ACLU Submission to the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression

February 10, 2015

The American Civil Liberties Union thanks the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression for the opportunity to submit these comments on the extraordinarily important and timely topics of encryption and anonymity online.

Over the last several decades, free speech, dissent, and journalism have increasingly become digital endeavors. Much of the speech at the core of the right to free expression now takes place online. Absent protection, however, online speech is fundamentally insecure: susceptible to interception, manipulation, or outright suppression. Governments, both democratic and authoritarian, have exploited that insecurity, as have criminal hackers around the world.

Technology companies, spurred by the recent revelations about the mass surveillance made possible by weak security, have begun to offer their consumers secure communications services. Governments—including the United States, the United Kingdom, and China—have criticized those efforts.

For two reasons, discussed at length in this submission, it would be a grave mistake to accede to official demands that technology companies be required to deliberately weaken the security of their products.

First, encryption and anonymity are the modern safeguards for free expression. Without them, online communications are effectively unprotected as they traverse the Internet, vulnerable to interception and review in bulk. Encryption makes mass surveillance significantly more costly, and anonymity allows dissidents, whistleblowers, and human-rights defenders to freely express themselves, organize, and expose governmental abuse without fear of retribution.

Second, and equally importantly, strong encryption is essential to cybersecurity. Over the last few years, hackers and repressive regimes have unleashed increasingly devastating cyberattacks on companies around the world, including American companies that hold the sensitive financial, medical, and other data of millions of individuals. Strong encryption is our best defense against the growing threat of such cyberattacks.

I. Background.

A. Background on encryption.

a. How encryption works.

Modern encryption provides a way to scramble information so that only someone who knows a secret can unscramble it. In its unscrambled form, the data is known as "cleartext," and in its scrambled form, it is known as "ciphertext." The secret that allows the unscrambling is known as a "key." The ciphertext can be stored ("data at rest"), transmitted over a network ("data in transit"), or both.

The main goal of encryption is to hide the cleartext from anyone who does not have the key, including from any adversaries who may have access to the ciphertext.

b. Symmetric and asymmetric encryption.

There are two common forms of encryption relevant here: symmetric encryption and asymmetric encryption.

Symmetric encryption uses the same key to both encrypt and decrypt. It can be used by a single party: for example, to lock their own data in storage so that only they can retrieve it. Or it can be used by multiple parties: if two parties share a key, they can use symmetric encryption to send messages to each other that no one else can access without the key.[1]

In asymmetric encryption, by contrast, the key for encryption is different from the key for decryption.[2] The encryption key is usually published (the "public key"), while the decryption key is held only by one individual (the "private key"). The two keys are mathematically related (which is why data encrypted with one can be decrypted by the other), but if the scheme is properly implemented, it is thought to be effectively impossible to compute the private key in any reasonable amount of time based only on knowledge of the public key.

Because asymmetric encryption is generally slower than symmetric encryption, most schemes that use asymmetric encryption use a hybrid form. In one common hybrid, the sender symmetrically encrypts her data with a new key, and then encrypts the new key itself asymmetrically with the recipient's public key.[3] The recipient then asymmetrically decrypts the new key, and then can use that key to decrypt the data.

c. Message integrity.

Modern forms of encryption also include message integrity protection, which aims to ensure that the ciphertext (and therefore the cleartext) has not been tampered with. These message integrity mechanisms are relevant both for data at rest (to ensure that the data

[1] Symmetric encryption schemes include AES, DES, RC4, Salsa, and ChaCha.

[2] Asymmetric encryption schemes include RSA, DSA, and Elliptic Curve Cryptography.

[3] Common hybrid schemes include OpenPGP and CMS email encryption, and some forms of Transport Layer Security.

has not been corrupted or modified since last use) and data in transit (to ensure that the message has not been corrupted or modified as it passes through the network).

d. Hop-by-hop versus end-to-end encryption.

While encryption can be used to encrypt data between any two parties, some messages are routed through intermediaries before reaching their final destination. As a general matter, there are two approaches to encrypting such messages: "hop-by-hop encryption" and "end-to-end encryption."

In hop-by-hop encryption, messages are encrypted separately for each hop of their journey. Ciphertext is sent in transit between hops, but the intermediary at each hop can see the cleartext. For example, if Alice and Bob use the same email server, and Alice sends a message to Bob through that server, Alice's connection to the server will be encrypted (anyone monitoring Alice's connection to the server sees only ciphertext), and Bob's connection to the server will be encrypted (anyone monitoring Bob's connection to the server sees only ciphertext). If hop-by-encryption encryption is being used, however, then anyone with access to the server itself will be able to see the cleartext of the message.

In end-to-end encryption, only the intended (i.e., final) recipient of the message will be able to see the cleartext. All of the intermediaries will see only ciphertext. For example, Alice could encrypt her message to Bob and then send the encrypted message to their shared mailserver. With end-to-end encryption, the mailserver would see only ciphertext. This is called end-to-end encryption because only the parties on either end of the communication have access to the cleartext.

End-to-end encryption is understood to be the more secure approach. In a hop-by-hop scheme, the intermediate nodes themselves can be compromised or adversarial without the knowledge of the communicating parties, depriving them of any effective guarantee of security.

e. Uses of encryption.

Everyone who uses the Internet today uses encryption in some form.

For example, visiting any website whose URL starts with https:// establishes an encrypted connection to that website using the HTTPS protocol. Someone observing the network while a user browses a website using HTTPS should not be able to see the contents of the web page sent. (By comparison, that same observer would be able to see all traffic in cleartext during a user's visit to an http:// website.) More significantly, if a user logs in to a website using HTTPS, the encryption protects their authentication credentials (e.g., their username and password) and hides the content of their activity from anyone snooping on the network.

A large fraction of all web traffic today is encrypted.[4] For example, the following activities on the web are all typically protected by encryption:

[4] One-third of page-loads from Mozilla's Firefox browser in the past month used HTTPS: http://mzl.la/1C1YnS9.

- Checking email through a webmail service like Gmail or Yahoo.
- Online banking and other financial transactions.
- Using a social network like Facebook to talk to friends and family.
- Purchasing goods and services.
- Blogging (e.g., Wordpress) or micro-blogging (e.g., Twitter) to provide public information.
- Communicating with physicians and other medical personnel.
- Online text, audio, and video chat, such as Firefox Hello.
- Using a search engine like Google, Yahoo, or Bing.
- Browsing videos on common video-hosting sites like YouTube.

