

350 Fifth Avenue, 34th Floor
New York, NY 10118-3299
Tel: +1-212-290-4700
Fax: +1-212-736-1300; 917-591-3452

Kenneth Roth, *Executive Director*

DEPUTY EXECUTIVE DIRECTORS

Michele Alexander, *Development and Global Initiatives*
Nicholas Dawes, *Media*
Iain Levine, *Program*
Chuck Lustig, *Operations*
Bruno Stagno Ugarte, *Advocacy*

Emma Daly, *Communications Director*
Dinah PoKempner, *General Counsel*
James Ross, *Legal and Policy Director*

DIVISION AND PROGRAM DIRECTORS

Brad Adams, *Asia*
Daniel Bekele, *Africa*
Maria McFarland Sánchez-Moreno, *United States*
Alison Parker, *United States*
José Miguel Vivanco, *Americas*
Sarah Leah Whitson, *Middle East and North Africa*
Hugh Williamson, *Europe and Central Asia*

Shantha Rau Barriga, *Disability Rights*
Peter Bouckaert, *Emergencies*
Zama Neff, *Children's Rights*
Richard Dicker, *International Justice*
Bill Frelick, *Refugees' Rights*
Arvind Ganesan, *Business and Human Rights*
Liesl Gernholtz, *Women's Rights*
Steve Goose, *Arms*
Diederik Lohman, *acting, Health and Human Rights*
Marcos Orellana, *Environment and Human Rights*
Graeme Reid, *Lesbian, Gay, Bisexual, and Transgender Rights*

ADVOCACY DIRECTORS

Maria Laura Canineu, *Brazil*
Louis Charbonneau, *United Nations, New York*
Kanae Doi, *Japan*
John Fisher, *United Nations, Geneva*
Meenakshi Ganguly, *South Asia*
Bénédicte Jeannerod, *France*
Lotte Leicht, *European Union*
Sarah Margon, *Washington, DC*
David Mepham, *United Kingdom*
Wenzel Michalski, *Germany*
Elaine Pearson, *Australia*

BOARD OF DIRECTORS

Hassan Elmasry, *Co-Chair*
Robert Kissane, *Co-Chair*
Michael Fisch, *Vice-Chair*
Oki Matsumoto, *Vice-Chair*
Amy Rao, *Vice-Chair*
Amy Towers, *Vice-Chair*
Catherine Zennström, *Vice-Chair*
Michael Fisch, *Treasurer*
Bruce Rabb, *Secretary*
Karen Herskovitz Ackman
Akwas Aidoo
Jorge Castañeda
Michael E. Gellert
Leslie Gilbert-Lurie
Paul Gray
Betsy Karel
David Lakhdir
Kimberly Marteau Emerson
Alicia Miñana
Joan R. Platt
Neil Rimer
Shelley Frost Rubin
Ambassador Robin Sanders
Jean-Louis Servan-Schreiber
Sidney Sheinberg
Bruce Simpson
Joseph Skrzynski
Donna Slaight
Siri Stolt-Nielsen
Darian W. Swig
Makoto Takano
Marie Warburg



HRW.org

Prof. Joseph Cannataci
Special Rapporteur on the right to privacy
Office of the High Commissioner for Human Rights
Palais Wilson
Rue des Paquis, 52
1201 Geneva
Switzerland

Re: Visit to the United States of America

May 31, 2017

Dear Prof. Cannataci:

We welcome your upcoming visit to the United States of America in your capacity as the Special Rapporteur on the right to privacy. This letter focuses on a few issues in depth that we believe would be important for you to explore and address as part of your visit.

We have long concluded that as a consequence of its surveillance laws, policies, and practices, the United States is not in compliance with its obligations under the International Covenant on Civil and Political Rights (ICCPR), including the right to freedom from arbitrary or unlawful interference with privacy and correspondence (Article 17). We hope your visit will help advance the country's respect for privacy and other fundamental rights where the treatment of communications and private data is concerned.

