February 10, 2015

Special Rapporteur on the promotion and protection
of the right to freedom of opinion and expression
Palais des Nations
CH-1211 Geneva 10
Switzerland
Fax: +41 22 917 9006

Re: Call for comments regarding the development of a report on the legal framework governing the relationship between freedom of expression and the use of encryption to secure transactions and communications, and other technologies to transact and communicate anonymously online.

Dear Special Rapporteur Kaye:

The Reporters Committee for Freedom of the Press and the Committee to Protect Journalists appreciate this opportunity to jointly comment on the appropriate scope of the right to freedom of expression as applied to encryption and anonymity.

In this comment we will explain why encryption and anonymity are needed to protect journalists and their sources; how encryption policies developed by companies and governments have strong normative power and far-reaching consequences; why the subversion of encryption standards harms journalism; and why the criminalization of protecting one's established right to private communication and association should not occur.

I. Encryption and anonymity devices are needed for journalists to protect information and sources

Journalism plays an essential role in realizing democratic and developmental[1] rights and serves a societal interest in transparency. Wherever they take place, acts of journalism often involve enormous risk to journalists and sources. This is especially true where journalists challenge power.

As the number of online journalists has increased, so have attacks and threats against them.[2] These can range from the illegal hacking of their accounts, monitoring of their online activities, their arbitrary arrest,

[1] *See, e.g.,* Robert Mahoney, *Putting Press Freedom at the Heart of Anti-Poverty Efforts* in Attacks on the Press in 2014, (Elana Beiser et al., eds.), *available at* https://www.cpj.org/2014/02/attacks-on-the-press-transparency-governance.php.

[2] *See, e.g.,* Office of the High Commissioner for Human Rights, *The Safety of Journalists: Report of the Office of the United Nations High Commissioner for Human Rights,* OHCHR, *available at* http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/24/23 (July 1, 2013).

detention, torture, and murder, and the blocking of websites that contain information critical of authorities.[3]

Encryption[4] and anonymity tools[5] help journalists improve their security and privacy and can help to mitigate or prevent some of these threats and attacks, as well as provide better protection for their sources.

Encryption helps journalists protect the content of their communications by scrambling the information in a way that only allows intended recipients to read it. Journalists can use encryption to prevent outside parties from reading or listening to a variety of digital communications—from email and instant messages to SMS and phone calls—by encrypting Internet traffic and stored data. Sophisticated systems can even hide who is communicating with whom, or that communication took place at all.

When journalists can't use tools like encryption, their work is put at risk. In 2011, Syrian security agents arrested British journalist and filmmaker Sean McAllister and seized his laptop, cell phone, camera, and footage for his documentary—which revealed, among other things, the identities of several dissidents he interviewed on camera while in the country. When dissidents heard McAllister had been arrested, many of them fled the country to avoid physical harm or arrest, but several were arrested.[6] Although McAllister's news outlet said he took steps to protect his material, it does not appear that his footage or his devices were encrypted at the time of his arrest. If they had been, this step could have better protected the identities of his sources.[7] Even though McAllister was not physically beaten or tortured while in jail, he said he witnessed other detainees experience both.[8]

Journalists are safest when all communications are encrypted by default, both because it prevents the use of encryption from raising a red flag of suspicion and because it reduces the chance of harm caused by human error.[9] The more automatic encryption becomes, the more widely it will be used by everyone, and thus the more journalists will benefit.

---

[3] Ibid.

[4] Encryption is a process that involves making a message unreadable except to the person who knows how to decrypt it back into readable form. Encryption can be used across a variety of platforms, including phone, Voice over Internet Protocol (VoIP), email, online chat, and file-sharing.

[5] Tools that can help provide anonymity include proxies, which channel communications through an intermediary device. Not all proxies provide anonymity, even if they can help journalists access information online that was previously censored. In addition, not all proxies utilize encryption and those that do, don't necessarily provide anonymity.