While many online newspapers and magazines have not yet switched to HTTPS websites, they are moving in that direction, with a coordinated push to finish by the end of 2015.[5]

Beyond web browsing, the use of encryption is widespread and growing. Businesses use encryption to protect their internal communications, their communications with partners, and their communications with customers.[6]

Governments use encryption to protect their internal communications and to communicate securely with other governments and the public.[7]

Network services that rely on databases of information—such as search engines—use encryption to connect to those databases to ensure confidentiality of the queries and results, as well as to ensure that no information has been tampered with as it flows across the network.[8]

---

[5] The New York Times has explained the many reasons for news organizations to move to HTTPS. Eitan Konigsburg, Rajiv Pant & Elena Kvochko, *Embracing HTTPS*, N.Y. Times, Nov. 13, 2014, http://open.blogs.nytimes.com/2014/11/13/embracing-https/.

[6] Kaspersky Lab, *Businesses Embracing Encryption to Protect Their Most Sensitive Data* (Dec. 10, 2012), http://www.kaspersky.com/about/news/business/2012/Businesses_embracing_encryption_to_protect_their_most_sensitive_data; Paul Rubens, *2014: The Year of Encryption*, BBC News, Jan. 9, 2014, http://www.bbc.com/news/business-25670315.

[7] Mem. from Clay Johnson III, Deputy Dir. of Mgmt. at the Exec. Office of the President's Office of Mgmt. & Budget, to the Heads of Dep'ts and Agencies (June 23, 2006), http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2006/m06-16.pdf (many recommendations, including: "Encrypt all data on mobile computers/devices which carry agency data unless the data is determined to be non-sensitive"); Charles H. Kennedy, *Complying with Personal ID Encryption Mandates*, Iron Mountain, http://www.ironmountain.com/Knowledge-Center/Reference-Library/View-by-Document-Type/White-Papers-Briefs/C/Complying-with-Personal-ID-Encryption-Mandates.aspx (last visited Feb. 9, 2015) (describing state government encryption of certain communications); IRS, *Encryption Requirements of IRS Publication 1075*, http://www.irs.gov/uac/Encryption-Requirements-of-IRS-Publication-1075 (last visited Feb. 9, 2015).

[8] Oracle, *Keeping Your Oracle Database Secure*, https://docs.oracle.com/cd/B28359_01/network.111/b28531/guidelines.htm (last visited Feb. 10, 2015); Martin Rakhmanov, *Network Encryption in Modern Relational Database Management Systems*, Team Shatter (Feb. 23, 2011), http://www.teamshatter.com/topics/general/

Businesses and governments use encrypted storage for sensitive data, to minimize the damage done when information is accidentally leaked.[9]

System administrators (people who maintain computers and networks) use encryption when connecting to the networks that they administer to ensure that their activity cannot be spied upon or interfered with.[10]

Journalists use encrypted email, encrypted chat, and encrypted document-submission systems to talk to sources, editors, and each other.[11]

Software engineers use encryption to communicate with each other to coordinate fixes to sensitive problems.[12]

Encryption is in widespread and rising use across all sectors of society.

B. Background on anonymity.

In the physical world, anonymity has long been made possible through practical obscurity. Pamphleteers who wanted to sow dissent without fear of retribution simply left their names off of their literature. Remaining nameless has generally been enough to provide reasonable anonymity.

In the digital world, however, it is remarkably difficult to keep one's identity hidden. Virtually every digital interaction leaves a digital trail, and those trails, especially when combined with each other, can effectively identify the user who generated them. When a user searches the internet for medical advice about cancer, for example, any number of electronic intermediaries between her computer and her search results might store her

---

team-shatter-exclusive/network-encryption-in-modern-relational-database-management-systems/; *see also* SpiderOak, *'Zero-Knowledge' Privacy* https://spideroak.com/zero-knowledge/ (last visited Feb. 9, 2015) (popular encrypted cloud storage service); Dropbox, *How Secure Is Dropbox?*, https://www.dropbox.com/help/27 (last visited Feb. 9, 2015) (popular cloud storage that uses encryption "to both transfer and store your data").

[9] In some cases, businesses are strongly encouraged to encrypt data to avoid expensive and embarrassing breach-notification requirements. *See, e.g.*, U.S. Dep't of Health and Human Servs., *Breach Notification Rule*, http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html (last visited Feb. 9, 2015). The Federal Trade Commission ("FTC") frequently cites companies for failing to protect consumers' information through the implementation of appropriately comprehensive privacy and data security programs. *See, e.g.*, FTC, *ValueClick to Pay $2.9 Million to Settle FTC Charges* (Mar. 17, 2008), http://www.ftc.gov/news-events/press-releases/2008/03/valueclick-pay-29-million-settle-ftc-charges.

[10] System administrators regularly use SSH (the Secure Shell protocol), which long ago replaced the unencrypted telnet. *See, e.g.*, Joe Gardiner, *Why Do We Use SSH Instead of Telnet?*, Cat[n] (Mar. 23, 2010), https://catn.com/2010/03/23/why-do-we-use-ssh-over-telnet/.

[11] *See, e.g.*, *infra* notes 24–30, 73, 82–83.

[12] *See, e.g.*, United States Computer Emergency Readiness Team, *Contact Us Page*, https://www.us-cert.gov/contact-us (last visited Feb. 9, 2015) (providing PGP keys for secure communication); OSS Security, *Operating System Distribution Security Contact Lists*, http://oss-security.openwall.org/wiki/mailing-lists/distros (last visited Feb. 9, 2015) (using PGP encryption to secure discussions of operation-system vulnerabilities).

query and related session information. Those bits of information might not contain her name, but they could easily be used to uniquely identify her.[13]

In other words, anonymity online is much more difficult to achieve, and it is not achieved simply by remaining nameless.[14]

Remaining anonymous online generally requires a combination of three tactics: (1) obscuring one's origin, (2) leaving as few traces as possible, and (3) ensuring that the remaining traces are not linkable to each other.

