Mr. Bruno Gencarelli
Head of Unit, Directorate-General Justice and Consumers
European Commission
Rue de la Loi / Wetstraat 200
1049 Brussels
Belgium

October 2, 2017

Dear Mr. Gencarelli:

Thank you for your outreach to civil society as part of your review of *Implementing Decision 2016/1250 on the adequacy of the protection provided by the EU-U.S. Privacy Shield* (Implementing Decision). The undersigned organizations write to address two matters in which you have recently expressed interest in relation to the review. These include the possibility that authorities in the United States of America (United States) may be able to gain access to personal data stored in the country by relying on Executive Order 12333 (EO 12333), and the authorities' potential use of parallel construction to conceal from defendants and judges the fact that intelligence surveillance data has been employed in a criminal investigation.

1. Access under Executive Order 12333 to Personal Data Stored in the United States

You have asked whether, under EO 12333, the US authorities have the power to obtain access to personal data that companies store in the United States.

As an initial matter, we note that the executive branch has revealed little information publicly about how it interprets its surveillance authorities under EO 12333. The government also has a documented history of adopting interpretations of surveillance laws that—in violation of human rights—are not clearly foreseeable based on the text of those laws.[1] It is therefore difficult for civil society members to state with certainty what powers the government exercises or could exercise under EO 12333.

However, we are aware of several potential legal loopholes that could enable the US authorities to use EO 12333 to obtain warrantless access to personal data transferred from the European

[1] See Mattathias Schwartz, "The Rabbit-Hole of 'Relevant'," N.Y. TIMES, June 23, 2015, https://www.nytimes.com/2015/06/28/magazine/the-rabbit-hole-of-relevant.html (discussing the government's expansive interpretation of the term "relevant" as it appeared in Section 215 of the USA Patriot Act prior to reforms adopted in 2015 in the USA Freedom Act, facilitating the bulk collection of United States telephone records); New America Open Technology Institute, "OTI Applauds End to NSA 'About Collection,' Urges Statutory Reform of Section 702," Apr. 28, 2017, https://www.newamerica.org/oti/press-releases/oti-applauds-end-nsa-about-collection-urges-statutory-reform-section-702/ (discussing lack of clear congressional intent to authorize the National Security Agency's practices of "upstream" searches and "about" collection under Section 702 of the Foreign Intelligence Act); *Schrems v. Data Protection Commissioner* (C-362/14), judgment, Oct. 6, 2015, ¶ 91 (indicating that interferences with privacy and other relevant rights must be subject to "clear and precise rules governing the scope and application" of the measures in question); *Malone v. United Kingdon*, application no. 8691/79, judgment (European Court of Human Rights, plenary), Aug. 2, 1984, ¶ 67 (establishing that a law permitting government surveillance that interferes with the right to privacy must be "sufficiently clear in its terms to give citizens an adequate indication as to the circumstances" in which this may take place).

Union and stored by companies in the United States. We note that the Privacy and Civil Liberties Oversight Board (which is currently inoperative due to vacancies) had previously expressed an intention to review and report on "collection that occurs within the United States or from U.S. companies" under EO 12333, suggesting that the Board viewed such collection as a possibility.[2]

At present, the broader question of whether officials are or should normally be required to obtain a warrant to gain access to the stored content of electronic communications remains the subject of constitutional and legislative debate.[3] The court of appeals in one federal jurisdiction has issued an important ruling finding that individuals have a reasonable expectation of privacy in their stored e-mails that are held by a service provider, and therefore that the warrant requirement found in the Fourth Amendment to the US Constitution applies (in the absence of a valid exception).[4] However, although the Justice Department has generally adopted a policy of using warrants to compel the disclosure of the content of communications stored by providers[5], we are not aware of any expression by the government of a conclusion that it is legally obligated to do so.