[6] *See, e.g.,* Matthieu Aikins, *The spy who came in from the code*, CJR, *available at* http://www.cjr.org/feature/the_spy_who_came_in_from_the_c.php?page=all (May 3, 2012)

[7] *See, e.g.,* Eva Galperin, *Don't get your sources in Syria killed*, CPJ, *available at* https://cpj.org/blog/2012/05/dont-get-your-sources-in-syria-killed.php (May 21, 2012); *see also* http://www.cjr.org/feature/the_spy_who_came_in_from_the_c.php?page=all

[8] *See, e.g.,* Channel 4, *The prisoners 'treated like animals' in Syria's dungeons, available at* http://www.channel4.com/news/the-prisoners-treated-like-animals-in-syrias-dungeons (Nov. 3, 2011).

[9] *See, e.g.,* Tom Lowenthal, *How automatic encryption ensures safety by default,* CPJ, *available at* https://cpj.org/blog/2014/10/how-automatic-encryption-ensures-safety-by-default.php (Oct. 2, 2014); *see also* http://www.cjr.org/behind_the_news/hacks_hackers_security_for_jou.php?page=all.

i. Limitations to encryption

Encryption does not protect the metadata, or the data about data, of communications. Far from being innocuous, metadata can provide extremely revealing information even if the content of communications remains secret.[10] Journalists and sources need to worry about the metadata of their communications because it can reveal reporter-source communications and relationships.

In 2013, U.S. law enforcement officials obtained the records for more than 20 telephone lines of Associated Press offices and journalists, including cell phones and home phones.[11] The seizure took place with a secret subpoena and without notification to The Associated Press. Law enforcement agents confirmed the source of the leaks in part by analyzing the AP phone records and comparing them with other evidence in their possession.[12] The source pled guilty and is currently serving a jail term.[13]

In 2009, the U.S. Department of Justice began investigating possible leaks of classified information about North Korea. In its investigation, it monitored Fox News reporter James Rosen by tracking his visits to the U.S. State Department and the timing of calls and his personal email. To prevent Rosen from being informed of ongoing surveillance, he was named a "criminal co-conspirator" and described as a "flight risk."[14] Although Rosen's source was already mentioned in an affidavit[15] in support of an application for a search warrant of Rosen's Gmail account, the metadata and content obtained from the warrant helped to make the case against Rosen's source.[16] Rosen's source was eventually found guilty and is currently serving a jail term.[17]

In January 2015, former CIA officer Jeffrey Sterling was convicted of giving confidential information to *New York Times* investigative reporter James Risen. Although Risen was subpoenaed and testified in an

---

[10] *See, e.g.,* Timothy B. Lee, *Here's how phone metadata can reveal your affairs, abortions, and other secrets.*, The Washington Post, *available at* http://www.washingtonpost.com/blogs/the-switch/wp/2013/08/27/heres-how-phone-metadata-can-reveal-your-affairs-abortions-and-other-secrets/ (Aug. 27, 2013); *see also,* Geoffrey King, *NSA puts journalists under a cloud of suspicion* in Attacks on the Press in 2014, (Elana Beiser et al., eds.), *available at* https://www.cpj.org/2014/02/attacks-on-the-press-surveillance-storage.php.

[11] *See, e.g., Charlie Savage, Phone Records of Journalists Seized by U.S.*, NY Times, *available at* http://www.nytimes.com/2013/05/14/us/phone-records-of-journalists-of-the-associated-press-seized-by-us.html?pagewanted=all&_r=0 (May 13, 2013).

[12] *See, e.g.,* Associated Press, *Yemen leak: former FBI man admits passing information to Associated Press*, The Guardian, *available at* http://www.theguardian.com/media/2013/sep/24/yemen-leak-sachtleben-guilty-associated-press

[13] *See, e.g.,* Associated Press, *Former FBI agent sentenced to three years in prison for Associated Press leak*, The Guardian, *available at* http://www.theguardian.com/world/2013/nov/14/former-fbi-agent-sentenced-associated-press-leak (Sep. 23, 2013).

[14] *See, e.g.,* Ann E. Marimow, *A rare peek into a Justice Department leak probe,* The Washington Post, *available at* http://www.washingtonpost.com/local/a-rare-peek-into-a-justice-department-leak-probe/2013/05/19/0bc473de-be5e-11e2-97d4-a479289a31f9_story.html?tid=pm_pop (May 19, 2013).

