A paper shield does not protect privacy – Privacy International's analysis of the "Privacy Shield" safeguards on surveillance

8 April 2016

1. Introduction

On 29 February 2016, the European Commission and the US government released the details of the proposed EU-U.S. "Privacy Shield".[1] The "Privacy Shield" replaces the now defunct so-called "Safe Harbor".[2]

The Privacy Shield is in fact a significant number of documents from various parts of the U.S. administration, which merely outline the existing, weak U.S. safeguards applicable to personal data of EU citizens. These documents are meant to serve as the basis for an "adequacy" decision by the European Commission that the U.S. has a data protection regime that is essentially equivalent to that applicable in the EU. In making that decision, the European Commission must also review issues related to government surveillance and consumer data protection.

Last month Privacy International joined other European and American NGOs in expressing concerns that the "Privacy Shield" will put users at risk, undermine trust in the digital economy, and perpetuate the human rights violations that are already occurring as a result of surveillance programs and other activities.[3]

We have now analysed in detail the government surveillance aspects of the proposed personal data transfers arrangements, and have found the shield isn't operational. These are our main conclusions:

- The "Privacy Shield" does not significantly limit the ability of US intelligence agencies to collect and use personal communications on a mass scale. Instead, it allows for "generalised" retention of personal data in ways contrary to the Schrems' judgment (https://cdt.org/blog/making-privacy-a-reality-the-safe-harbor-judgment-and-its-consequences-for-us-surveillance-reform/).

---

[1] See: http://europa.eu/rapid/press-release_IP-16-433_en.htm

[2] In its recent Schrems' judgment, the EU Court of Justice annulled the "Safe Harbour" because it could not adequately protect against generalized access (read mass surveillance) of personal data by US public authorities and because the US legislation did not give EU citizens the right to effective legal remedies. See https://www.privacyinternational.org/node/654

[3] See: https://www.accessnow.org/cms/assets/uploads/2016/03/Priv-Shield-Coalition-LtrMar2016.pdf

- The Presidential Directive (PPD-28) imposes new rules limiting the use and dissemination of non-U.S. persons' information. However, it does not limit its bulk collection.
- The "Privacy Shield" provides a weaker standard ("as tailored as feasible" and "reasonable") than the test of necessity and proportionality required under international human rights law.
- The proposed Ombudsperson lacks independence from the executive, as he/she is appointed by and reports to the Secretary of State.

The coming months will be crucial in revealing if the "Privacy Shield" in its current form will pass the "adequacy" test, when challenged, and be deemed sufficient to protect the privacy of EU citizens. Most notably, next week the European data protection authorities (Article 29 Working Party) are due to adopt its opinion on the draft Commission adequacy decision based on the "Privacy Shield".

END OF BLOG

2. "Privacy Shield" and U.S. surveillance

Privacy International has reviewed the main features of the current "Privacy Shield" as they pertain to the limitation of access to personal data of EU citizens by U.S. intelligence and law enforcement agencies. [4] The brief analysis below compares the provisions contained in these documents to the relevant findings in the Schrems' judgment and other European case law on surveillance and the right to privacy, including recent judgments by the European Court on Human Rights in Szabó and Vissy v. Hungary and Zakharov v. Russia.[5]

2.1 Bulk collection, "use" of bulk data and retention of personal data

Privacy Shield	**Schrems' judgment**
"PPD-28 […] provides that signals intelligence collected in bulk can only be used for six specific purposes: detecting and countering certain activities of foreign powers;	"Legislation is not limited to what is strictly necessary where it authorises, on a generalised basis, storage of all the personal data of all the persons whose data has been transferred from the

[4] The limits and safeguards of access by U.S. authorities of personal data under U.S. laws and policies are elaborated in the representations by the Office of Director of National Intelligence related to foreign intelligence (Annex VI); and the US Department of Justice (Annex VII) related to access of data for law enforcement and other public interest purposes. Further, the US State Department outlines, in Annex III, the functions and powers of the Ombudsperson, as a venue for redress. As the EU Commission draft adequacy decision refers to these representations, which are considered to be part of the "Privacy-Shield", references are made to them (rather than the text of the existing US laws).