Attempting to obscure one's origin involves trying to conceal the connection between one's online activity and other personal information. Many of these connections are simple: visiting a website from a home Internet connection leaves a trail on the webserver associated with the time and network address of the connection. This information can be trivially associated with a city of residence,[15] and, when correlated with Internet Service Provider ("ISP") account records, can reveal personally identifying information. One can attempt to obscure one's origin in any number of ways, from the relatively unsophisticated (but expensive) method of using a new computer over a public Internet connection, to the more sophisticated approach of using Internet relays.

Leaving little behind involves minimizing the traces that one's online activity leaves so that, even if they would be identifying, they do not persist long enough to be reliably collected by one's adversaries. There are a number of ways to minimize one's digital footprint, such as using network services that do not retain activity logs.[16]

Avoiding linkable traces is difficult: an individual logged into a website that retrieves content from other sites (e.g., advertisements or other third-party services) often leaks personally identifying information to those third parties.[17] If those third parties provide services to other websites that the person visits, the third parties can connect the different sessions to build a profile of the user that is linked back to the identifying information. Even when specific personally identifiable information (like ISP account records) is unavailable, collections of linked traces can be used to approximate demographic

---

[13] *See* Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. Rev. 1701, 1724 (2010), *available at* http://uclalawreview.org/pdf/57-6-3.pdf (noting that the digital world is "awash in data about people" that can be used to uniquely identify them).

[14] Helen Nissenbaum, *The Meaning of Anonymity in an Information Age*, Info. Soc'y 15:141–44 (1999), *available at* http://www.nyu.edu/projects/nissenbaum/paper_anonimity.html. According to some, digital anonymity may in fact be impossible to achieve in any robust way. *See* Ohm, *supra* note 13, at 1716–31 (discussing the de-anonymization of purportedly anonymized digital information). *But see* Felix Wu, *Defining Privacy and Utility in Data Sets*, 84 U. Colo. L. Rev. 1117, 1126–29 (2013), *available at* http://lawreview.colorado.edu/wp-content/uploads/2013/11/13.-Wu_710_s.pdf.

[15] IP address (network address) geolocation: http://ipinfodb.com/ip_database.php (last visited Feb. 9, 2015).

[16] Electronic Frontier Foundation: Surveillance Self-Defense, *Choosing the VPN That's Right for You* (Oct. 17, 2014), https://ssd.eff.org/en/module/choosing-vpn-thats-right-you.

[17] Balachander Krishnamurthy & Craig E. Wills, *On the Leakage of Personally Identifiable Information via Online Social Networks* (Aug. 2009), http://www.research.att.com/~bala/papers/wosn09.pdf.

information that is often detailed enough to uniquely identify individuals.[18] One can avoid leaving linkable traces on the Internet by using throwaway computer accounts (and changing them frequently), and by carefully auditing and configuring the software, protocols, and services used.[19]

The most popular online anonymizing tool today is Tor (The Onion Router).[20] Tor assists users who wish to hide their network location by encapsulating their traffic in three layers of encryption and routing that traffic through a series of relays. Those relays do not retain activity logs, and they successively remove the layers of encryption added to the traffic at the outset, so that no single relay can connect the source and destination of the network traffic. While even this sophisticated approach does not guarantee anonymity,[21] it makes identification more costly to potential adversaries by disguising the origin of its users' traffic and by minimizing the digital footprint left behind.

One particularly noteworthy use of the Tor network is a whistleblower submission system called SecureDrop.[22] SecureDrop allows media organizations to receive documents from anonymous sources, such as government whistleblowers, while attempting to maintain their anonymity. To do so, it relies on websites that can be accessed only via the Tor network, thereby "creat[ing a] significantly more secure environment for sources to get information [to journalists] than exists through normal digital channels."[23]

A number of media organizations now offer SecureDrop submissions: Forbes, the Washington Post, the New Yorker, ProPublica, the Guardian, the Intercept, and others.[24]

---

[18] Arvind Narayanan, *Reidentification as Basic Science*, 33 Bits of Entropy Blog (May 2013), http://33bits.org/2013/05/27/reidentification-as-basic-science/.

[19] Web browsing is not the only source of privacy concerns for network users who wish to avoid identification. There is a growing understanding of the privacy and anonymity risks when using many other network protocols, particularly as more devices and systems come online. *See* Alissa Cooper et al., *Privacy Considerations for Internet Protocols* (2013), https://tools.ietf.org/html/rfc6973.

[20] Tor: Overview, https://www.torproject.org/about/overview (last visited Feb. 9, 2015). Many users of Tor rely on the "Tor Browser Bundle," which includes other anti-tracking features in addition to the Tor network anonymization.

[21] *See id.* (acknowledging the difficulty of providing anonymity online).

[22] Freedom of the Press Found., *SecureDrop*, https://freedom.press/securedrop (last visited Feb. 7, 2015). *See generally DeadDrop / StrongBox Security Assessment*, Univ. of Wash. Dep't of Comp. Sci. & Eng'g (Aug. 11, 2013), http://www.czeskis.com/research/pubs/UW-CSE-13-08-02.PDF (detailed technical discussion of SecureDrop).

[23] *Id.*; *see also id.* (". . . but there are always risks."). Another particularly noteworthy application of the Tor network is Tails (The Amnesiac Incognito Live System), which is an ephemeral operating system that runs from a DVD, USB drive, or SD card and which forces all of its internet connections through the Tor network. *See* Tails, https://tails.boum.org/; *see also* Freedom of the Press Found., *Tails*, https://freedom.press/organization/tails (describing uses of Tails by journalists and human-rights defenders).

[24] Forbes SafeSource, https://safesource.forbes.com (last visited Feb. 9, 2015) ("SafeSource is based on the open-source, security-audited architecture known as SecureDrop . . . ."); Washington Post SecureDrop, https://ssl.washingtonpost.com/securedrop (last visited Feb. 9, 2015); New Yorker Strongbox, http://projects.newyorker.com/strongbox/ (last visited Feb. 9, 2015) ("The New Yorker Strongbox is powered by SecureDrop."); ProPublica SecureDrop, https://securedrop.propublica.org (last visited Feb. 9, 2015); Guardian SecureDrop, https://securedrop.theguardian.com (last visited Feb. 9, 2015); Intercept SecureDrop, https://firstlook.org/theintercept/

II. Strong encryption is essential to cybersecurity.

Absent encryption, all networked communications are fundamentally insecure. Anyone with access to the servers that store our data or the networks that transmit it would be able to intercept any communication, tamper with it, or delete it altogether. That fact poses a critical threat to the security of us all in our use of the Internet to store and send our most sensitive medical, financial, and otherwise private information.