[15] *See, e.g.,* Reginald B. Reyes, *Affidavit in support of application for search warrant, available at* http://fas.org/sgp/jud/kim/warrant.pdf (May 28, 2010).

[16] *See, e.g.,* Steven Aftergood, *Reporter Deemed "Co-Conspirator" in Leak Case,* Federation of American Scientists, *available at* http://fas.org/blogs/secrecy/2013/05/kim-rosen-warrant/ (May 20, 2013).

[17] *See, e.g.,* Josh Gerstein, *Stephen Kim pleads guilty in Fox News leak case*, Politico, *available at* http://www.politico.com/story/2014/02/stephen-kim-james-risen-state-department-fox-news-103265.html?utm_source=dlvr.it&utm_medium=twitter (Feb. 7, 2014).

unusual bench hearing, he refused to reveal any information identifying his source, and the prosecutors did not to call him to testify further. Despite this, jurors in a U.S. District Court convicted Sterling of Espionage Act violations based in part on evidence collected through metadata of his communications with Risen. Sterling's lawyer has stated that he plans to appeal.[18]

To protect metadata, journalists need to use anonymity tools that hide the location and identity of the sender. One such tool, Tor, also protects communications and sources from passive Internet surveillance known as "traffic analysis," which can allow an outsider to ascertain who is talking to whom and thereby track interests and behavior.[19] Tor protects journalists from this surveillance by distributing journalists' transactions over several places on the Internet, so no single point can link the journalist to his or her destination.

Tor also provides hidden services which protect browsing by encapsulating a regular connection within Tor's encrypted and anonymous channel, and which is never available to an exit node or to an Internet service provider (ISP). Platforms like SecureDrop[20], an anonymous whistleblowing submission system run on Tor hidden services. Facebook recently decided to adopt a dedicated Tor hidden service for Facebook users[21], which allows journalists to cultivate sources without showing their Internet Protocol address to outside parties, although it doesn't prevent Facebook from knowing a journalist's name or seeing their activity on the site.[22]

II. Encryption policy affects journalists worldwide

As discussed above, encryption protects journalists and the confidentiality of their sources by helping to ensure the privacy of their communications. While valid law enforcement and intelligence reasons for reviewing encrypted communications may exist, the threat to journalism posed by mass surveillance counsels in favor of skepticism toward state claims that encryption is the exclusive province of criminals, terrorists, and spies. In reality, untold numbers of journalists use encryption to protect themselves, their sources, and the free flow of news.

The United States is a primary innovator of encryption technologies, as well as the guardian of perhaps the most sophisticated signals intelligence architecture known to humankind. While substantial legal

---

[18] *See, e.g., United States of America v. Jeffrey Alexander Sterling, available at* https://www.documentcloud.org/documents/229733-judge-leonie-brinkemas-ruling-quashing-subpoena.html (July 29, 2011.); *see also*, Adam Liptak, A High-Tech War on Leaks, NY Times, *available at* http://www.nytimes.com/2012/02/12/sunday-review/a-high-tech-war-on-leaks.html?hpw=&pagewanted=all&_r=0 (Feb. 11, 2012); *see also* Department of Justice, *CIA Officer Convicted For Unauthorized Disclosure of National Defense Information and Obstruction of Justice*, DOJ, *available at* http://www.justice.gov/opa/pr/former-cia-officer-convicted-unauthorized-disclosure-national-defense-information-and (Jan. 26, 2015); *and see* Greg Miller, *Former CIA officer Jeffrey A. Sterling charged in leak probe*, The Washington Post, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2011/01/06/AR2011010604001_2.html?sid=ST2011010604303 (Jan. 6, 2011).

