From Snowden to Schrems: How the Surveillance Debate has Impacted US-EU Relations and the Future of International Data Protection

by Alan Butler & Fanny Hidvegi

In the Spring of 2013, a group of international journalists, human rights activists, and civil liberties groups suffered a major defeat in the US Supreme Court: the Supreme Court held that the groups could not challenge the law permitting the collection of international communications because they could not show that their communications would be specifically targeted and collected under the law.[1] Little did the Court and the parties know, within a few months, the scope of the National Security Agency surveillance activities would be exposed in a series of news stories based on documents obtained by Edward Snowden.[2] What followed was a period of unprecedented global scrutiny over government surveillance activities—in particular, scrutiny of US surveillance programs targeting Europeans. The surveillance debate fundamentally altered the diplomatic landscape, influencing negotiations over the new data protection regulation. These changes recently culminated in a decision by the Court of Justice for the European Union (the "*Schrems Decision*") finding that the "Safe Harbor" framework, relied upon by many of the companies transferring personal data between the US and the EU, did not provide adequate protection for Europeans' data.[3]

The *Schrems* decision, which discussed at length US surveillance programs revealed by Snowden, has further shifted the dynamic of US-EU data protection relations. Trans-border data flows have become ubiquitous as many companies seek a global user base. But, as a result of the *Schrems* decision, the United States and other countries will be forced to incorporate EU data protection principles into cybersecurity, encryption, surveillance, and other privacy regimes (or risk exclusion of US companies from international technology markets). The US has already taken steps to reform domestic surveillance laws following the Snowden disclosures, but so far Congress has not established remedies for Europeans or other foreigners subject to surveillance.[4]

Alan Butler *is Senior Counsel at the Electronic Privacy Information Center (EPIC) in Washington, D.C. He received his J.D. from the UCLA School of Law.*
Fanny Hidvegi *is the International Privacy Fellow at the Electronic Privacy Information Center (EPIC) in Washington, D.C. She received her J.D. from Eötvös Loránd University.*

The *Schrems* decision has shifted incentives for US government officials and for companies to find both diplomatic and legislative solutions to the data protection problem. European companies may also face challenges as France, the United Kingdom, and other countries seek to expand surveillance powers and limit access to encryption and other data protection tools in response to recent attacks. The potent combination of surveillance disclosures, reform proposals, and recent European court decisions has shifted the balance in the diplomatic negotiations over data protection regulations.

A BRIEF HISTORY OF RECENT NSA SURVEILLANCE REVELATIONS

The recent debates over the scope of surveillance by the US National Security Agency and its foreign partners have focused on three types of surveillance: (1) the bulk collection of metadata records from communications providers in the United States, (2) the monitoring of communications in the United States that are reasonably believed to originate abroad, and (3) the collection of data or surveillance of communications not subject to the Foreign Intelligence Surveillance Act rules.

Bulk Metadata Collection

The first NSA surveillance story published by *The Guardian* in June 2013 concerned the bulk collection of telephone call detail records (metadata).[5] The story revealed an order by the US Foreign Intelligence Surveillance Court (FISA Court), issued to Verizon Business Network Services (Verizon) pursuant to the "business records" provision of the USA PATRIOT Act (Patriot Act).[6] Specifically, Verizon was ordered by the FISC to produce to the NSA on an "ongoing daily basis" all "call detail records" for "communications (i) between the United States and abroad; or (ii) wholly within the United States, including local telephone calls."[7] These call detail records or "telephony metadata" included "comprehensive communications routing information" but not the "substantive content of any communication."[8] This metadata collection program had been in place since the fall of 2001 and operated under FISA Court orders since 2006.[9] During that period, the NSA obtained all telephone metadata from the three major US service providers.[10] NSA collected, analyzed, and retained that metadata for five years.[11]

Once collected, the NSA used "sophisticated analysis of the massive volume of metadata" to identify "the network of contacts linked to targeted numbers or addresses."[12] The agency was also, as of 2011, collecting e-mail and other Internet metadata in bulk and using the same "contact chaining" methods to identify connections between users.[13] The NSA metadata program was authorized by the FISA Court subject to certain "minimization procedures."[14]