To the extent that the government believes it must normally obtain a warrant to gain access to a stored communication, Section 2.5 of EO 12333 grants it the power to avoid doing so in potentially broad circumstances. The provision states that the Attorney General has "the power to approve the use for intelligence purposes, within the United States … of any technique for which a warrant would be required if undertaken for law enforcement purposes," as long as "the Attorney General has determined in each case that there is probable cause to believe that the technique is directed against a foreign power or an agent of a foreign power."[6] It is unclear how the government may be interpreting this potentially broad reference to "the technique"—a term that may be susceptible to a construction that permits bulk or large-scale surveillance affecting individuals who could not legitimately be regarded as "foreign power[s]" or agents thereof.

Section 2.5 of EO 12333 further provides that the power it grants, "including the authority to approve the use of electronic surveillance as defined in the Foreign Intelligence Surveillance Act of 1978" (FISA), must be "exercised in accordance with that Act."[7] However, we do not know the extent to which the government interprets FISA's definition of "electronic surveillance" as applying to communications stored by a service provider.[8]

---

[2] Privacy and Civil Liberties Oversight Board, "PCLOB Examination of E.O. 12333 Activities in 2015," undated, https://pclob.gov/library/20150408-eo12333_project_description.pdf.
[3] See Electronic Frontier Foundation, "EFF Supports Senate Email and Location Privacy Bill," July 27, 2017, https://www.eff.org/deeplinks/2017/07/eff-applauds-senate-email-and-location-privacy-bill; United States v. Warshak, 631 F.3d 266 (6th Cir. 2010), available at http://www.opn.ca6.uscourts.gov/opinions.pdf/10a0377p-06.pdf.
[4] Warshak, *supra* n. 3.
[5] See In re Search of Information Associated with [Redacted]@gmail.com that Is Stored at Premises Controlled by Google, Inc., Case No. 16-mj-00757 (D.D.C.), Memorandum Opinion, July 31, 2017, available at http://www.dcd.uscourts.gov/sites/dcd/files/Google_FINAL_UNSEALED_20170731.pdf.
[6] Executive Order 12333: United States Intelligence Activities, as amended, § 2.5, available at https://fas.org/irp/offdocs/eo/eo-12333-2008.pdf.
[7] *Id.*
[8] The definition appears at 50 U.S.C. § 1801(f), available at https://www.law.cornell.edu/uscode/text/50/1801 and reproduced in an annex to this letter.

Even if the government believes the definition applies, the specific terms of the definition appear to render it applicable only to monitoring that "intentionally target[s]" a known United States person[9] who is in the United States; the acquisition in the United States of communications to or from a United States person; the intentional acquisition of a communication when all the parties to that communication are in the United States; and the installation or use of a surveillance device in the United States for monitoring that would require a warrant if done for law enforcement purposes.[10] This definition contains multiple potential loopholes that the government may be able to use to gain warrantless access to stored communications or other personal data on the basis of EO 12333: for example, when the surveillance employs methods executed or devices used outside the United States, and/or when it is not intended to acquire the communications of a US person or communications that take place solely between people in the United States. Such loopholes would leave much prospective leeway for the United States government to gain access to communications—especially those of non-United States persons—under EO 12333.

We encourage the European Commission to ask the United States executive branch to provide clear and comprehensive explanations on these points; we also encourage the Commission to make any such explanations it receives available to the public.

2. Parallel Construction

In the context of discussions of whether the United States provides adequate notification to individuals who have been monitored as well as access to effective redress, you have also indicated an interest in the practice known as "parallel construction."

In brief, "parallel construction" is a term that describes deliberate efforts by US government officials or agencies, as part of an investigation or prosecution, to conceal the true origins of evidence by creating an alternative explanation for how the authorities discovered it. The practice was initially brought to the public's attention by the news agency Reuters in August 2013. Focusing on the Drug Enforcement Administration (DEA), journalists John Shiffman and Kristina Cooke found that a "secretive" unit known as the Special Operations Division was "funneling information from intelligence intercepts, wiretaps, informants and a massive database of telephone records to authorities across the nation to help them launch criminal investigations of Americans." Documents they had obtained, the reporters wrote, showed that "federal agents are trained to 'recreate' the investigative trail to effectively cover up where the information originated," including by staging pretextual traffic stops and subsequent searches.[11] The reporters quoted an anonymous senior DEA official who depicted the practice as "a bedrock concept" that is "decades old" and that the government employs daily.[12]