[5] European Court of Human Rights, *Zakharov v Russia* (2015) and European Court on Human Rights, Case of Szabó and Vissy v. Hungary (2015).

counterterrorism; counter-proliferation; cybersecurity; detecting and countering threats to U.S. or allied armed forces; and combating transnational criminal threats, including sanctions evasion." (Annex VI) "The priorities in the National Intelligence Priorities Framework [which is classified] are at a fairly high level of generality." [Annex VI] "It is important to emphasize that any bulk collection activities regarding Internet communications that the U.S. Intelligence Community performs through signals intelligence operate on a small proportion of the Internet. Additionally, the use of targeted queries, as described above, ensures that only those items believed to be of potential intelligence value are ever presented for analysts to examine. These limits are intended to protect the privacy and civil liberties of all persons, whatever their nationality and regardless of where they might reside." (Annex VI) "Information […] may not be retained for more than five years, unless […] continued retention is in the national security interests of the United States." (Annex VI)	European Union to the United States without any differentiation, limitation or exception being made in the light of the objective pursued and without an objective criterion being laid down by which to determine the limits of the access of the public authorities to the data, and of its subsequent use, for purposes which are specific, strictly restricted and capable of justifying the interference which both access to that data and its use entail."

Bulk Collection

Bulk collection amounts to mass surveillance and it infringes upon the right to privacy. The Presidential Privacy Directive (PPD-28) does not significantly limit the ability of US intelligence agencies to collect and use personal communications on a mass scale. Instead, it allows for "generalized" retention of personal data in ways contrary to Schrems' judgment.

Bulk interception and collection of personal data is an impermissible interference with the right to privacy because of its indiscriminate nature. In a judgment last year, the Grand Chamber of the European Court of Human Rights considered the use of surveillance powers and the level of specificity needed to ensure interception powers were not used arbitrarily. It confirmed that to ensure the test of necessity

and proportionality had been properly applied the interception authorisation must clearly identify "a specific person to be placed under surveillance or a single set of premises as the premises in respect of which the authorisation is ordered. Such identification may be made by names, addresses, telephone numbers or other relevant information."[6]

As noted by the UN Special Rapporteur on the right to privacy, "this decision sets up a very important benchmark highlighting as it does the requirements for reasonable suspicion and prior judicial authorisation as well as the unacceptable nature of 'a system…which enables the secret service and the police to intercept directly the communications of each and every citizen without requiring them to show an interception authorisation'."[7]

Distinction between collection and "use"

The Presidential Directive (PPD-28) imposes new rules limiting the use and dissemination of non-U.S. persons' information. However, it does not limit bulk collection.

Section 2 of the PPD-28 only restricts the "use" of intelligence collected in bulk. That does not limit bulk collection or acquisition of data per se. In fact footnote 5 in that section notes that "the limitations contained in this section do not apply to signals intelligence data that is temporarily acquired to facilitate targeted collection". This means that the limits on the use of bulk collection do not apply to data that is collected or acquired in bulk and held for a "temporary" and unspecified period of time in order to facilitate "targeted" surveillance.

As such the PPD-28 does not circumscribe the collection of data under Section 702 or Executive Order 12.333, which remain the legal basis for bulk collection of foreign intelligence information -- the main concern raised in Schrems' judgment.

The Draft EU Commission adequacy decision seeks to distinguish between collection and use. In paragraph 63, the draft decision notes that "even where *bulk collection* cannot be avoided, further "use" of such data through access is *strictly limited* to specific, legitimate national security purposes."

However, as supported by relevant jurisprudence, any capture of communications (including communications data) is potentially an interference with privacy and, further, the collection and retention of such communications amounts to an interference with privacy whether or not those data are subsequently consulted or used. The acquisition or copying of personal information constitute an "interference" with the right to privacy, regardless of whether the information is subsequently processed, examined, or used by the government.

---

[6] European Court of Human Rights, *Zakharov v Russia* (2015), paragraph 264.

