed by telecommunications providers as well as individual mobile applications	Secure Messaging and Voice Software*:* Tools that apply transport encryption and cryptographic protocols for text messages and voice calls, providing more secure communications, over either the normal telephony network or the mobile data channel, with less exposure to surveillance or metadata collection. May also encrypt the data stored locally on devices. (Examples: TextSecure, RedPhone, Silent Circle) Anonymization Services: Software that conceals the destination of traffic to network operators and masks the original source to the end destination through the use of encryption and routing the connection across other computers. Anonymization services can reduce the amount of metadata available to service providers and intermediaries. (Example: Orbot)
Confidential storage of data	File or Disk Encryption	Seizure of Devices or Extraction of Private Information Information Disclosure by Third Party Services Entrusted with User Data[11] Legal and Regulatory Measures • Compelled disclosure of information by communications platform or service providers	File or Disk Encryption: Encryption of files, folders or the entire content of a storage device into a format that is only readable with the correct credentials, such as a password or private key. Disk encryption can provide incidental protection for some attempts to compromise devices through preventing the direct modification of system files. (Examples: TrueCrypt, AES Crypt, PGP)

CIVIL SOCIETY REQUIREMENT	APPLICATIONS AND ACTIVITIES	DIGITAL THREATS	UTILITY OF ENCRYPTION OR ANONYMITY IN MITIGATING RISK
Reliable publication of information over the Internet	Content Publishing or File Sharing	**Compromise of Account Credentials or Communications Platform**[12] **Seizure of or Physical Attacks Against Infrastructure** • Internet names and numbers (e.g., domain names and IP addresses) can be seized by authorities • Hardware providing content and services can be confiscated or destroyed by authorities and non-state actors • Internet connectivity to targeted services can be curtailed **Digital Attacks** • Denial of service attacks[13] and computer network exploitation[14] **Legal and Regulatory Measures** • Local laws or threat of legal action limit the publication of content • Removal of content by third party hosts on basis of falsified claims, such as copyright takedown notices	**Hidden Services or "Dark Web" Networks:** Systems that conceal the destination of Internet traffic in order to hide where an online website or resource is located. Such networks generally also encrypt the contents of the traffic to every node in the network and operate in a decentralized manner in order to prevent the ability to deny access or to seize sites. Hidden services may also provide protection against denial of service attacks and compromise attempts. (Examples: Tor, I2P, Freenet) **Distributed Hash Tables (DHT)**: Decentralized technique for discovering information through querying a crowd with a specific key rather than relying on a central directory service. (Example: BitTorrent DHT)

ENDNOTES

1 In this case "intermediaries" refers primarily to network providers within the path of traffic, not only the user's Internet service provider, but also the operator that connects that network to the global Internet. Often censorship does not occur within the user's ISP but at the "international gateway"—the gatekeeper between the country's domestic network and the rest of the world. Such censorship and manipulation, and the level of resources required, can depend on access to the content of traffic through specialized "deep packet inspection," but it can also take the form of less sophisticated blocking that is achievable with any basic network equipment (such as restricting access to particular IPs).

2 Malware can be inserted into content accessed online through a variety of techniques. One method is a "drive-by download": malicious code is implanted into a website and requires a user to only visit the page in order to trigger installation of the malware. See, e.g., Steven Adair and Ned Moran, "Cyber Espionage & Strategic Web Compromises – Trusted Websites Serving Dangerous Results," Shadowserver, May 15, 2012, http://blog.shadowserver.org/2012/05/15/cyber-espionage-strategic-web-compromises-trusted-websites-serving-dangerous-results/; Citizen Lab, "Information Operations and Tibetan Rights in the Wake of Self-Immolations: Part I," March 9, 2012, https://citizenlab.org/2012/03/information-operations-and-tibetan-rights-in-the-wake-of-self-immolations-part-i/. Another technique is referred to as "network injection." Network injection relies on inserting malware into normal content retrieved over unencrypted connections, such as software updates or application installers. See, e.g., Morgan Marquis-Boire, "Schrodinger's Cat Video and the Death of Clear-Text," Citizen Lab, August 15, 2014, https://citizenlab.org/2014/08/cat-video-and-the-death-of-clear-text/.

