US surveillance practices and its legal system - a short history in light of Schrems II

1. Introduction

In the Schrems II judgement of 16 July 2020[1] the European Court of Justice (ECJ) invalidated the Privacy Shield Decision of the European Commission.[2] The ECJ reasoned that for EU personal data transferred to the US, the Privacy Shield framework could not circumvent the mass surveillance practices in the US and the lack of possibilities for judicial redress for EU citizens subject of such surveillance.

As legal background, the transfer of personal data to recipients outside the EU is restricted under the EU General Data Protection Regulation 2016/679/EC (GDPR) and its predecessor, the EU Data Protection Directive 95/46/EC. Such transfers are allowed if the country of the recipient is deemed by the European Commission to offer an adequate level of personal data protection under EU standards. The list of so-called 'adequate countries' currently includes Canada, New Zealand, Argentina and Japan.[3] The European Commission has never decided on the US as offering such adequate level of protection. To nevertheless support the vast amount of transatlantic data transfers, the European Commission has issued decisions on the Safe Harbour and subsequent Privacy Shield framework, which allow US companies to self-certify and as such to offer an adequate level of data protection under EU law. All in vain, the Safe Harbour Decision was invalidated by the ECJ in 2015[4], the Privacy Shield Decision this summer through Schrems II.

Under the GDPR, transfers of personal data to non-adequate countries are also allowed when the EU 'data exporter' and non-EU 'data importer' conclude Standard Contractual Clauses (SCCs).[5] These SCCs are drafted by the European Commission to contractually bind the data importer as recipient to provide for an adequate level of protection for the personal data it receives. In Schrems II the validity of these SCCs was confirmed. The ECJ did however add that the parties to the SCCs should not only take into account their contractual obligations under the SCCs. Parties should also be accountable for the assessment of the adequacy of the level of data protection in the country of the recipient, e.g. in light of access by governmental authorities to the transferred personal data and the relevant aspects of the legal system. This article gives a short description of that governmental access in the US[6] and some history and relevant aspects of US privacy law.[7,8]

---

[1] Judgement of 16 July 2020, *Schrems II*, Case C-311/18.
[2] Commission Decision 2016/1250/EU of 12 July 2016 pursuant to Directive 95/46 on the adequacy of the protection provided by the EU-US Privacy Shield, OJ 2016 L 207.
[3] See article 45 GDPR, full list of adequate countries to be found here.
[4] Judgement of 6 October 2015, *Schrems I*, Case C-362/14.
[5] E.g. Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council, OJ 2010 L 39.
[6] This article does not discuss surveillance practices of other countries, EU or non-EU. However, please follow the Judgments in Case C-623/17, *Privacy International*, and in Joined Cases C-511/18, *La Quadrature du Net and Others*, C-512/18, *French Data Network and Others*, and C-520/18, *Ordre des barreaux francophones et germanophone and Others*, where the ECJ confirmed that "that EU law precludes national legislation requiring a provider of electronic communications services to carry out the general and indiscriminate transmission or retention of traffic data and location data for the purpose of combating crime in general or of safeguarding national security".
[7] This article talks about privacy law, with the word 'privacy' commonly used in the US, as opposed to 'data protection' law as the word used mostly in the EU. The evolution of word 'privacy' into 'data protection' took place in the EU following the realization that protecting mere privacy did not prevent the mass collection and use of data by companies. This article will not go into the difference in that terminology. Just remember, data protection leads to privacy, but the terms are not interchangeable: data protection can apply when the right to privacy has lapsed, e.g. when data is already disclosed, while it does not prevent privacy invading acts without data (e.g. someone peaking in the shower).
[8] As Schrems II relates to federal surveillance practices, this article focuses on US privacy law applying to federal surveillance. This article does not discuss US privacy law regulating behaviour of private parties, a lack of a fundamental US privacy right means these are different

After reading, you should have a flavour of what to think of when dealing with the additional requirements imposed by the ECJ on the parties to SCCs.