[7] UN Special Rapporteur on the right to privacy, UN doc. A/HRC/31/64, 8 March 2016.

The Court of Justice of the European Union has held that bulk "collection" is a disproportionate violation of the rights to privacy and data protection under the Charter of the EU.[8] The European Court of Human Rights has found that storage of personal data can interfere with privacy, and that "subsequent use of stored information has no bearing on that finding."[9] Even the mere possibility of communications information being captured creates an interference with privacy.[10]

Retention of personal data

The Privacy Shield does not require that the necessity and proportionality of keeping personal information on non-U.S. persons be assessed. Instead, under the Presidential Directive (PPD-28), for the first time there is a requirement to delete information on non-U.S. persons within five years.

However, even this provision is qualified, allowing longer retention if the information is "relevant to, among other things, an authorized foreign intelligence requirement," or if "continued retention is in the interest of national security." In addition to this broad exception, different agencies operate under different interpretations of this retention exception. For example, the NSA's procedures except information in unintelligible form, such as encrypted or enciphered information, and emphasize that the deletion requirement applies only to information in its "original and transcribed" form, which could exclude finished intelligence products.[11]

2.2 No test of strict necessity

"Privacy Shield"	**Schrems' judgment**
"U.S. signals intelligence activity must always be as ***tailored as feasible***, taking into account the availability of other sources of information. This means, among other things, that whenever practicable, signals intelligence collection activities are conducted in a targeted manner rather than in bulk" (Annex VI)(emphasis added)	"Protection of the fundamental right to respect for private life at EU level requires derogations and limitations in relation to the protection of personal data to apply only in so far as is ***strictly necessary***." (emphasis added)

[8] See Court of Justice of the European Union, Judgment in Joined Cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and Others, 8 April 2014.
[9] European Court of Human Rights, *Amann v. Switzerland*, 16 February 2000.
[10] European Court of Human Rights, *Klass and others v. Germany,* 6 September 1978.
[11] See Nat'l Sec. Agency, USSID 18 SP0018: Supplemental Procedures for the Collection, Processing, Retention, and Dissemination of Signals Intelligence Information and Data of Non-United States Persons §§ 3.2, 3.4 (2015), available at https://www.nsa .gov/public_info/_files/nsacss_policies/PPD-28.pdf; quoted Daniel Severson, American Surveillance of Non-U.S. Persons: Why New Privacy Protections Offer Only Cosmetic Change, Harvard International Law Journal / Vol. 56, Number 2, Summer 2015.

"As for the concept of '***reasonableness***', it is a bedrock principle of U.S. law. It signifies that Intelligence Community elements will not be required to adopt any measure theoretically possible, but rather will have to balance their efforts to protect legitimate privacy and civil liberties interests with the practical necessities of signal intelligence activities." (Annex VI) (emphasis added)	

The test of necessity under international human rights law requires that the interference with privacy must be strictly and demonstrably necessary to achieve a legitimate aim, such as the protection of national security. This includes proving that the interference is the only means of achieving a legitimate aim, or, when there are multiple means, it is the means least likely to infringe upon human rights. Further, the sensitivity of the information accessed and the severity of the infringement on human rights and other competing interests must also be considered.[12]

Requiring that an interference need only be "as tailored as feasible and "reasonable" is a significantly weaker standard than the necessity requirement under under international human rights law. To satisfy that latter requirement, an interference must be effective to achieve a legitimate aim, necessary (i.e. "least intrusive") and proportionate to the legitimate aim.

The Draft EU Commission adequacy decision states that "targeted collection is clearly prioritised, while bulk collection is limited to (exceptional) situations where targeted collection is not possible for technical or operational reasons" (paragraph 63). And then concluded that "there are rules in place in the United States designed to limit any interference for national security purposes with the fundamental rights of the persons whose personal data are transferred from the Union to the United States under the EU-U.S. Privacy Shield to what is strictly necessary to achieve the legitimate objective in question." (Paragraph 75.)