Although the summaries below go into some detail about specific legal authorities and concepts, we believe it is important to emphasize that the US executive branch has embraced a set of practices and theories that effectively allow it to avoid proper independent authorization, oversight, and accountability. The result is a system that provides a patina of law while giving rise to serious abuses or a risk thereof. At heart, many of the US's intelligence gathering practices contravene the US's treaty obligations under the ICCPR, failing the requirements of legality, necessity, and proportionality.

I. Executive Order 12333

One of our greatest areas of concern is Executive Order 12333 ("EO 12333"), which the executive branch issued in 1981 and which has since

been amended on several occasions (most recently in 2008).¹ As a general matter, the order governs the US intelligence agencies' activities, including the gathering of information through means such as communications surveillance. The order appears to grant free rein to the agencies to conduct surveillance of communications outside US borders of non-US persons.² It may also serve as the basis for the surveillance of US persons in some broad circumstances.³

EO 12333 remains largely uncodified and the legislature had no role in its adoption. In November 2013, the then-chair of the Senate Select Committee on Intelligence suggested that Congress also plays little or no role in overseeing surveillance that takes place under this authority, and Human Rights Watch is not aware of any change in this respect.⁴ Additionally, surveillance under the order is not subject to judicial authorization or oversight, and the government believes it is not required to notify any individual—including a criminal defendant—that his or her communications have been surveilled under this authority.⁵

It has been reported that the US has used EO 12333 as the basis for vast surveillance programs around the world that have involved, among other things:

- The interception of hundreds of millions of text messages and billions of mobile telephone location updates daily;
- The interception of large quantities of data, including the content of communications, as it was being transmitted between non-US data centers belonging to major Internet companies; and
- The acquisition of records of all [mobile] telephone calls in five countries, and the acquisition of the content of those conversations in two of those countries.⁶

US government officials have implied that the government does not consider electronic information to have been “collected” until that information is processed in some way or examined by a human being.⁷ This assertion is echoed in regulations that govern

¹ Executive Order 12333: United States Intelligence Activities (as amended), available at <https://fas.org/irp/offdocs/eo/eo-12333-2008.pdf>.

² See 50 USC s. 1801(i), “United States person” includes US citizens, lawful permanent residents, and some associations and corporations; Executive Order 12333, *supra* n. 1, § 2.3. While the surveillance-related provisions of EO 12333 can be read to suggest that the intent of the order is to enable US’ intelligence agencies to use surveillance to acquire information “for foreign intelligence and counterintelligence purposes,” and while Presidential Policy Directive 28 appears to impose such a stricture, we are not aware of any measure that enforces such a requirement. The order also defines the term “foreign intelligence” to include, *inter alia*, “information relating to the capabilities, intentions, or activities of ... foreign persons” (§ 3.5(e)). It is difficult to imagine meaningful correspondence by non-US persons that would not meet this definition.

³ Executive Order 12333, *supra* n. 1, § 2.3.

⁴ Ali Watkins, “Most of NSA’s data collection authorized by order Ronald Reagan issued,” McCLATCHY, Nov. 21, 2013, <http://www.mcclatchydc.com/news/nation-world/national/national-security/article24759289.html>.

⁵ Charlie Savage, “Reagan-Era Order on Surveillance Violates Rights, Says Departing Aide,” N.Y. TIMES, Aug. 13, 2014, <https://mobile.nytimes.com/2014/08/14/us/politics/reagan-era-order-on-surveillance-violates-rights-says-departing-aide.html>.

⁶ American Civil Liberties Union & Center for Democracy & Technology, “Secret Surveillance: Five Large-Scale Global Programs,” May 2015, <https://cdt.org/files/2014/09/cdt-aclu-upr-9152014.pdf>.

⁷ See Kurt Opsahl and Trevor Timm, “The NSA’s Word Games Explained: How the Government Deceived Congress in the Debate Over Surveillance Powers,” EFF Deeplinks, June 11, 2013,

intelligence gathering activities by specific agencies: for example, “Data acquired by electronic means is ‘collected’ only when it has been processed into intelligible form.”⁸ Significantly, this interpretation implies that the US may acquire vast stores of digital information without running afoul of the already limited safeguards against arbitrary “collection” of such information in US policy. This interpretation also affects how the US government views its obligations under Article 17 since the US believes it has not interfered with the right to privacy if personal data is acquired and stored in a database, but not yet processed by a human being.