My personal take on this is that lawyers can not deal with the matter raised by the ECJ. It is difficult to imagine solutions without either revising a part of the US law system or changing the EU take on privacy. And that is not what we want. We therefore need politicians and industry leaders working outside the legal ecosystem to come up with a solution.

2. US law system

Some insight on the US law system is required in order to appreciate the privacy regulations around US surveillance practices. Under the US Constitution, the scope of US federal law is limited to delegated powers and implied or inherent powers. Federal statutes can in principle only relate to certain mostly interstate subjects like aviation, regulation of commerce, telecommunications and declaration of war (other national security matters fall within the executive power of the President). State law can cover all other subjects, but can never conflict with federal law. In practice, the fact that federal law includes powers to regulate commerce means it can regulate almost any subject matter with some form of interstate commercial impact. A third source of US law is common law (i.e. courts making law based on previous court cases, both on federal and state level). [9]

A conservative view on the US legal system argues that a (new) right, like the right to privacy, can only be established by an amendment to the Constitution or by statute. Legal liberalists say that a new right can also be established through common law. The conservative view is best illustrated by the dissident opinion of conservative Judge Black in *Griswold v. Connecticut* (1965)[10]: "I like my privacy as well as the next one, but I am nevertheless compelled to admit that government has the right to invade it unless prohibited by some specific constitutional provision." In any case, for the right to privacy to exist under US law it should be found in federal law, state law or, under the liberal view, common law.

3. Privacy protection against federal surveillance practices

a. The Fourth Amendment

The 1791 Bill of Rights to the US Constitution consists of ten amendments.[11] With the infringements of the British government still in the minds of the people, the Bill of Rights confirmed personal rights and freedoms of the American people and limited governmental power. The Fourth Amendment provides a basis for a right to privacy in relation to federal 'searches':

> *The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.*[12]

The fact that the 'privacy' right described in the Fourth Amendment not only relates to places but also to people was subject of much debate and only confirmed for the first time in 1967 in *Katz v.*

---

subjects. Beautifully kick-started in 1890 by Brandeis and Waller in their Harvard law review article on the '*Right to Privacy*', privacy regulations in the US for private parties are currently mostly sectoral, e.g. relating to health data processed by hospitals, financial data collected in scope of financial services, genetic testing kits or online childrens' data. Some states are expected to enact privacy laws similar to the EU General Data Protection Regulation and California was the first to do so beginning of this year.

[9] State and federal administrative agencies have a delegated power to regulate certain areas of law, like banking or social security, but can not operate without a basis of law in federal, state or common law.

[10] *Griswold v. United States*, 381 U.S. 479 (1968).

[11] United States Bill of Rights, 15 December 1791.

[12] United States Constitution, Amendment IV, passed by Congress in September 1789, ratified in December 1791.

United States[13,14], where the interception (through a wiretap) of a telephone call made by Mr. Katz from a public phone booth was considered a search. Mr. Katz had a 'reasonable expectation of privacy' when making the call, meaning that the search required a warrant under the Fourth Amendment.

b. Wiretapping

Wiretapping was eventually regulated in the Omnibus Crime Control and Safe Streets Act (1968)[15] which was enacted as a response to roaring crime rates, but also codified the *Katz* case. Until then, without Fourth Amendment protection, the only legal limitation for federal wiretapping was the fact that the evidence obtained could not be used in court.[16] Federal wiretapping before 1968 had been soaring, most prominently in scope of the Cold War era. The Wiretap Act, as part of the Omnibus Crime Control and Safe Streets Act was also called, criminalized private tapping and required federal agents to obtain a warrant through a federal judge before tapping.