---

[9] Under FISA, "United States person[s]" include United States citizens, lawful permanent residents, and some corporations and associations. 50 U.S.C. § 1801(i).
[10] *Supra* n. 8.
[11] John Shiffman & Kristina Cooke, "Exclusive: US directs agents to cover up program used to investigate Americans," Reuters, Aug. 5, 2013, http://www.reuters.com/article/us-dea-sod/exclusive-u-s-directs-agents-to-cover-up-program-used-to-investigate-americans-idUSBRE97409R20130805.
[12] *Id.*

Reuters subsequently reported that a manual available to Internal Revenue Service personnel between 2005 and 2007 had described the practice of parallel construction and "instructed agents of the U.S. tax agency to omit any reference to tips supplied by the DEA's Special Operations Division, especially from affidavits, court proceedings or investigative files."[13] In 2014, journalist CJ Ciaramella obtained and released DEA training materials concerning parallel construction pursuant to a freedom of information request.[14]

Attorneys at multiple civil society organizations have published analyses expressing concerns about the possibility that the United States government may use parallel construction to avoid notifying criminal defendants about any intelligence surveillance involved in their cases.[15] Human Rights Watch expects to publish research addressing this issue during the next several months.

* * *

We hope this information assists your review of the Implementing Decision. Please do not hesitate to contact us for further details regarding these matters.

Sincerely,

Access Now

Amnesty International

Electronic Frontier Foundation

Human Rights Watch

[13] John Shiffman & David Ingram, "Exclusive: IRS manual details DEA's use of hidden intel evidence," REUTERS, Aug. 7, 2013, http://www.reuters.com/article/us-dea-irs/exclusive-irs-manual-detailed-deas-use-of-hidden-intel-evidence-idUSBRE9761AZ20130807.

[14] See Shawn Musgrave, "DEA teaches agents to recreate evidence chains to hide methods," MUCKROCK, Feb. 3, 2014, https://www.muckrock.com/news/archives/2014/feb/03/dea-parallel-construction-guides/.

[15] See, e.g., Patrick C. Toomey, "Why Aren't Criminal Defendants Getting Notice of Section 702 Surveillance—Again?", JUST SECURITY, Dec. 11, 2015, https://www.justsecurity.org/28256/arent-criminal-defendants-notice-section-702-surveillance-again; Sarah St.Vincent, "We Have Good Reason to Be Concerned About the Impact of Section 702 on the Criminal Justice System," JUST SECURITY, June 7, 2017, https://www.justsecurity.org/41811/good-reasons-concerned-impact-section-702-criminal-justice-system/; Michelle Richardson, Statement for the Record, Senate Judiciary Committee, June 27, 2017 Hearing on the FISA Amendments Act: Reauthorizing America's Vital National Security Authority and Protecting Privacy and Civil Liberties, undated, https://cdt.org/files/2017/06/CDT-Statement-for-the-Record-SJC-FISA-hearing-June-27-2017.pdf.

Annex: Definition of "Electronic Surveillance" for Purposes of the Foreign Intelligence Surveillance Act

As per 50 U.S.C. § 1801(h), the term "electronic surveillance" for the purposes of the Foreign Intelligence Surveillance Act of 1978, as amended, means:

> ***(1)*** *the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication sent by or intended to be received by a particular, known United States person who is in the United States, if the contents are acquired by intentionally targeting that United States person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes;*
>
> ***(2)*** *the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs in the United States, but does not include the acquisition of those communications of computer trespassers that would be permissible under section 2511(2)(i) of title 18;*
>
> ***(3)*** *the intentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States; or*
>
> ***(4)*** *the installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information, other than from a wire or radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes.*