[19] *See, e.g.,* Tor: Overview, *available at* https://www.torproject.org/about/overview.html.en

[20] *See, e.g.,* SecureDrop, *available at* https://freedom.press/securedrop

[21] Facebook Tor hidden service can be accessed here: https://facebookcorewwwi.onion

[22] *See, e.g.,* Tom Lowenthal, *How Facebook's Tor hidden service improves safety for journalists,* CPJ, *available at* https://cpj.org/blog/2014/11/how-facebooks-tor-hidden-service-improves-safety-f.php (Nov. 5, 2014).

protections exist to protect U.S. persons from surveillance falling outside the context of a targeted criminal investigation, it is nonetheless true that large amounts of data about U.S. persons is swept up in the NSA's dragnet.[23] In addition, U.S. law provides little protection to non-U.S. persons based abroad.

The U.S. Constitution protects journalists and media in the United States by prohibiting the making of any law "abridging the freedom of speech, or of the press."[24] Despite this sweeping constitutional statement, in practice, journalistic protections in the United States are not monolithic. While many states have recognized constitutional, common law, or statutory rights that protect a reporter from being compelled to reveal his or her source, this "reporter's privilege" is usually limited, or "qualified." Several federal appellate courts have recognized a constitutional privilege as well.[25] However, the protections of the reporter's privilege differ in scope and extent depending on the jurisdiction in which the privilege is asserted. As a result, encryption and anonymity play an important role in safeguarding journalists' legally recognized obligations to protect the confidentiality of their sources.

Encryption itself also enjoys substantial protection under the U.S. Constitution. Notably, the First Amendment was drafted in part via encrypted comments exchanged by post between Thomas Jefferson and James Madison.[26] Under the First Amendment, computer code—including source code for encryption programs—is a form of expression entitled to protection. In a 1999 case, a federal appellate court recognized that while cryptography had military roots, it had "blossomed in the civilian sphere, driven on the one hand by dramatic theoretical innovations within the field, and on the other by the needs of modern communication and information technologies."[27] A year later, another federal appellate court held that encryption software is "expressive" and entitled to constitutional protection, ending a long period in which encryption software was difficult to release or obtain.[28]

In the United States, major technology companies have begun to add encryption to their products by default, prompting pushback from law enforcement and intelligence agencies. For example, the director of the Federal Bureau of Investigation claimed that the FBI would not be able to "access the evidence we need to prosecute crime and prevent terrorism even with lawful authority,"[29] a claim that has been shown

---

[23] *See, e.g.,* Charlie Savage, *N.S.A. Said to Search Content of Messages to and From U.S.,* NY Times, *available at* http://www.nytimes.com/2013/08/08/us/broader-sifting-of-data-abroad-is-seen-by-nsa.html (Aug. 8, 2013).
[24] U.S. Const. Am. I.
[25] *See Gonzales v. Nat'l Broadcasting Co.*, 194 F.3d 29 (2d Cir. 1999) (recognizing a constitutional reporters' privilege); *In re Cusumano v. Microsoft Corp.*, 162 F.3d 708 (1st Cir. 1998) (same); *Riley v. City of Chester*, 612 F.2d 708 (3rd Cir. 1979) (same); *but see United States v. Sterling*, 724 F.3d 482, 492 (4th Cir. 2013) (rejecting the assertion of a reporter's privilege in a criminal prosecution).
[26] 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* www.vjolt.net/vol2/issue/vol2_art2.html.
[27] *Bernstein v. Dep't of Justice,* 176 F.3d 1132, 1137 (9th Cir. 1999) (decision withdrawn)
[28] Junger v. Daley, 209 F.3d 481 (6th Cir. 2000).
[29] *See e.g.,* Hannah Bloch-Wehba, Tech companies' announcement of new encryption policies prompts pushback from law enforcement, *available at* http://www.rcfp.org/browse-media-law-resources/news/tech-companies-announcement-new-encryption-policies-prompts-pushback (Oct. 21, 2014); *see also,* James B. Comey, *Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?*, FBI, *available at* *http://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course* (Oct. 16, 2014).

to be dubious.[30] As of this writing, no U.S. legislation bars technology companies from encrypting their products by default. Nonetheless, U.S. law enforcement agencies have sought and obtained court orders to compel service providers to unlock phones. Some commentators have inferred that law enforcement agencies may seek to similarly compel providers to decrypt communications.[31]