Modern encryption is an answer to that threat. Properly implemented, it ensures that journalists, dissidents, human-rights defenders, and others can safely use the Internet to freely express their ideas and to report on governmental abuses. It promises, too, to protect all of our digital assets from the increasingly frequent and costly cyberattacks that have exposed so much sensitive information to malicious hackers or oppressive regimes.

As the administration of President Barack Obama wrote in 2011:

> [N]etworked systems must retain our trust. Users need to have confidence that their data will be secure in transit and storage, as well as reliable in delivery.[25]

The risks of weak security can range from annoyances, like spurious calendar appointments[26] or modified road signs[27]; to serious privacy breaches, like leaks of email archives,[28] user information,[29] or health records[30]; to grave disasters, like failures of power systems,[31] engineering infrastructure,[32] civilian and government communications,[33] or

---

securedrop (last visited Feb. 9, 2015); Freedom of the Press Found., *Official SecureDrop Directory*, https://freedom.press/securedrop/directory (last visited Feb. 9, 2015).

[25] White House, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World* (May 2011), http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

[26] Brian Krebs, *Spammers Using Google, Outlook Calendars to Get Your Attention*, Wash. Post, Apr. 10, 2008, http://voices.washingtonpost.com/securityfix/2008/04/spammers_scheduling_google_out.html.

[27] Jesus Diaz, *How to Hack the New Road Signs*, Gizmodo (Oct. 10, 2011), http://gizmodo.com/5848247/how-to-hack-the-new-road-signs.

[28] Mark Seal, *An Exclusive Look at Sony's Hacking Saga*, Vanity Fair, Mar. 2015, http://www.vanityfair.com/hollywood/2015/02/sony-hacking-seth-rogen-evan-goldberg; Raphael Satter & Cassandra Vinograd, *Stratfor Emails Published by WikiLeaks Reveal Private Intelligence*, Huffington Post (Feb. 27, 2012), http://www.huffingtonpost.com/2012/02/27/stratfor-emails-wikileaks_n_1304501.html.

[29] Jon Skillings, *Overexposed: Snapchat User Info from 4.6M Accounts*, CNET (Jan. 1, 2014), http://www.cnet.com/news/overexposed-snapchat-user-info-from-4-6m-accounts/; Graham Cluley, *United Nations Hacked—Email Addresses and Passwords Leaked*, Naked Security (Nov. 29, 2011), https://nakedsecurity.sophos.com/2011/11/29/united-nations-hacked-email-addresses-and-passwords-leaked/.

[30] Reed Abelson & Matthew Goldstein, *Millions of Anthem Customers Targeted in Cyberattack*, N.Y. Times, Feb. 5, 2015, http://www.nytimes.com/2015/02/05/business/hackers-breached-data-of-millions-insurer-says.html; Ryan Singel, *Probe Targets Archives' Handling of Data on 70 Million Vets*, Wired, Oct. 1, 2009, http://www.wired.com/2009/10/probe-targets-archives-handling-of-data-on-70-million-vets.

[31] Bill Sweet, *U.S. Power System Security*, IEEE Spectrum (Mar. 26, 2010), http://spectrum.ieee.org/energywise/energy/the-smarter-grid/us-power-system-security.

military systems.[34] These failures can have serious consequences for governments, corporations, journalists, medical providers, law firms, and private citizens alike.

A. Encryption is a basic requirement for security in the digital age.

Cybersecurity broadly encompasses the integrity and confidentiality of stored information and of information in transit over communications networks. Modern, strong encryption is one of the only mechanisms we have to protect these information systems and the social structures that rely on them.

That encryption is essential to this task is well understood within the technical community. Nearly two decades ago, the Internet Architecture Board ("IAB") and the Internet Engineering Steering Group ("IESG") wrote:

> The IAB and IESG would like to encourage policies that allow ready access to uniform strong cryptographic technology for all Internet users in all countries. . . . The Internet is becoming the predominant vehicle for electronic commerce and information exchange. It is essential that the support structure for these activities can be trusted.[35]

According to a recent news story, a U.S. government report from 2009 explained the importance of encryption to cybersecurity: "A secret US cybersecurity report warned that government and private computers were being left vulnerable to online attacks from Russia, China and criminal gangs because encryption technologies were not being implemented fast enough."[36]

More recently, a review group hand-selected by President Obama echoed that view, recommending that the U.S. government

> take additional steps to promote security, by (1) fully supporting and not undermining efforts to create encryption standards; (2) making clear that it will not in any way subvert, undermine, weaken, or make vulnerable generally available commercial encryption; and (3) supporting efforts to

---

[32] Fahmida Y. Rashid, *Military Database of U.S. Dams Compromised by Attackers: Report*, Security Wk. (May 1, 2013), http://www.securityweek.com/military-database-us-dams-compromised-attackers-report; *60 Minutes: Stuxnet: Computer Worm Opens New Era of Warfare* (CBS News television broadcast June 4, 2012, http://www.cbsnews.com/news/stuxnet-computer-worm-opens-new-era-of-warfare-04-06-2012/.

[33] Mark Landler & John Markoff, *Digital Fears Emerge After Data Siege in Estonia*, N.Y. Times, May 29, 2007, http://www.nytimes.com/2007/05/29/technology/29estonia.html.

[34] Ellen Nakashima, *Defense Official Discloses Cyberattack*, Wash. Post, Aug. 24, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/08/24/AR2010082406495.html.

[35] IAB and IESG Statement on Cryptographic Tech. & the Internet (Aug. 1996), https://tools.ietf.org/html/rfc1984.

[36] James Ball, *Secret US Cybersecurity Report: Encryption Vital to Protect Private Data*, Guardian, Jan. 15, 2015, http://www.theguardian.com/us-news/2015/jan/15/-sp-secret-us-cybersecurity-report-encryption-protect-data-cameron-paris-attacks.