Referring to EO 12333, a State Department whistleblower warned in 2014 that “some [US] intelligence practices remain so secret, even from members of Congress, that there is no opportunity for our democracy to change them.”⁹ The whistleblower also appeared to suggest that the intelligence agencies might be using the order as the basis for warrantlessly capturing the audio of US persons’ telephone calls on a large scale.

The executive branch’s virtually unfettered power to conduct surveillance under EO 12333, its lack of accountability to Congress or other oversight bodies for actions taken under this authority, as well as the activities it allegedly conducts pursuant to this authority, undermine privacy rights and are likely to produce violations.

We urge you to raise these issues with both executive and Congressional leaders you meet, and to encourage consideration of narrowing the scope of EO 12333 and including in reporting requirements to Congress and the public.

II. Section 702 of the Foreign Intelligence Surveillance Act

Adopted by Congress in 2008, Section 702 of the Foreign Intelligence Surveillance Act (“FISA”) empowers the intelligence agencies to “target” non-US persons overseas for warrantless telephone or Internet monitoring. As confirmed by the Privacy and Civil Liberties Oversight Board in a 2014 report, the agencies operate at least two large-scale, warrantless surveillance programs pursuant to this provision.¹⁰ One, “Upstream” scanning, allegedly involves the automated bulk searching of communications that flow over the Internet infrastructure that links the US to the rest of the globe.¹¹ The other, PRISM, enables the National Security Agency (“NSA”)—with the assistance of the Federal Bureau of Investigation (“FBI”)—to demand private communications such as e-mails and instant messages from US Internet companies without warrants. Documents disclosed by former NSA contractor Edward Snowden beginning in 2013 indicate that

<https://www.eff.org/deeplinks/2013/06/director-national-intelligences-word-games-explained-how-government-deceived>.

⁸ USSID 18, October 20, 1980, <http://cryptome.org/nsa-ussid18-80.htm> (accessed February 12, 2014), Section 3.4.

⁹ John Napier Tye, “Meet Executive Order 12333: The Reagan rule that lets the NSA spy on Americans,” WASH. POST, July 18, 2014, available at https://www.washingtonpost.com/opinions/meet-executive-order-12333-the-reagan-rule-that-lets-the-nsa-spy-on-americans/2014/07/18/93d2ac22-0b93-11e4-b8e5-d0de80767fc2_story.html.

¹⁰ Privacy and Civil Liberties Oversight Board, REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (2014), available at <https://www.pclob.gov/library/702-Report.pdf>.

¹¹ Ashley Gorski & Patrick Toomey, “Unprecedented and Unlawful: The NSA’s ‘Upstream’ Surveillance,” ACLU, Sept. 23, 2016, <https://www.aclu.org/blog/speak-freely/unprecedented-and-unlawful-nasas-upstream-surveillance>.

these companies include, among others, Internet giants such as Google, Apple, and Facebook.¹²

The purposes for which the government may monitor communications under Section 702 are broad and provide a great deal of latitude: the executive branch need only certify that “a significant purpose” of the surveillance is to obtain “foreign intelligence information.”¹³ The latter term is expansively defined to include, for example, “information with respect to a foreign power or foreign territory that relates to ... the conduct of the foreign affairs of the United States.”¹⁴

Surveillance under Section 702 must formally “target” a non-US person outside of the United States, such as a French national in France.¹⁵ While the Foreign Intelligence Surveillance Court (“FISC”) must annually approve targeting and other procedures that are intended to provide certain protections for US persons,¹⁶ neither the FISC nor any other independent body authorizes or reviews individual targeting decisions or is obligated to ensure that the human rights of non-US persons are respected. (The FISC itself is a problematic body, as many of its operations are secret.)¹⁷