Tapping for national security purposes remained unrestricted and was left to the President's executive powers.[17] In the 1972 case *United States v. U.S. District Court*, or *Keith* case, the Supreme Court ruled that domestic security issues were not left to the executive powers of the President, thereby deciding against such claim of the Nixon administration.[18]

In the same week as the *Keith* judgement, five people were arrested for a break-in at the Watergate office complex in Washington, D.C. The subsequent Watergate hearings brought to light a widespread practice of warrantless tapping of phones and other undercover investigations of political opponents by the Nixon administration.[19] This 'violation of constitutional rights' of US citizens eventually lead to impeachment proceedings and the subsequent resignation of president Nixon in August 1974.[20] It also initiated a step towards federal privacy legislation.

c. Federal privacy legislation following Watergate

The Privacy Act of 1974

The public uproar following Watergate, combined with the increasing governmental data processing activities possible through the development of computers[21], led to the federal Privacy Act of 1974. This Privacy Act imposed principle based rules on federal agencies collecting and using personal data, including on access and correction, purpose limitation and security. Since 1974, federal agencies are required to record their personal data recording systems in the Federal Register.[22] Given the multiple exemptions applying to law enforcement, the vague 'routine use' exemption and the absence of a Privacy Commission responsible for enforcement of the Privacy Act, the Privacy Act did not provide

[13] *Katz v. United States*, 389 U.S. 347 (1967).
[14] An example were it was ruled differently is Supreme Court case *Olmstead v. United States*, 277 U.S. 438 (1928). No violation of the Fourth Amendment was found as only 'material things' and not the 'spoken word' were considered protected. With Judge Brandeis (still in practice!) dissenting that, through the Bill of Rights, the founders had "conferred against the government, the right to be let alone – the most comprehensive of rights and the right most favored by civilized men".
[15] Omnibus Crime Control and Safe Street Act of 1968, 34 U.S.C. § 10101.
[16] Federal Communication Act of 1934, 47 U.S.C. § 605; *Nardone v. United States*, 302 U.S. 379 (1937).
[17] 18 U.S.C. § 2511(3) (1968) ("Nothing contained in this chapter […] shall limit the Constitutional power of the President to take such measures as he deems necessary to protect the Nation against actual or potential attack or other hostile acts of a foreign power, to obtain foreign intelligence information deemed essential to the security of the United States, or to protect national security information against foreign intelligence activities […]").
[18] *United States v. U.S. District Court*, 407 U.S. 297 (1972).
[19] E.g. see Frederick S. Lane, *American Privacy: The 400-Year History of Our Most Contested Right* (Beacon Press, 2009), 184-189.
[20] US Federal Government, Legislative Branch, Articles of Impeachment adopted by the House Judiciary Committee on July 27, 1974.
[21] U.S. Department of Health, Education and Welfare, *Secretary's Advisory Committee on Automated Personal Data Systems, Records, computers, and the Rights of Citizens*, 1973.
[22] Recording, per agency, each new system of records in the Federal Register (www.federalregister.gov, the official journal of the US federal government). Each record based on the Privacy Act 1974 are a few pages long, and include detailed information about the categories of data, the routine use and policies for e.g. retrieval and retention.

the framework of checks and balances hoped for by many after the shock waves of the Watergate scandal.[23]

FISA and Executive Order 12333

Another set of legislation aimed at limiting governmental use of personal data followed in 1978 with the Foreign Intelligence Surveillance Act of 1978 (FISA)[24], which regulated the limitations to foreign surveillance practices which might involve US Persons.[25] Where foreign intelligence gathering was the significant purpose[26] of a surveillance, but the likelihood of a US Person being part of that surveillance was more than substantial, a special enacted United States Foreign Intelligence Surveillance Court (FISC) needed to grant a warrant through classified proceedings. The warrant compelled telecommunications companies to cooperate and usually prevented them to go public with this through a so-called gag order. Intelligence agencies could obtain a FISA warrant on the probable cause that the subject was a foreign power. Procedural requirements of a warrant included standards for targeting[27] and data minimization[28].