> encourage the greater use of encryption technology for data in transit, at rest, in the cloud, and in storage.[37]

These recent pronouncements have precedent in the U.S. government's long history of funding and supporting encryption projects that provide secure communications to dissidents and human-rights defenders.[38] This support has helped to create encryption and anonymity tools such as Tor[39] and to produce the powerful end-to-end encryption that is being deployed in popular tools like WhatsApp.[40]

The European Parliament and the Council of Europe also recognize the importance of encryption in defending against surveillance,[41] as has the United Nations and, in particular, the Special Rapporteur for Freedom of Opinion and Expression, Mr. Frank La Rue.[42]

Governments, companies, journalists, and private citizens alike are rapidly adopting strong encryption in response to the uniform understanding of the importance of encryption to security.[43]

---

[37] President's Review Grp. on Intelligence & Commc'ns Techs., *Liberty and Security in a Changing World* 22 (2013), http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

[38] *See, e.g.*, About the Program, Open Technology Fund, https://www.opentechfund.org/about (noting creation of the Open Technology Fund ("OTF") with U.S. government funding, and OTF's goal of securing access to the Internet with "encryption tools").

[39] Roger Dingledine et al., Naval Research Lab., *Tor: The Second-Generation Onion Router* (2004), *available at* http://www.nrl.navy.mil/itd/chacs/sites/www.nrl.navy.mil.itd.chacs/files/pdfs/Dingledine%20etal2004.pdf; *see also* Tor: Overview, https://www.torproject.org/.

[40] WhatsApp is adopting encryption mechanisms developed by Open Whisper Systems, which is funded by the Open Technology Fund. *See* Projects, Open Technology Fund, https://www.opentechfund.org/projects; *Open Whisper Systems Partners with WhatsApp to Provide End-to-End Encryption*, Open Whisper Systems Blog (Nov. 18, 2014), https://whispersystems.org/blog/whatsapp/; *see also* White House, National Security Strategy 21 (Feb. 2015), http://www.whitehouse.gov/sites/default/files/docs/2015_national_security_strategy_2.pdf ("The United States is countering this trend by providing direct support for civil society and by advocating rollback of laws and regulations that undermine citizens' rights. We are also supporting technologies that expand access to information, enable freedom of expression, and connect civil society groups in this fight around the world.").

[41] European Parliamentary Research Serv., PE 527.409, *Mass Surveillance: Part 1—Risks and Opportunities Raised by the Current Generation of Network Services and Applications* 2, 15 (2014), *available at* http://www.europarl.europa.eu/RegData/etudes/STUD/2015/527409/EPRS_STU(2015)527409_REV1_EN.pdf; European Parliamentary Research Serv., PE 527.410, *Mass Surveillance: Part 2—Technology Foresight, Options for Longer Term Security and Privacy Improvements* 11 (2014), *available at* http://www.europarl.europa.eu/RegData/etudes/STUD/2015/527410/EPRS_STU(2015)527410_REV1_EN.pdf; Rapporteur, Comm. on Legal Affairs & Human Rights, Council of Europe, *Mass Surveillance*, ¶¶ 63–69, 119–20 (2015) (by Pieter Omtzigt), *available at* http://website-pace.net/documents/19838/1085720/20150126-MassSurveillance-EN.pdf/df5aae25-6cfe-450a-92a6-e903af10b7a2.

[42] Special Rapporteur on the Promotion & Protection of the Right to Freedom of Opinion & Expression, *Report on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, Human Rights Council, ¶ 71, U.N. Doc. A/HRC/23/40 (Apr. 17, 2013) (by Frank La Rue) [hereinafter La Rue *Report*], *available at* http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf.

[43] *See, e.g.*, Eric Mill, U.S. General Servs. Admin., *Why We Use HTTPS for Every .gov We Make*, 18F Blog (Nov. 13, 2014), https://18f.gsa.gov/2014/11/13/why-we-use-https-in-every-gov-website-we-make/; Adam Langley, *Overclocking SSL*, ImperialViolet Blog (June 25, 2010), https://www.imperialviolet.org/2010/06/25/overclocking-

B. Government proposals to weaken encryption would make everyone's communications and private data less secure.

We have recently heard calls from national governments, including the United States,[44] United Kingdom,[45] and China,[46] demanding "backdoor" mechanisms that would guarantee government access to encrypted communications and data. These mechanisms would likely rely either on key escrow (where the cryptographic keys in any system are duplicated and stored with a third party who can turn them over to law enforcement) or hop-by-hop encryption (where a communications intermediary is able to see the cleartext of any communication and hand it over to law enforcement). Some governments have also tried to weaken cryptographic mechanisms in secret. For example, it is now widely reported that the U.S. National Security Agency introduced, standardized, and encouraged private industry to deploy cryptographic technology that was deliberately weakened.[47]

If adopted, these backdoor measures would undermine the security of the Internet for everyone. Creating backdoor channels of any sort, whether for lawful interception or otherwise, weakens the cybersecurity of the system as a whole. Backdoors are points of weakness that can be exploited not only by law-abiding governments but by rival nation states, repressive regimes, criminals, and others.

The risk of such exploitation is not theoretical. For example, in 2004 and 2005, the mobile phones of dozens of members of the Greek government were spied upon by an unknown adversary who exploited a backdoor intended for law enforcement.[48] And in 2009, Google

---

ssl.html; Brian Naylor, *Apple Says iOS Encryption Protects Privacy; FBI Raises Crime Fears*, NPR, Oct. 8, 2014, http://www.npr.org/blogs/alltechconsidered/2014/10/08/354598527/apple-says-ios-encryption-protects-privacy-fbi-raises-crime-fears; Elec. Frontier Found., HTTPS Everywhere, https://www.eff.org/https-everywhere; Open Whisper Systems, About, https://whispersystems.org/about/; Encrypt All The Things, https://encryptallthethings.net/.

[44] Craig Timberg & Greg Miller, *FBI Blasts Apple, Google for Locking Police Out of Phones*, Wash. Post, Sept. 25, 2014, http://www.washingtonpost.com/business/technology/2014/09/25/68c4e08e-4344-11e4-9a15-137aa0153527_story.html; James B. Comey, Dir. of FBI, Remarks at the Brookings Institution (Oct. 16, 2014), http://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course.

[45] *Cameron to Push Obama on 'Backdoor' Encryption Access for Cyber Spies*, Globe & Mail, Jan. 16, 2015, http://www.theglobeandmail.com/technology/tech-news/cameron-to-push-obama-on-backdoor-encryption-access-for-cyber-spies/article22485748/.

[46] Paul Mozur, *New Rules in China Upset Western Tech Companies*, N.Y. Times, Jan. 28, 2015, http://www.nytimes.com/2015/01/29/technology/in-china-new-cybersecurity-rules-perturb-western-tech-companies.html.