Moreover, though the executive branch claims its acquisition of information is “targeted,” Section 702 appears to authorize the government to capture a potentially very large number of communications “incidentally.”¹⁸ When the *Washington Post* evaluated a set of 160,000 leaked e-mails and instant messages the agencies had gathered under Section 702, it found that 90 percent of the account holders to whom the communications belonged were not the “targets” of this surveillance.¹⁹

We believe Section 702 does not comply with the US Constitution and therefore violates the “legality” prong of the right to privacy. Additionally, while an elaborate set of rules and decisions formally govern surveillance under the law,²⁰ they do not require judicial review of the monitoring on an individualized basis, permit unnecessary and disproportionate interferences with privacy rights, do not include adequate safeguards

¹² See “NSA slides explain the PRISM data-collection program,” WASH. POST, July 10, 2013, <http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/>.

¹³ 50 USC § 1881a(g)(2)(A)(v).

¹⁴ 50 USC § 1801(e).

¹⁵ 50 USC § 1881a(a)-(b).

¹⁶ 50 USC § 1881a(d)-(e), 50 USC § 1801(h).

¹⁷ For more information on the FISA Court, see generally Elizabeth Goitein & Faiza Patel, WHAT WENT WRONG WITH THE FISA COURT? (2015), available at https://www.brennancenter.org/sites/default/files/publications/What_Went_%20Wrong_With_The_FISA_Court.pdf.

¹⁸ See, e.g., Brief of Amicus Curiae, United States Foreign Intelligence Surveillance Court, Oct. 16, 2015, p. 11, available at <https://www.aclu.org/foia-document/brief-fisc-amicus-curiae-amy-jeffress?redirect=foia-document/brief-amicus-curiae> (“The scope of the incidental collection is broad”); Robyn Greene, “It’s Not Just Trump. We Are All Victims of ‘Incidental Collection’,” *Newsweek*, Mar. 28, 2017, <http://www.newsweek.com/its-not-just-trump-we-are-all-victims-incidental-collection-574776>.

¹⁹ Barton Gellman et al., “In NSA-intercepted data, those not targeted far outnumber the foreigners who are,” WASH. POST, July 5, 2014, available at https://www.washingtonpost.com/world/national-security/in-nsa-intercepted-data-those-not-targeted-far-outnumber-the-foreigners-who-are/2014/07/05/8139adf8-045a-11e4-8572-4b1b969b6322_story.html?tid=a_inl&utm_term=.6fc55f584d8c.

²⁰ Office of the Director of National Intelligence, “Release of the FISC Opinion Approving the 2016 Section 702 Certifications and Other Related Documents,” May 11, 2017, <https://icontherecord.tumblr.com/post/160561655023/release-of-the-fisc-opinion-approving-the-2016>.

against discriminatory decision-making, and do not provide meaningful access to an effective remedy. We are also concerned about the potentially disparate impact of these activities on US immigrants and border communities.²¹

Section 702 expires at the end of 2017 and the debate about whether to reauthorize the law, and in what form, is under way among US policymakers. It is also under challenge in a lawsuit in which Human Rights Watch was a plaintiff.²² We encourage you to meet with members from the House and Senate Judiciary Committees, as well as civil society and industry groups, to discuss concerns about the law and how to ensure it comports with international human rights standards.

III. Intelligence-sharing Agreements

EO 12333 allows the Director of National Intelligence to “enter into intelligence and counterintelligence arrangements and agreements with foreign governments and international organizations.”²³ These agreements do not require the approval of the legislature.

Although the executive branch has released certain historic documents concerning an agreement between the US and the United Kingdom,²⁴ and Edward Snowden disclosed to journalists a memorandum of understanding suggesting that the US shares raw surveillance data with Israel,²⁵ we are unaware of any intelligence-sharing arrangements whose current scope or details the government has made available to the public.