This contrasts starkly with applicable jurisprudence. In Szabó v. Hungary, the European Court of Human Rights specified that necessity test requires the

[12] See Court of Justice of the European Union, Judgment in Joined Cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and Others, 8 April 2014 and European Court on Human Rights, Case of Szabó and Vissy v. Hungary, paragraph 73. See also reports by UN High Commissioner on Human Rights (2014, UN doc. A/HRC/27/37), UN Special Rapporteur on counter-terrorism (2014, UN doc. A/69/397) and UN Special Rapporteur on freedom of expression (2013, UN doc. A/HRC/23/40).

interference to be “strictly necessary, as a general consideration, for the safeguarding the democratic institutions” *and* “strictly necessary, as a particular consideration, for the obtaining of vital intelligence in an individual operation.” The Court concluded that “any measure of secret surveillance which does not correspond to these criteria will be prone to abuse by the authorities with formidable technologies at their disposal.”[13]

2.3 Redress

Privacy Shield	**Schrems’ judgment**
"Senior Coordinator for International Information Technology Diplomacy" (Senior Coordinator) […] “will serve as the Privacy Shield Ombudsperson” The Ombudsperson is designated by the Secretary of State and “reports directly to the Secretary of State, and is independent from the Intelligence Community.“ (Annex III) “Privacy Shield Ombudsperson will provide in a timely manner an appropriate response to the submitting EU individual complaint handling body, subject to the continuing obligation to protect information under applicable laws and policies. The Privacy Shield Ombudsperson will provide a response to the submitting EU individual complaint handling body confirming (i) that the complaint has been properly investigated, and (ii) that the U.S. law, statutes, executives orders, presidential directives, and agency policies, providing the limitations and safeguards described in the ODNI letter, have been complied with, or, in the event of non-compliance, such non-compliance has been remedied. The Privacy Shield Ombudsperson will neither confirm nor deny whether the individual has been the target of surveillance nor will the Privacy Shield Ombudsperson confirm	“Legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data, does not respect the essence of the fundamental right to effective judicial protection” (paragraph 95)

[13] European Court on Human Rights, Case of Szabó and Vissy v. Hungary, paragraph 73.

the specific remedy that was applied."(Annex III)	

The draft EU Commission adequacy decision notes that the venues of redress in the US for EU data subjects are patchy and limited: "While individuals, including EU data subjects, therefore have a number of avenues of redress when they have been the subject of unlawful (electronic) surveillance for national security purposes, it is equally clear that at least some legal bases that U.S. intelligence authorities may use (e.g. E.O. 12333) are not covered. Moreover, even where judicial redress possibilities in principle do exist for non-U.S. persons, such as for surveillance under FISA, the available courses of action are limited and claims brought by individuals (including U.S. persons) will be declared inadmissible where they cannot show "standing", which restricts access to ordinary courts."[14]

In an effort to address these shortcomings, the Privacy Shield introduces a Privacy Shield Ombudsperson whose role and function is described in a communication from the U.S. State Department (Annex III). The role of the Ombudsperson is to handle complaints from EU citizens concerning access to their personal data by US national intelligence authorities.

The proposed Ombudsperson lacks independence from the executive, as he/she is appointed by and report to the Secretary of State. Contrary to assertions in the draft EU Commission adequacy decision, the independence and impartiality of such a mechanism, including the perception of such independence, is questionable. Concerns about this lack of independence were raised by the EU Ombudsman office.[15]

Further, the Ombudsperson will have limited powers of redress. This is very starkly stated in paragraph 4(e) of Annex III, where it states that "the Privacy Shield Ombudsperson will neither confirm nor deny whether the individual has been the target of surveillance nor will the Privacy Shield Ombudsperson confirm the specific remedy that was applied."

Both of these flaws in the proposed redress mechanism mean it falls short of providing effective redress, as described, for example, in the recommendations by the Council of Europe's Commissioner for human rights.[16]

[14] Draft EU Commission adequacy decision, paragraph 99, footnotes omitted.

[15] See http://www.ombudsman.europa.eu/en/resources/otherdocument.faces/en/64157/html.bookmark

[16] Council of Europe Commissioner for Human Rights, Democratic and effective oversight of national security services, May 2015.