[47] Rapporteur, *Mass Surveillance*, *supra* note 41, ¶¶ 64–65, 68–69; Joseph Menn, *Secret Contract Tied NSA and Security Industry Pioneer*, Reuters, Dec. 20, 2013, http://www.reuters.com/article/2013/12/20/us-usa-security-rsa-idUSBRE9BJ1C220131220; Matthew Green, *The Many Flaws of DUAL_EC_DRBG*, Cryptography Engineering Blog (Sept. 18, 2013), http://blog.cryptographyengineering.com/2013/09/the-many-flaws-of-dualecdrbg.html.

[48] Vassilis Prevelakis & Diomidis Spinellis, *The Athens Affair*, IEEE Spectrum (June 29, 2007), http://spectrum.ieee.org/telecom/security/the-athens-affair.

servers were breached by Chinese hackers who gained access to a sensitive database with years' worth of information about the U.S. government's surveillance targets.[49]

From an engineering perspective, this risk is also well known. The IAB and IESG commented on deliberately weakened cryptosystems:

> Systems that are breakable by one country will be breakable by others, possibly unfriendly ones. Large corporations and even criminal enterprises have the resources to break many cryptosystems.[50]

And the Internet Engineering Task Force ("IETF") has described the tradeoff clearly:

> We cannot defend against the most nefarious actors while allowing monitoring by other actors no matter how benevolent some might consider them to be, since the actions required of the attacker are indistinguishable from other attacks.[51]

The security of everyone, our information systems, and our private data, all depend today on the continued existence, development, and wide deployment of strong end-to-end encryption mechanisms.

C. Surveillance v. security.

High-ranking U.S. and U.K. officials have warned that widespread use of encryption will make surveillance harder. There is an unavoidable respect in which that might be true: securing our communications with encryption necessarily secures them against everyone—against democracies, oppressive regimes, and criminal hackers alike. But the debate over encryption is simultaneously about much less and much more: much less because encryption poses nothing like the existential threat officials have cautioned, and much more because the proposals offered thus far would not simply trade a little security for a little surveillance. Rather, they would wholly subvert our security by sacrificing our best defense against the growing threat of cyberattack: strong encryption. In other words, the security that encryption provides is not a problem in need of a solution, but rather the solution (or at least a critical part of one) to a looming disaster. This is so for several reasons.

First, law-enforcement authorities are now operating in a "golden age of surveillance."[52] While technology promises to secure the content of our communications, it has at the same time made our lives more transparent to law enforcement than ever before. With little

---

[49] Ellen Nakashima, *Chinese Hackers Who Breached Google Gained Access to Sensitive Data, U.S. Officials Say*, Wash. Post, May 20, 2013, http://www.washingtonpost.com/world/national-security/chinese-hackers-who-breached-google-gained-access-to-sensitive-data-us-officials-say/2013/05/20/51330428-be34-11e2-89c9-3be8095fe767_story.html.

[50] *See* IAB and IESG Statement, *supra* note 35.

[51] IETF: Pervasive monitoring is an attack: https://tools.ietf.org/html/rfc7258 (last visited Feb. 9, 2015).

[52] Peter Swire, *'Going Dark' Versus a 'Golden Age for Surveillance,'* Ctr. for Dem. & Tech. (Nov. 28, 2011), https://cdt.org/blog/%E2%80%98going-dark%E2%80%99-versus-a-%E2%80%98golden-age-for-surveillance%E2%80%99/.

effort, police forces can now determine a suspect's exact location over a period of months, his every confederate, and every other digital fingerprint he leaves when interacting with technology. Federal, state, and local law-enforcement authorities in the United States have eagerly embraced these unprecedented surveillance capabilities.[53] The security that encryption provides must be judged not in a vacuum, but in the context of the pervasive surveillance enabled by our increasingly digitized lives.

Second, prohibiting technology companies from offering backdoor-free communication services would do little to aid in the most important investigations. Sophisticated criminals and terrorists already have access to a wide array of encryption technologies that do not rely on intermediaries like Apple or Google.[54] The primary effect of preventing Apple and Google from offering their own backdoor-free encryption, therefore, would only be to make *everyone else* less secure.

Third, for those who do pose serious threats, governments often have other tools at their disposal. For example, where the NSA cannot crack the encryption used by its targets, it circumvents it in other ways.[55] The FBI, too, has tools that allow it to remotely hack into its targets' computers and surreptitiously log passwords or gain access to private data.[56] Those methods generally have the virtue of being targeted in nature. In other words, they do not undermine the security of everyone in order to monitor the few.

Proposals to deliberately weaken encryption must be recognized for what they are: efforts to prioritize surveillance over cybersecurity.[57] The balance should come out exactly the other way. In recent years, there have been major hacks of U.S. government agencies, educational institutions, and private corporations.[58] Tens or hundreds of millions of individuals have

---

[53] *See, e.g.*, John Kelly, *Cellphone Data Spying: It's Not Just the NSA*, USA Today, June 13, 2014, http://usat.ly/1HSGldF (describing local police use of "tower dumps," "Stingrays" or cell-site simulators, and location-tracking orders); Michael S. Schmidt & Matt Apuzzo, *U.S. Discloses New Trove of Phone Call Records*, N.Y. Times, Jan. 16, 2015, http://nyti.ms/1HSyehi (discussing a database maintained by the Drug Enforcement Administration of the records of phone calls made between phone numbers in the United States and overseas).

[54] Cory Doctorow, *What David Cameron Just Proposed Would Endanger Every Briton and Destroy the IT Industry*, boingboing.net (Jan. 13, 2015), http://boingboing.net/2015/01/13/what-david-cameron-just-propos.html ("The very best in secure communications are already free/open source projects, maintained by thousands of independent programmers around the world.").

[55] Tom Simonite, *NSA Leak Leaves Crypto-Math Intact but Highlights Known Workarounds*, MIT Tech. Rev., Sept. 9, 2013, http://www.technologyreview.com/news/519171/nsa-leak-leaves-crypto-math-intact-but-highlights-known-workarounds/.

[56] *FBI Sheds Light on 'Magic Lantern' PC Virus*, Reuters, Dec. 13, 2001, http://usatoday30.usatoday.com/life/cyber/tech/2001/12/13/magic-lantern.htm.