In a 2014 interview with Human Rights Watch, a senior US intelligence official claimed that the government is permitted to *receive* intelligence concerning US persons from foreign States even in circumstances where it would be illegal for the US to conduct the surveillance itself, although the authorities cannot *request* such intelligence.²⁶

More recently, during the Senate Select Committee on Intelligence’s confirmation hearing for Mike Pompeo, now CIA Director, Senator Ron Wyden stated:

Absent a specific request from the CIA, a foreign partner, company, organization or individual may nonetheless provide the CIA with the results of extensive cyber operations or other surveillance, including targeted collection against, or bulk collection that includes the

²¹ Sarah St.Vincent, “How US Intelligence Surveillance May Affect Immigrants,” Feb. 21, 2017, <https://www.hrw.org/news/2017/02/21/how-us-intelligence-surveillance-may-affect-immigrants>.

²² *Wikimedia et al. v. National Security Agency*, case no. 1:15-cv-00662 (United States District Court of Maryland), complaint, filed March 10, 2015, <https://www.aclu.org/legal-document/wikimedia-v-nsa-complaint>.

²³ EO 12333, s. 1.4(b)(4)(A).

²⁴ National Security Agency/Central Security Service, “UKUSA Agreement Release: 1940-1956,” May 3, 2016, <https://www.nsa.gov/news-features/decclassified-documents/ukusa/>.

²⁵ Memorandum of Understanding (MOU) Between the National Security Agency/Central Security Service (NSA/CSS) and the Israeli SIGINT National Unit (ISNU) Pertaining to the Protection of U.S. Persons (undated), available at <http://www.statewatch.org/news/2013/sep/nsa-israel-spy-share.pdf>.

²⁶ Human Rights Watch, WITH LIBERTY TO MONITOR ALL (2014), available at <https://www.hrw.org/report/2014/07/28/liberty-monitor-all/how-large-scale-us-surveillance-harming-journalism-law-and>.

communications of U.S. persons. That information could include the communications of U.S. political figures and political activists, leaders of nonprofit organizations, journalists, religious leaders, businesspeople whose interests conflict with those of President Trump, and countless innocent Americans.²⁷

While the information provided by the senior intelligence official and Wyden focuses on US persons, there are no publicly known strictures that would prevent these remarks from being equally accurate with respect to non-US persons.

As has been widely reported, the US has historically had close intelligence-sharing arrangements with other Anglophone allies (known as the “Five Eyes”) as well as with many other state partners.²⁸ Such intelligence-sharing is a staple of counter-terrorism and law enforcement cooperation. However, these arrangements are almost always a function of executive policy rather than legislation, and the details are withheld from the public.

Human Rights Watch is concerned that the nearly complete opacity of the US’ intelligence-sharing arrangements with other states, as well as the apparent lack of oversight by independent bodies, some of these arrangements may entail or facilitate violations of fundamental rights on a significant scale. We urge you to emphasize to officials in the Administration and Congress that the lack of information and oversight of these arrangements can enable a subversion of domestic controls on state surveillance that would safeguard privacy rights (of both US and non-US persons), and violate the principle of legality.

IV. Parallel Construction

In 2013, Reuters reported that a “secretive” unit within the Drug Enforcement Administration (“DEA”), the Special Operations Division, was furnishing tips to US law enforcement agents based on intelligence surveillance data, while instructing those agents to create an alternative explanation for how they found any resulting evidence—thus concealing the original tip.²⁹ This practice, known as “parallel construction,” prevents criminal defendants (and, potentially, even judges) from discovering the true origins of information employed in the investigations in their cases, and thus from challenging the lawfulness of its collection or dissemination under these authorities.

DEA training materials disclosed in response to a subsequent Freedom of Information Act request confirm this practice and discuss legal and policy rationales for it.³⁰ Other government documents, as well as a senior DEA official quoted by Reuters, suggest that

²⁷ Senate Select Committee on Intelligence, “Questions for the Record: Mike Pompeo” (completed), Jan. 18, 2017, p. 5, <https://www.intelligence.senate.gov/sites/default/files/documents/qfr-011217.pdf>.