FISA did (and still does) not apply to surveillance practices which are entirely foreign, e.g. because they fully occur abroad without involvement of US Persons. Considered pure foreign affairs matters, these remain to fall under the executive power of the President, requiring no warrant or other form of judicial oversight.[29] Under President Reagan's Executive Order 12333 of 1981 (E.O. 12333)[30], procedures were set up for this form of foreign intelligence surveillance conducted by various intelligence agencies (themselves, without compelling third parties to cooperate). In relation to US Persons, E.O. 12333 afforded a number of privacy safeguards to US Persons including on data minimization and retention limitation.[31]

4. USA PATRIOT ACT

Part of the protections provided by FISA were withdrawn by the USA PATRIOT Act (Patriot Act), which was drafted within a matter of weeks after the terrorist attacks of 9 September 2001 and signed into law by President Bush on 26 October 2001.[32] The Patriot Act is not an independent act, but amends numerous acts, including FISA.

On Capitol Hill, the need was felt to broaden the domestic scope of FISA – traditional domestic surveillance regulations allowed for surveillance of US Persons for criminal investigations, but not for terrorism investigations.[33] Through the Patriot Act, surveillance of US Persons was no longer limited to 'ordinary' criminal activity. A much debated §501 FISA (based on §215 Patriot Act) was included, allowing for a FISC warrant for intelligence agencies to compel telecommunication companies to

[23] E.g. see James Beverage, *The Privacy Act of 1974: An Overview*, 1976 DUKE L.J. 301, 314 (1976) "*enforcement is at the moment largely a function of agency goodwill and good faith, congressional oversight, and individual action in pursuit of the rights granted to citizens by the Act*".
[24] 50 U.S.C. § 1801-1885c (1978).
[25] See note 43 for the definition of US Persons.
[26] Interpreted as *primary* purpose before the Patriot Act.
[27] 50 U.S. Code § 1881a (Procedures for targeting certain persons outside the United States other than United States persons).
[28] 50 U.S. Code § 1801h, not applying to non-US Persons.
[29] E.g. see *United States v. Truong Dinh Hung*, 629 F.2d 908 (4th Cir. 1980).
[30] Exec. Order No. 12,333, 3 C.F.R. 200 (1981).
[31] Exec. Order No. 12,333 (Part 2, Conduct of Intelligence Activities, 2.3 Collection of Information).
[32] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Washington, D.C.: U.S. Dept. of Justice.
[33] As explained by then Senator Joe Biden during the floor debate on the Patriot Act, "the FBI could get a wiretap to investigate the mafia, but they could not get one to investigate terrorists. To put it bluntly, that was crazy! What's good for the mob should be good for terrorists." (Cong. Rec., 10/25/01).

disclose to them 'all tangible things' necessary 'to protect against international terrorism or clandestine intelligence activities'.[34]

The Patriot Act was a temporarily measure, expiring at sunset on 31 December 2005. Through prolongations and the current USA Freedom Act of 2015 many provisions of the Patriot Act remain intact.[35]

5. First NSA revelations

In December 2005, the New York Times revealed an – until that time unknown – Terrorist Surveillance Program (TSP) of the National Security Agency (NSA).[36] TSP involved warrantless bulk telephone metadata collection involving US Persons and was secretly approved by the Bush Administration shortly after 9/11. Discussions as to the legality of TSP eventually led to extensive amendment of FISA through the FISA Amendment Act (FAA) of 2008.[37] Although the FAA was aimed at confirming privacy rights of US Persons in scope of foreign surveillance, it raised controversy due to the immunity granted to the telecommunication companies that had cooperated and would cooperate with FISA requests.

FAA expended FISA with sections 703 and 704, regulating surveillance *abroad* where the target is a US Person (if that person is an agent of foreign power, or an officer or employee of a foreign power). Previously falling under E.O. 12333, these surveillance practices now required an individualized warrant from FISC and were thus covered by the (privacy) requirements of FISA. The newly enacted FISA §702 compelled US based telecommunication facilities to disclose electronic information of non-US Persons reasonably believed to be outside the US for foreign intelligence purposes. As such, FISA §702 codified part of the NSA's TSP surveillance practice. The FISC warrant obtained for this purpose could last up to a year and contained another gag order.[38] Should personal information of US Persons be collected, FISA §702 provided that such data should be deleted unless relevant to a foreign intelligence purpose.