3 For example, a Turkish telecommunication company, Türk Telekom, advertised that it owned network addresses associated with Google and other DNS providers in order to prevent users from bypassing the country's censorship of Twitter and YouTube. Collin Anderson, Philipp Winter, and Roya, "Global Network Interference Detection over the RIPE Atlas Network," FOCI 2014, http://cartography.io/foci2014.pdf.

4 Examples provided herein are for illustrative purposes only, and do not imply endorsement by Citizen Lab or Collin Anderson.

5 Disclosure: Psiphon was originally invented in the Citizen Lab and is now a private Canadian company. Ronald Deibert, Director of Citizen Lab, retains ownership shares in Psiphon. Our inclusion of Psiphon as an example is illustrative only and implies no endorsement of Psiphon.

6 Devices may be wholly compromised by Remote Access Trojans or intrusion software installed on a machine after a user triggers an exploit through a malicious link or attachment, security vulnerabilities in the software of the user's device are exploited, or the user retrieves content over the Internet in which malware is inserted. These programs typically include functionality to, *inter alia*, enable keylogging, remote loading of additional programs, exfiltration of data, and commandeering of audio and visual components.

7 See Citizen Lab, *Communities @ Risk: Targeted Digital Threats Against Civil Society*, November 11, 2014, Executive Summary p. 21-22, https://targetedthreats.net/ ("Social engineering is an attacker's method of crafting the delivery vector for the malware—typically an email—in a manner designed to entice recipients to open the infected payload. Attackers often 'spoof' the sender identity to appear as someone the target already knows and trusts; reference timely and target-specific issues and events; repurpose real content taken from other sources of interest to the target; or attempt to exploit the emotions of the target by addressing sensitive, provocative, or inflammatory subjects. Good social engineering thus requires some knowledge of a target's contacts, areas of interest, and current priorities or activities.").

8 Attackers may utilize a sender email address crafted to appear as similar to the spoofed, legitimate contact as possible. See, e.g., Citizen Lab, *Communities @ Risk: Targeted Digital Threats Against Civil Society*, November 11, 2014, Extended Analysis p. 53, https://targetedthreats.net/media/2-Extended%20Analysis-Full.pdf. Alternatively, attackers may assume an identity likely to be of interest to the target in chat sessions or other live virtual contact. For example, attackers targeting members of the Syrian opposition created Skype accounts with female avatars that "had generic but country-appropriate names and profile images, [which] would develop a rapport with the victim before sending a malicious file." Daniel Regalado, Nart Villeneuve, and John Scott Railton, "Behind the Syrian Conflict's Digital Frontlines," *FireEye*, February 2015, https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-behind-the-syria-conflict.pdf.

9 See supra n. 6. Mobile platforms are also vulnerable to malicious software. For example, Citizen Lab research has documented the use of mobile malware to target civil society organizations. See Citizen Lab, "Permission to Spy: An Analysis of Android Malware Targeting Tibetans," April 18, 2013, https://citizenlab.org/2013/04/permission-to-spy-an-analysis-of-android-malware-targeting-tibetans/.

10 See, e.g., Citizen Lab, "Asia Chats: LINE keyword filtering upgraded to include regular expressions," October 7, 2014, https://citizenlab.org/2014/10/asia-chats-line-keyword-filtering-upgraded-include-regular-expressions/; "Asia Chats: Investigating Regionally-based Keyword Censorship in LINE," November 14, 2013, https://citizenlab.org/2013/11/asia-chats-investigating-regionally-based-keyword-censorship-line/; "Asia Chats: Analyzing Information Controls and Privacy in Asian Messaging Applications," November 14, 2013, https://citizenlab.org/2013/11/asia-chats-analyzing-information-controls-privacy-asian-messaging-applications/.

11 Including cloud storage providers, service platforms and other third parties with incidental contact to devices or communications.

12 When attackers obtain a target's web publication platform account credentials, they may also acquire the ability to insert malicious code onto the target's website, exposing visitors to that website to "drive-by downloads" as detailed above, supra n. 2.

13 Denial of service attacks are attempts to overwhelm a computer or Internet connection with traffic or queries in order to disrupt its ability to serve legitimate requests from others.

14 Computer network exploitation is a general term for hacking and other attempts at unauthorized access to devices.