²⁸ See, e.g. Privacy International, “Eyes Wide Open,” <https://www.privacyinternational.org/sites/default/files/Eyes%20Wide%20Open%20v1.pdf> and Privacy International, *The Five Eyes* <https://www.privacyinternational.org/node/51>.

²⁹ John Shiffman & Kristina Cooke, “Exclusive: U.S. directs agents to cover up program used to investigate Americans,” Reuters, Aug. 5, 2013, <http://www.reuters.com/article/us-dea-sod-idUSBRE97409R20130805>.

³⁰ These materials are available for perusal at Muckrock, “DEA policies on ‘parallel construction’,” <https://www.muckrock.com/foi/united-states-of-america-10/dea-policies-on-parallel-construction-6434/#file-15532>.

the technique is so longstanding that it may have become a “bedrock concept.” One now-declassified 1983 document suggests that the practice dates back years. It addressed the “problem” of “how to maximize dissemination to and use of intelligence by law enforcement agencies while maintaining appropriate security standards for that intelligence.” One aspect of this “problem,” according to the document, arose from “federal criminal procedures which enable a defendant to seek through a discovery motion relevant information regarding any evidence presented by the prosecution.”³¹ As a solution to the problem, the document explicitly contemplates recommending:

[I]ntelligence support processes for drug enforcement that will enable drug agencies to develop intelligence independently and reduce the likelihood that intelligence sources and methods will be regarded essential to a criminal defendant’s case; in effect, build a firebreak in the evidentiary trial [*sic*] leading to sources and methods.³²

We fear that viewing the defendants’ prospective access to intelligence-based evidence as a problem, rather than a right, may remain current and widespread within US intelligence and law enforcement agencies. We are concerned that practices such as parallel construction—which, according to the same senior official quoted by Reuters, is employed “every day”—undermine fair-trial rights and risk weakening the integrity of the US criminal justice system overall. The issue merits far greater congressional, judicial, and public scrutiny than it has received. We look forward to discussing it further with you during your visit, and hope it will be an issue you raise with law enforcement officials you meet, including in the FBI, DEA, and Department of Justice.

V. Encryption³³

Concerted advocacy by industry, information security technologists, and digital rights organizations successfully opposed efforts in the US to weaken encryption last year. When media organizations released a “discussion draft” of Senators Dianne Feinstein and Richard Burr’s Compliance with Court Orders Act in April 2016, widespread criticism of the bill’s negative effects on cybersecurity, privacy, and other rights led the sponsors to decline to formally introduce the proposal.³⁴ The bill would have required technology companies to provide access to encrypted information in an “intelligible format” (that is, unencrypted) if asked to by a court. The bill does not specify how companies would have to unscramble encrypted information, but it would have effectively forced a range of

³¹ Terms of Reference: CIPC Narcotics Working Group’s Panel on the Use of Classified Intelligence Information by Drug Enforcement Agencies, Sept. 19, 1983, available at https://www.hrw.org/sites/default/files/supporting_resources/cipc_narcotics_working_group.pdf.

³² *Ibid.*

³³ For HRW’s full analysis of encryption and human rights, see Human Rights Watch, Comments Submitted to the UN Special Rapporteur on the Protection and Promotion of the Right to Freedom of Opinion and Expression On the Use of Encryption and Anonymity in Digital Communications, February 18, 2015, <https://www.hrw.org/news/2015/02/18/comments-submitted-un-special-rapporteur-protection-and-promotion-right-freedom>.

³⁴ Cynthia Wong, “Dispatches: Regressive US Encryption Bill Harms Security,” April 8, 2016, <https://www.hrw.org/news/2016/04/08/dispatches-regressive-us-encryption-bill-harms-security>.

companies to build in a “back door” to bypass encryption and other security features in products.