[57] See generally Susan Landau, *Surveillance or Security? The Risks Posed by New Wiretapping Technologies* (MIT Press, 2011); Going Dark: Lawful Electronic Surveillance in the Face of New Technologies: Hearing Before the Subcomm. on Crime, Terrorism, and Homeland Sec. of the H. Comm. on the Judiciary, 112th Cong. 23–34 (2011) (statement of Prof. Susan Landau), available at http://judiciary.house.gov/_files/hearings/pdf/Landau02172011.pdf.

[58] Linzi Oliver, *10 Notable Privacy & Security Breaches of 2014*, SpiderOak Blog (Dec. 31, 2014), https://blog.spideroak.com/20141231115421-10-notable-privacy-security-breaches-2014-tips-protect-personal-data; Lillian Ablon, *Keeping Safe in the New Year: After a Year of Major Hacks, Cybersecurity Resolutions for 2015*, U.S. News & World Report, Dec. 31, 2014, http://www.usnews.com/opinion/blogs/world-report/2014/12/31/after-a-year-of-major-hacks-2015-resolutions-to-bolster-cybersecurity.

had their private data compromised. Major companies have endured unprecedented intrusions into their systems.[59] And even the government has seen sensitive military information stolen.[60] Virtually every high-level intelligence official in the United States has identified cyberattacks as the most serious threat to the nation's security.[61]

Strong encryption is our first line of defense against that threat. Weakening that encryption would make us all—private citizens and companies alike—more vulnerable to attack. Backdoor access may make law enforcement more efficient, but it would do so only at the expense of everyone's security.

III. Encryption and anonymity are essential tools of free expression.

The explosion of online speech and association has fostered democratic accountability around the world.[62] So too, however, has it empowered governments to identify, monitor, and silence their critics with a convenience never before possible. Encryption and anonymity are the only effective safeguards against that assault on the freedom of expression and association.[63] Indeed, privacy is "an essential requirement for the realization of the right to freedom of expression."[64]

There is, in fact, nothing new about the connection between free expression and both cryptography and anonymity. Since America's founding, both have enabled political dissent.

James Madison, for example, relied on ciphers both in a political capacity as Secretary of State and in his personal correspondence with Thomas Jefferson.[65] Archives of Madison's encrypted letters show him discussing topics ranging from his unsuccessful courtships, to his personal political rivals, to his views on the need to raise taxes.[66] James Lovell, a member of the Continental Congress, designed codes and ciphers that were used widely by

---

[59] Ronald Grover, Mark Hosenball & Jim Finkle, *Sony Suffered the Most Devastating Hack of a Major U.S. Company Ever*, Business Insider (Dec. 3, 2014), http://www.businessinsider.com/the-size-and-scope-of-the-sony-hack-is-incredible-2014-12; Brian X. Chen, *Apple Says It Will Add New iCloud Security Measures After Celebrity Hack*, N.Y. Times, Sept. 5, 2014, http://nyti.ms/18KS2DJ.

[60] Luis Martinez et al., *Major U.S. Weapons Compromised by Chinese Hackers, Report Warns*, ABC News, May 28, 2013, http://abcn.ws/18KQAkC

[61] *See, e.g.*, Jim Garamone, *Clapper Places Cyber at Top of Transnational Threat List*, Am. Forces Press Serv. (Mar. 12, 2013), http://www.defense.gov/news/newsarticle.aspx?id=119500; James B. Comey, Dir. of FBI, *Remarks at RSA Cyber Security Conference* (Feb. 26, 2014), http://www.fbi.gov/news/speeches/the-fbi-and-the-private-sector-closing-the-gap-in-cyber-security.

[62] Carol Huang, *Facebook and Twitter Key to Arab Spring Uprisings: Report*, The National, June 6, 2011, http://www.thenational.ae/news/uae-news/facebook-and-twitter-key-to-arab-spring-uprisings-report; Jose Antonio Vargas, *Spring Awakening: How an Egyptian Revolution Began on Facebook*, N.Y. Times, Feb. 17, 2012, http://www.nytimes.com/2012/02/19/books/review/how-an-egyptian-revolution-began-on-facebook.html.

[63] *See* La Rue *Report*, *supra* note 42, ¶¶ 23, 47, 51, 69, 88–90.

[64] *See id.* ¶ 24.

[65] The James Madison Papers, *James Madison's Ciphers*, Library of Congress, http://memory.loc.gov/ammem/collections/madison_papers/mjmciphers.html (last visited Feb. 9, 2015).

[66] Ralph E. Weber, Masked Dispatches: Cryptograms and Cryptology in American History, 1775–1900 83 (2011).

members of the congress and their families. John and Abigail Adams famously used Lovell's ciphers to encrypt their personal correspondence.[67] Other early encryptors included George Washington, James Monroe, Alexander Hamilton, Aaron Burr, and John Jay, the first Chief Justice of the U.S. Supreme Court.[68]

The role of anonymity in founding-era America was, if anything, even more pronounced: "Our history as a republic was shaped by essays written by anonymous authors."[69] Many of the early American statesmen who debated the principles upon which our country was founded did so behind a veil of anonymity. Indeed, the influential Federalist Papers were published under fictitious names, such as Publius, Americanus, and Caesar.[70] For these "Framers and their contemporaries, anonymity was the deciding factor between whether their writings would produce a social exchange or a personal beating."[71]

The use of encryption and anonymity in the United States as enablers of free expression continues to this day, all the more so since the revelations by Edward Snowden that the National Security Agency is engaging in mass surveillance of innocent individuals around the world.[72]

Journalists, for example, rely heavily on their ability to maintain the anonymity of their sources and the confidentiality of their communications. According to our recent research, journalists in the United States covering sensitive zones of government activity—such as national security, intelligence, and law enforcement—face increasing challenges in doing their work, largely because the developing technology of surveillance has made it much more difficult for them to protect their sources.[73] Many prominent journalists reported losing long-standing sources or struggling to develop new ones, specifically because of the government's ability to unmask and pursue them.[74] Even more troublingly, we have found that sources are, for the same reason, increasingly reluctant to discuss even unclassified

---

[67] David Kahn, *The Code-Breakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet* 181 (1996); The James Madison Papers, *supra* note 65; Weber, *supra* note 66, at 83.