6. NSA revelations through Snowden

Through the Snowden revelations of the summer of 2013, more of NSA's surveillance practices became public.[39] The Snowden papers revealed that the NSA used FISA §702 for its bulk downstream (formerly PRISM) and upstream communications collection. Domestic uproar was caused by the fact that the bulk data collections included vast amounts of data of US Persons. Through so-called 'three hop' targeting the NSA looked at targets and their friends, their friends and their friends. It was calculated that this could potentially lead to more than a million people around a single target. The Snowden revelations did not only cause domestic protests – considerable international uproar and diplomatic tensions were raised through the disclosure of US mass surveillance on foreigners abroad.

7. International foreign surveillance and privacy

a. US Persons vs Non-US Persons

Insight on the difference between the protection of US Persons vs non-US Persons is required to understand the international implications of the US federal surveillance practices.

---

[34] 50 U.S.C. §1861 (2001).
[35] USA Freedom Act of 2015, Washington, D.C.: U.S. Dept. of Justice. The Freedom Act limited the use of gag orders and prevented the bulk surveillance collections previously performed by e.g. the NSA as made public through Snowden.
[36] New York Times, *Bush Lets U.S. Spy on Callers Without Courts*, 16 December 2005.
[37] 50 U.S.C. §1801 et seq.
[38] Partly de-classified under the Obama Administration, see here.
[39] E.g. see The Guardian here.

Before FISA, foreign intelligence surveillance was unregulated, and considered in numerous court cases as not requiring a warrant under the Fourth Amendment as it did not surveil on 'ordinary crime' which could lead to a conviction in court.[40,41] FISA (as well as E.O. 12333) confirmed that practice for non-US Persons.[42,43] Clearly, the purpose of FISA was to protect the rights of US Persons in relation to foreign surveillance, not to protect 'foreigners' as such.

As (somewhat inaccurately) suggested in the Schrems II judgement, non-US Persons including EU citizens do not miss protection under the Fourth Amendment per se (since the Fourth Amendment refers to 'persons').[44] However, surveillance of non-US Persons is usually done in scope of pure foreign national security matters, which mainly fall under the President's executive power[45] and are not governed by the Fourth Amendment. As is clear from the US law system, a legal right requires a basis in constitution, statute or common law. Thus far, such right to privacy for non-US Persons does not exist.

b. Response through Presidential Policy Directive 28

Nevertheless, following the international pressure after the Snowden revelations, the Obama administration acknowledged the interest of non-US Persons in protection of their privacy and took a step at regulating such protection through Presidential Policy Directive 28 (PPD-28).[46] PPD-28 establishes protections to be afforded to non-US persons in the context of US foreign intelligence.[47] In this scope, PPD-28 introduces the principles of minimization, data security and access, data quality and oversight "to be applied equally to the personal information of all persons, regardless of nationality", all "to the maximum extent feasible consistent with the national security".[48] While US intelligence agencies have altered their surveillance policies and procedures to reflect the PPD-28 principles, it is felt that PPD-28 has not altered foreign surveillance practices to the effect that US Persons and Non-US Persons are treated equally.[49]

8. Schrems II in light of all that…

The nature of the US surveillance practices and relevant regulations were known to the European Commission during its political pressure-cooker Privacy Shield Decision of 2016, as it was made after the Snowden revelations and the subsequent mostly administrative/diplomatic privacy safeguards for non-US Persons through PPD-28. In the Decision, the European Commission acknowledged the limitations to the privacy protection of non-US Persons.[50]