At the same time, the Fourth Amendment to the U.S. Constitution protects against unreasonable searches and seizures of persons, houses, papers, and effects. The Fourth Amendment applies to governmental searches of communications, including the bulk collection of international communications pursuant to the USA PATRIOT ACT that was revealed by former NSA contractor Edward Snowden in 2013.[32] The Foreign Intelligence Surveillance Act, the statute authorizing this programmatic surveillance, requires the government to use "minimization procedures" to limit unnecessary and inappropriate use of the information collected.[33] But the minimization procedures in place authorize the National Security Agency to retain communications for an unlimited period of time if they are encrypted or "reasonably believed to contain secret meaning."[34] Encrypted communications may be retained indefinitely if they "are, or are reasonably believed likely to become, relevant to a current or future foreign intelligence requirement."[35] In practice, U.S. intelligence services may rely on this broad and sweeping provision to retain journalists' encrypted communications indefinitely. And while the minimization procedures contain particular provisions to segregate and protect attorney-client communications, journalist-source communications are not afforded comparable protections.[36] As a result, it is not clear that the minimization procedures in place provide adequate protections for key constitutional rights.

Finally, constitutional protections against self-incrimination may apply where a person is a criminal defendant and the prosecution seeks to compel him or her to turn over a decryption key. The Fifth Amendment to the U.S. Constitution protects a criminal defendant's right not to incriminate him or herself. This "prohibition of compelling a man in a criminal court to be witness against himself" applies, in some circumstances, to forced decryption.[37] The only U.S. appellate court to address this issue has held that forcing a criminal defendant to decrypt a hard drive containing evidence is a Fifth Amendment

---

[30] *See e.g.,* Geoffrey King, *How DOJ, FBI resistance to encryption jeopardizes journalism,* CPJ, *available at* https://cpj.org/blog/2014/10/doj-resistance-to-encryption-jeopardizes-journalis.php (Oct. 16, 2014); *see also* Dan Froomkin and Natasha Vargas Cooper, *The FBI Director's Evidence Against Encryption is Pathetic,* The Intercept, *available at* https://firstlook.org/theintercept/2014/10/17/draft-two-cases-cited-fbi-dude-dumb-dumb (Oct. 17, 2014); *and see* Geoffrey King, *Classifying media and encryption as a threat is danger to press freedom,* CPJ, *available at* https://www.cpj.org/blog/2015/01/classifying-media-and-encryption-as-a-threat-is-da.php (Jan. 21, 2015).

[31] *See e.g.,* Danny Yadron, *Case Suggests How Government May Get Around Phone Encryption*, Wall Street Journal, *available at* http://blogs.wsj.com/digits/2014/11/25/case-suggests-how-government-may-get-around-phone-encryption/ (Nov. 25, 2014).

[32] *See e.g.,* James Ball and Spencer Ackerman, *NSA loophole allows warrantless search for US citizens' emails and phone calls*, The Guardian, *available at* http://www.theguardian.com/world/2013/aug/09/nsa-loophole-warrantless-searches-email-calls (Aug. 9, 2013).

[33] 50 U.S.C. § 1881a(e).

[34] Section 702 minimization procedures, http://www.dni.gov/files/documents/Minimization%20Procedures%20used%20by%20NSA%20in%20Connection%20with%20FISA%20SECT%20702.pdf

[35] *Id.*

[36] *Id*.

[37] *Holt v. United States*, 218 U.S. 245, 252 (1910).

violation.[38] Many federal district and state courts, however, have held that under the "foregone conclusion" doctrine, production of the unencrypted contents of a storage device does not implicate the Fifth Amendment if the documents therein are already known to the government.[39]

III. The criminalization of secure means of communication would abrogate key international protections for free expression and association, due process and privacy, and would lead to the prosecution of journalists around the world

Many of the protections for U.S. persons discussed above are inapplicable within the international context. Considerable evidence exists that the U.S. takes a much freer hand when conducting purely foreign surveillance. Additionally, other states may feel relatively unrestrained about targeting their own citizens, of whom journalists are an oft-targeted subset.