[68] John A. Fraser, III, *The Use of Encrypted, Coded and Secret Communications Is an 'Ancient Liberty' Protected by the United States Constitution*, 2 Va. J.L. & Tech 2 (1997), *available at* http://www.vjolt.net/vol2/issue/vol2_art2.html. In the century following the invention of the telegraph in 1844, forty-four new commercial ciphers were patented by Americans for both commercial and private uses. *See* Simon Singh, *The Code Book* 61, 79 (1999); Kahn, *supra* note 67, at 191.

[69] Jonathan Turley, Registering Publius: The Supreme Court and the Right to Anonymity, 2002 Cato Sup. Ct. Rev. 57, 59 (2002).

[70] *Id.* at 59–60.

[71] *Id.* at 58.

[72] PEN America, *Chilling Effects: NSA Surveillance Drives U.S. Writers to Self-Censor* (Nov. 12, 2013), http://www.pen.org/sites/default/files/Chilling%20Effects_PEN%20American.pdf; ACLU & Human Rights Watch, *With Liberty to Monitor All: How Large-Scale US Surveillance Is Harming Journalism, Law, and American Democracy* 22–48 (2014), https://www.aclu.org/sites/default/files/assets/dem14-withlibertytomonitorall-07282014.pdf; Jesse Holcomb & Amy Mitchell, *Investigative Journalists and Digital Security: Perceptions of Vulnerability and Changes in Behavior*, Pew Research Ctr. (Feb. 5, 2015); http://www.journalism.org/2015/02/05/investigative-journalists-and-digital-security/.

[73] With Liberty to Monitor All, *supra* note 72, at 22–48.

[74] *Id.* at 24–30.

matters with journalists, impeding even the everyday but no-less-essential reporting on government activities.[75]

Journalists have responded by adopting a variety of measures designed to protect their sources. Some, for example, have eschewed electronic communication, while others have attempted to enhance their digital security and anonymity—using technologies that both secure their communications and anonymize their Internet usage.[76] It remains to be seen whether these tactics are sufficient to restore the trust of sources in their ability to communicate safely with journalists.[77]

Journalists are far from the only ones who rely heavily on encryption and anonymity in their free expression. Political dissidents and human-rights defenders increasingly utilize new technologies to expose governmental abuses,[78] but without sufficiently secure and anonymous access to those tools, they cannot safely criticize those in power.[79]

In recent years, these groups have been subjected to increasingly sophisticated attacks on their digital security.[80] Intercepted information has been used to track their activities and whereabouts, leading to a greater number of arrests and direct censorship.[81] This trend has led to the development of security tools intended specifically for human-rights defenders and activists, including the Security In-a-Box toolkit[82] and Detekt.[83]

Digital anonymity is especially important for a separate reason. Technology has facilitated automated censorship—through which repressive regimes automatically flag content from

---

[75] *Id.* at 29.

[76] *Id.* at 30–38.

[77] *Id.* at 29–30, 40–42 (describing mixed success of journalists).

[78] *See, e.g.*, Keith B. Richburg, *China's 'weibo' Accounts Shuttered as Part of Internet Crackdown*, Wash. Post, Jan. 3, 2013, http://www.washingtonpost.com/world/chinas-weibo-accounts-shuttered-as-part-of-internet-crackdown/2013/01/03/f9fd92c4-559a-11e2-89de-76c1c54b1418_story.html.

[79] *See, e.g.*, La Rue *Report*, *supra* note 42, ¶ 53 ("Indeed, throughout history, people's willingness to engage in debate on controversial subjects in the public sphere has always been linked to possibilities for doing so anonymously."); Jon Leibowitz, FTC Comm'r, *Remarks on Spam, Authentication and the Promise of the Internet* (Nov. 10, 2004), http://www.ftc.gov/sites/default/files/documents/public_statements/spam-authentication-and-ensuring-promise-internet/041110eauthsummit.pdf ("Political dissidents, victims of domestic abuse, and others must be able to communicate freely and anonymously.").

[80] Cynthia Romero, *What Next?: The Quest to Protect Journalists and Human Rights Defenders in a Digital World*, Freedom House (Feb. 2014), https://freedomhouse.org/sites/default/files/What%27s%20Next%20-%20The%20Quest%20to%20Protect%20Journalists%20and%20Human%20Rights%20Defenders%20in%20a%20Digital%20World.pdf.

[81] Stephanie Hankey & Daniel Ó Clunaigh, *Rethinking Risk and Security of Human Rights Defenders in the Digital Age*, 5:3 J. Hum. Rts. Prac. 535 (Nov. 2013), http://protectionline.protectioninternational.org/files/2013/11/J-Human-Rights-Practice-2013-Hankey-535-47.pdf; Human Rights Watch, *Ethiopia: Telecom Surveillance Chills Rights* (Mar. 25, 2014), http://www.hrw.org/news/2014/03/25/ethiopia-telecom-surveillance-chills-rights.

[82] Security In-a-Box, https://securityinabox.org/ (last visited Feb. 9, 2015).

[83] Detekt, https://resistsurveillance.org/ (last visited Feb. 9, 2015) (a tool to detect surveillance spyware).

dissidents or disfavored websites for suppression. China is notorious for such strategies.[84] Dissidents and activists seeking to evade that mechanized censorship have resorted to the same anonymizing tools discussed above. Unfortunately, some governments have responded by attempting to block access to or use of such tools.[85]

IV. Conclusion.

To preserve the promise of expression online, our laws must adequately protect the rights to communicate securely and to remain anonymous. Without these tools, political dissidents, journalists, whistleblowers, human-rights defenders, activists, and those living under repressive regimes would become even more vulnerable to persecution. And without strong encryption, in particular, we leave everyone defenseless against the ever-more-destructive cyberattacks that are occurring with only increasing regularity.

For more information on this submission, please contact:

Alex Abdo
Staff Attorney | Speech, Privacy, and Technology Project
American Civil Liberties Union
125 Broad Street, 17th Floor
New York, NY 10004
aabdo@aclu.org

[84] Andrew Jacobs, *China Further Tightens Grip on the Internet*, N.Y. Times, Jan. 19, 2015, http://www.nytimes.com/2015/01/30/world/asia/china-clamps-down-still-harder-on-internet-access.html.

[85] *China Blocks Virtual Private Network Use*, BBC News, Jan. 26, 2015, http://www.bbc.com/news/technology-30982198.