---

[40] *Clapper v. Amnesty International USA,* 133 S. Ct. 1138 (2013), a minor 5-4 decision.
[41] The question whether the Fourth Amendment protection applied to national security (involving non-US Persons) was deliberately not part of the abovementioned Katz and Keith cases. In the Katz case, a footnote simply mentioned that 'Whether safeguards other than prior authorization by a magistrate would satisfy the Fourth Amendment in a situation involving the national security is a question not presented by this case. In the Keith case, it was confirmed that it 'involves only the domestic aspects of national security. We have not addressed and express no opinion as to, the issues which may be involved with respect to activities of foreign powers or their agents'.
[42] This article does not discuss the question if this US practice violates the International Covenant on Civil and Political Rights on the right to privacy.
[43] A US Person is a defined term in FISA and Exec. Order 12,333, meaning 'a citizen of the United States or a permanent resident alien lawfully admitted into the United States'.
[44] Under the US constitution, only the right to vote and the right to participate in federal elections are limited to U.S. citizens.
[45] *United States v Duggan*, 743 F.2d 59 (2d Cir. 1984).
[46] https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities
[47] Acknowledging PPD-28, §4 that "our signals intelligence activities must take into account that all persons should be treated with dignity and respect, regardless of their nationality or wherever they might reside, and that all persons have legitimate privacy interests in the handling of their personal information".
[48] PPD-28, §4
[49] See for instance, Daniel Severson, "American Surveillance of Non-U.S. Persons: Why New Privacy Protections Offer Only Cosmetic Change", *Harvard International Law Review*, Volume 56, Number 2, Summer 2015.
[50] Privacy Shield Decision, in relation to individual redress in the US, recital 115: "… 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

These limitations are now a fundamental part of the invalidation of the Privacy Shield Decision through Schrems II. Although the reasoning of Schrems II is broadly opposed in the US Department of Commerce White Paper responding to Schrems II[51], the invalidation of the Privacy Shield Decision by the ECJ seems inevitable in light of what is written in this article.

Conclusion 1 – The nature of the US law system, the limitations of the Fourth Amendment and the extent of the Presidential powers limit regulatory privacy protection of US and non-US Persons in scope of foreign surveillance. For US companies governed by the US law system, more is required than a principles based self-certification mechanism like the Privacy Shield to allow them to provide privacy protection for EU personal data deemed adequate under EU standards.

Conclusion 2 – As for the SCCs alternative, the judgement of the ECJ that parties should take into account governmental access and the local legal system seems as natural as it is unpractical, at least for the US as is shown in this article. It seems to me that what the European Commission could not get right in its Privacy Shield Decision, will be difficult to get right for private parties.

The supplementary measures announced by the European Data Protection Board are therefore eagerly anticipated. [52] Quite a task - matters such as the lack of judicial oversight for surveillance under E.O. 12333 and the lack of a more fundamental right of privacy to step in were the protection of the Fourth Amendment stops, seem to indicate that you should either change part of the US law system or the EU privacy standards to solve the issue raised by the ECJ. I can therefore only imagine a solution outside the legal system, through change in policy or industry practice.

Within the legal system, a US federal law creating a fundamental right to privacy for all individuals dealing with the government would be a proper solution. The history of US federal privacy legislation shows that it responds to public uproar. Who knows, maybe this time the tone can come from the top? Presidential candidate Joe Biden did indicate that the US "should be setting standards not unlike the Europeans are doing relative to privacy".[53] Looking forward to that promise!

Annemarie Bloemen, 2 November 2020

for non-U.S. persons, such as for surveillance under FISA, the available causes 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".

[51] U.S. Department of Commerce White Paper, James M. Sullivan, Deputy Assistant Secretary for Services, *Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers after Schrems II*, September 2020.

[52] The European Data Protection Board created a taskforce following Schrems II. This taskforce will prepare recommendations to assist controllers and processors with their duty to identify and implement appropriate supplementary measures to ensure adequate protection when transferring data to third countries.

[53] Interview conducted Dec. 16, 2019 by the New York times, and published Jan. 17, 2020, here.