However, freedom from arbitrary surveillance enjoys robust protection under international law. The right to freedom of opinion and expression is codified under articles 19 of the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights ("ICCPR"), Article 9 of the African Charter on Human and Peoples' Rights, Article 13 of the American Convention on Human Rights, and Article 10 of the Convention for the Protection of Human Rights and Fundamental Freedoms. Privacy, a necessary condition to expression, is guaranteed by Article 12 of the Universal Declaration of Human Rights, Article 17 of the ICCPR, Article 16 of the Convention on the Rights of the Child, Article 14 of the International Convention on the Protection of All Migrant Workers and Members of Their Families, Article 8 of the European Convention on Human Rights, and Article 11 of the American Convention on Human Rights. Notably, both the European Court of Justice[40] and the U.S. Supreme Court[41] have issued sweeping decisions protecting the privacy of electronic communications within the last year. As many experts have noted, these decisions recognize that "digital is different" and that changing norms lend significant support to protecting the privacy of communications data and data stored on (generally encrypted) devices.

Although free expression and privacy are sometimes in tension, much of the practice of journalism lies at their confluence. As former Special Rapporteur Frank LaRue concluded in his landmark report on the relationship between privacy, free expression, and mass surveillance, "[w]ithout adequate protection to privacy, security and anonymity of communications, no one can be sure that his or her private communications are not under states' scrutiny."[42] As Special Rapporteur LaRue further explained, "[t]he

[38] *See, e.g., In re Grand Jury Subpoena Duces Tecum*, March 25, 2011, 670 F.3d 1335, 1349 (11th Cir. 2012) (upholding a Fifth Amendment privilege against decryption).
[39] *See, e.g.*, *In re Boucher*, No. 2:06-mj-91, 2009 WL 424718 (D.Vt. Feb. 19, 2009) (compelling production of a decrypted version of an encrypted storage device); *United States v. Fricosu*, 841 F. Supp. 2d 1232, 1237 (D. Col. 2012) (compelling production of a decrypted version of an encrypted storage device); *Commonwealth v. Gelfgatt*, 468 Mass. 512, 514 (Mass. 2014) (compelling decryption where it "would not communicate facts of a testimonial nature to the Commonwealth beyond what the defendant already had admitted to investigators").
[40] Digital Rights Ireland Ltd (C-293/12) v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung (C-594/12) and Others (2014).
[41] Riley v. California, 573 U.S. ___ (2014).
[42] *See, e.g.,* Office of the High Commissioner for Human Rights. *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, OHCHR, *available at*

security and anonymity of communications are … undermined by laws that limit the use of privacy-enhancing tools that can be used to protect communications, such as encryption."[43]

Although legitimate law enforcement reasons may necessitate surveillance of targets based on individualized suspicion, the use of cryptographic tools should not itself be criminalized by states, nor should the failure to disclose one's cryptographic key. Laws regulating cryptography exist in a number of states,[44] and several notable examples already exist of such laws being used against journalists. In the United Kingdom, David Miranda, the partner of journalist Glenn Greenwald, was held for several hours under that country's Terrorism Act and threatened with jail time should he refuse to cooperate.[45] At the time, Miranda was carrying encrypted memory sticks from Laura Poitras in Berlin back to Glenn Greenwald in Brazil.[46] In addition, in Ethiopia, the Zone 9 bloggers[47] are reportedly charged with receiving encryption training.[48]

Significantly, states may be in the early stages of a general trend toward increasing regulation of privacy-protecting technologies. In the U.K., Prime Minister David Cameron recently pledged to ban end-to-end encrypted messaging should his party win the country's general election in May; it also has been repeatedly revealed that the country's security services have surveilled journalists and even classified them as threats to national security.[49] In China, a country that threatens journalism within[50] and outside[51]

---

http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf (April 17 2013).

[43] Ibid.

[44] See generally Nathan Saper, *International Cryptography Regulation and the Global Information Economy,* 11 Nw. J. Tech. & Intell. Prop. 673 (2013), *available at* http://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1205&context=njtip; see also Simon Hunt, *International Crypto and Encryption Law*, Google Maps, *available at* https://www.google.com/maps/d/u/1/viewer?oe=UTF8&ie=UTF8&msa=0&mid=zknWAukjyXLQ.kfXWg3sqZpn4.