However, the delay in formal introduction of this bill appears to have been only a temporary reprieve. US law enforcement officials continue to pressure major tech companies to roll back security improvements they have begun to adopt, including end-to-end encrypted chat applications and default disk encryption, and demand legislation to mandate exceptional access.³⁵ Although President Barack Obama declined to pursue legislation, he also failed to take a strong stance against encryption backdoors—or any firm position on the matter.³⁶ On several separate occasions before former FBI Director James Comey’s dismissal, including in testimony before Congress, Comey raised the need for some “solution” to widespread encryption.³⁷ Senators Feinstein and Burr also reportedly circulated a revised draft of their anti-encryption bill in September, though the exact details haven’t been made public.³⁸

In short, we believe it very likely that various quarters of government, federal and state, will continue to demand that companies weaken encryption and allow exceptional law enforcement access to encrypted communications. Forcing companies to remove end-to-end encryption will weaken security for all Internet and mobile phone users, while being ineffective at keeping encryption out of the hands of determined malicious actors. In the digital age, strong encryption is essential for the enjoyment of the right to communicate anonymously and privately. Online communications flow over Internet networks that are inherently vulnerable to covert and unwanted monitoring by state and non-state actors. Our digital data is also increasingly stored remotely with cloud service providers, whom we rely on to ensure data is not breached without authorization.

Privacy online in the twenty-first century hinges entirely on strong encryption. And unfortunately, weak or partial encryption provides not just weak or partial protection, but no protection at all to well-equipped intelligence agencies and capable hackers. Thus, the ICCPR requires that any limits on strong encryption, including a state mandate to require decryption of data, must be provided in law, proportionate, and necessary for a legitimate aim. In our advocacy with the US government on the issue, we have argued that a requirement of assured decryptability for all online communications, including the billions that involve no suspicion of threat to public order or national security, could not

³⁵ See Joseph Marks, "New York DA to Trump: Have Our Backs Against Cop-Proof Encryption," NextGov, February 17, 2017, <http://www.nextgov.com/cybersecurity/2017/02/new-york-prosecutor-trump-have-our-backs-against-cop-proof-encryption/135526/>.

³⁶ Joint letter to President Barack Obama Re: Encryption, October 27, 2016, <https://www.hrw.org/news/2016/10/27/joint-letter-president-obama-re-encryption>.

³⁷ Taylor Armerding, "Comey: Strong encryption “shatters” privacy-security bargain," CSO ONLINE, March 8, 2017, <http://www.csoonline.com/article/3178299/security/comey-strong-encryption-shatters-privacy-security-bargain.html>; Michael Kan, "FBI director floats international framework on encrypted data access," COMPUTERWORLD, March 23, 2017, <http://www.computerworld.com/article/3184478/security/fbi-director-floats-international-framework-on-encrypted-data-access.html>; Lorenzo Franceschi-Bicchierai, "The FBI Director Thinks a Law Against Encryption Is Possible Under Trump," MOTHERBOARD, May 3, 2017, https://motherboard.vice.com/en_us/article/fbi-director-comey-law-against-encryption-trump.

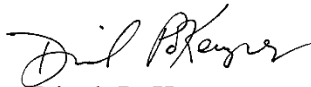
³⁸ Julian Sanchez, "Feinstein-Burr 2.0: The Crypto Backdoor Bill Lives On," JUST SECURITY, September 9, 2016, <https://www.justsecurity.org/32818/feinstein-burr-2-0-crypto-backdoor-bill-lives>.

be proportionate and has never been shown to be necessary. The law, including human rights law, does not view every member of society as a suspect when speaking online.

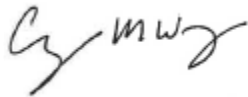
We urge you to raise the importance of strong encryption for the protection of privacy and other human rights with federal and state law enforcement officials and Congressional policymakers as part of your US visit.

There are, of course, many other issues relating to other aspects of privacy as well as privacy and digital technology that are both of concern to Human Rights Watch and deserving of your attention. We are happy to facilitate your visit in any way we can, including by convening a meeting with other NGOs, and by meeting with you in person, either in advance or at the time of your visit. An appendix of our reports and work relevant to your visit is attached.