[45] *See e.g.,* Jonathan Watts, David Miranda: *'They said I would be put in jail if I didn't co-operate',* The Guardian, *available at* www.theguardian.com/world/2013/aug/19/david-miranda-interview-detention-heathrow (Aug. 19, 2013).

[46] *See e.g.,* Bruce Schneier, *The Real, Terrifying reason Why British Authorities Detained David Miranda,* The Atlantic, *available at* http://www.theatlantic.com/international/archive/2013/08/the-real-terrifying-reason-why-british-authorities-detained-david-miranda/278952/ (Aug. 22, 2013); *see also,* Ryan Devereaux, *UK Court: David Miranda Detention Legal Under Terrorism Law*, The Intercept, https://firstlook.org/theintercept/2014/02/19/uk-court-david-miranda-detention-legal-terrorism-law/ (Feb. 19, 2014).

[47] *See, e.g.,* Rachael Levy, *Zone 9 blogger urges world to call for freedom in Ethiopia,* CPJ, *available at* https://cpj.org/blog/2014/07/zone-9-blogger-urges-world-to-call-for-freedom-in-.php (July 7, 2014).

[48] *See, e.g.,* Ellery Biddle, *Zone 9 Bloggers Charged With Terrorism in Ethiopia, Global Voices, available at* http://globalvoicesonline.org/2014/07/18/zone-9-bloggers-charged-with-terrorism-in-ethiopia/ (July 18, 2014).

[49] *See, e.g.,* James Ball, *GCHQ captured emails of journalists from top international media*, The Guardian, *available at*, http://www.theguardian.com/uk-news/2015/jan/19/gchq-intercepted-emails-journalists-ny-times-bbc-guardian-le-monde-reuters-nbc-washington-post (Jan. 19, 2015), *see also* Geoffrey King, *Classifying media and encryption as a threat is a danger to press freedom,* CPJ, *available at* https://cpj.org/blog/2015/01/classifying-media-and-encryption-as-a-threat-is-da.php (Jan. 21, 2015), *and see* Mark Scott, *British Prime Minister Suggests Banning Some Online Messaging Apps*, NY Times, *available at* http://bits.blogs.nytimes.com/2015/01/12/british-prime-minister-suggests-banning-some-online-messaging-apps/ (Jan. 12, 2015).

[50] *See, e.g.,* Shazdeh Omari, *China is world's worst jailer of the press; global tally second worst on record,* CPJ, *available at* https://www.cpj.org/reports/2014/12/journalists-in-prison-china-is-worlds-worst-jailer.php (Dec. 17, 2014).

[51] *See, e.g.,* Danny O'Brien, *Drawing lessons from Chinese attacks on U.S. media*, CPJ, *available at* https://www.cpj.org/blog/2013/02/drawing-lessons-from-chinese-attacks-on-us-media.php. (Feb. 7, 2013).

its borders, new rules would require the installation of back doors into both hardware and software sold to China's banking industry.[52]

In addition to their obligation not to mandate backdoors to secure communications tools, states must not be allowed to criminalize the use of secure communication tools, as to do so would allow states unbridled discretion in violating journalists' speech, privacy, expression, association, and due process rights.

The world is at a turning point. The technological advancements that enable ubiquitous surveillance also facilitate transparency, free expression, freedom of association, privacy, and due process in ways never before possible. In order to be fully realized, these rights must be exercised more vigorously—and guarded more carefully—than ever before, and journalists are on the leading edge of both. Thus we respectfully request that your office reiterate privacy protections consistent with the formal rights of journalists, as well as enable journalists' ability to secure and safeguard those rights themselves.

Thank you.

Sincerely,
The Reporters Committee for Freedom of the Press
Committee to Protect Journalists

[52] *See e.g.,* Paul Mozur, *New Rules in China Upset Western Tech Companies*, NY Times, *available at* www.nytimes.com/2015/01/29/technology/in-china-new-cybersecurity-rules-perturb-western-tech-companies.html (Jan. 28, 2015).