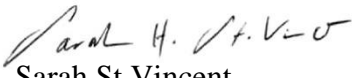
Sincerely,



Dinah PoKempner
General Counsel



Cynthia M. Wong
Senior Internet Researcher



Sarah St. Vincent
Researcher/Advocate on US Surveillance, National Security, and Domestic Law Enforcement

Encl.: Appendix

Appendix

[*With Liberty to Monitor All*](#) (July 28, 2014)

An investigative report on how large-scale US surveillance is harming journalism and legal practices.

[“Broad Warrantless Surveillance Threatens to Undermine the Criminal Justice System”](#)

(April 26, 2017)

A post for *Just Security* about newly released government documents that highlights the need to ask hard questions about US warrantless surveillance practices and their impact on fair-trial rights.

[“How US Intelligence Surveillance May Affect Immigrants”](#) (February 21, 2017)

A dispatch about the potential impact of US intelligence surveillance on immigrants, minorities, and border communities.

[“US: Curb Executive Branch Surveillance Powers”](#) (March 2, 2017)

A press release containing basic information about Section 702 of the FISA, issued following a House Judiciary Committee hearing on the potential re-authorization of the law.

[“Is the Privacy of Europeans at Risk?”](#) (March 1, 2017)

A dispatch and joint letter raising concerns about the flawed US-EU Privacy Shield.

[“Fact Sheet: Impact of Warrantless Section 702 Surveillance on People in the United States”](#) (March 1, 2017)

A fact sheet about Section 702 surveillance, with an emphasis on the impact on US persons.

[“Your Papers and Social Media Passwords, Please”](#) (February 21, 2017)

A dispatch on a US proposal to require visa applicants and visitors to disclose social media passwords to US authorities.

[“A little-noticed move by Trump could make it easier to deport immigrants”](#) (January 27, 2017)

A Washington Post article by Craig Timberg and Jerry Markon, highlighting an issue Human Rights Watch helped bring to light.

[“National Security Agency Databases Open for Business”](#) (January 13, 2017)

A dispatch examining how new guidelines will allow 16 US intelligence agencies to search certain NSA surveillance databases.

[“Unchecked Presidential Surveillance Powers are Dangerous”](#) (November 17, 2016)

A dispatch explaining why US intelligence surveillance powers are a recipe for abuse by the executive branch, including the (then-incoming) Trump Administration.

[“US Still Dodging Questions on Yahoo! Spying”](#) (October 26, 2016)

A dispatch about secret laws, rules, and legal interpretations concerning US surveillance.

["Why President Obama Should Pardon Edward Snowden Now"](#) (September 14, 2016)

An appeal to President Obama to grant a pardon to Edward Snowden.

[“Baltimore Police Stretch Laws to Spy on Thousands”](#) (August 30, 2016)

A dispatch concerning police aerial surveillance in Baltimore that stretched a legal loophole and may have violated human rights.

[“US Surveillance Court Opinion Shows Harm to Rights”](#) (April 22, 2016)

A dispatch about a then-newly declassified FISA Court opinion that bolstered concerns about the FBI’s “backdoor queries” of Section 702 surveillance data.

["Regressive US Encryption Bill Harms Security"](#) (April 8, 2016)

A dispatch raising privacy and security concerns related to the Burr-Feinstein anti-encryption bill, the Compliance with Court Orders Act.

["Apple’s Standoff and Security for All"](#) (February 18, 2016)

A dispatch on the FBI vs. Apple encryption case.

["Yahoo and the Death of User Trust"](#) (October 5, 2016)

A dispatch on the role and responsibilities of major US Internet companies in safeguarding user rights.

Submissions to UN bodies:

[Joint Submission Re. National Security Surveillance and Human Rights in a Digital Age for the 2015 Universal Periodic Review of the United States](#) (July 1, 2014)

[Joint Submission to OHCHR Consultation in Connection with General Assembly Resolution 68/167 “The Right to Privacy in the Digital Age”](#) (April 1, 2014)

[Human Rights Watch and the Electronic Frontier Foundation Supplemental Submission to the Human Rights Committee During its Consideration of the Fourth Periodic Report of the United States](#) (February 14, 2014)