Following the disclosure of the NSA metadata program a number of organizations filed suit alleging that the bulk collection of metadata was illegal and unconstitutional.[15] Shortly after these suits were filed, the FISA Court issued its first written opinion explaining the legal basis for the program.[16] Specifically, Judge Eagan held that the Fourth Amendment did not impose "an impediment to the government's proposed collection" of telephone metadata and that "the entire mass of collected metadata is relevant to investigating [international terrorist groups]" because bulk collection is "necessary to identify the much smaller number of [international terrorist] communications."[17] A federal appellate court later ruled that all telephone metadata could not be "relevant" under the statute and that the program had been operating unlawfully.[18] A federal district court also found that the program likely violated the Fourth Amendment.[19]

The NSA metadata program was also reviewed by congressional committees, a presidentially-appointed expert review group, and an independent oversight agency. All of these independent reviews reached the same conclusion: the program did not contribute significantly to any terrorism investigations. Not only was the program overly broad and invasive, it was not necessary or especially important. Congressional leaders "not convinced" by the administration's early attempts to show that the program was effective.[20] The Privacy and Civil Liberties Oversight Board also concluded, after a lengthy investigation, that the program did not impact the outcomes of any counterterrorism investigations.[21] The President's Review Group on Intelligence and Communications Technologies reached a similar conclusion.[22]

PRISM Program and Upstream

The same day that the NSA metadata program was revealed, another significant surveillance program code-named "PRISM" was also made public.[23] This program involved, according to documents published by the Washington Post, the collection of communications "directly from

the servers" of US Internet service providers including "Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube, Apple."[24] This story caused widespread controversy both domestically and internationally, and drew criticism from privacy advocates and technology companies alike. But the program was being operated under the same statutory scheme that previously been the subject of criticisms from privacy groups,[25] and an unsuccessful legal challenge in the US Supreme Court,[26] referred to as "Section 702" or the "FISA Amendments Act."

The PRISM program was first developed as part of the secret President's Surveillance Program (which came to be known as the Terrorist Surveillance Program) in 2001.[27] The theory behind the original program was that certain international communications, which were being routed through servers in the United States, could be obtained without a warrant as long as the "target" of the surveillance was not a United States person.[28] The program was not subject to any judicial oversight until after the New York Times revealed it to the public in December of 2005.[29] Following a brief transition period where the program operated under normal FISA rules, the Government proposed and Congress enacted a statutory framework that authorized the Intelligence Community to target and acquire certain communications without specific court approval.

"The program was not subject to any judicial oversight until after the New York Times revealed it to the public."

Even more controversial than the "PRISM" collection program was the NSA's collection of Internet communications directly from the Internet backbone referred to as "Upstream" collection.[30] The Upstream program operates by filtering communications as they transit the core telecommunications lines in the United States.[31] The NSA first requests that the telecom companies provide access to certain portions of "Internet traffic it believes most likely to contain foreign intelligence."[32] Then the NSA uses "selectors" to decide which messages to keep.[33] This system "is designed to look for communications that either originate or end abroad" but also sweeps in "purely domestic" communications because of its broad scope.[34]

Under the Section 702 authority, the Attorney General and Director of National Intelligence jointly authorize surveillance to engage in "targeting of persons reasonably believed to be located outside of the United States to acquire foreign intelligence information."[35] Once authorized, this surveillance is not limited to a particular location or facility, and the government does not

have to seek a separate court order or otherwise justify each target. There are a few limitations imposed by Section 702: (1) the surveillance must comply with certain "targeting procedures,"[36] (2) the government must apply with "minimization procedures,"[37] (3) government officials must "certify" that the procedures are being followed and that a "significant purpose" of the surveillance is to obtain foreign intelligence information,[38] and (4) more restrictive measures apply when targeting a US person.

Following the 2013 revelations, a group of Senators requested that the Privacy and Civil Liberties Oversight Board, an independent agency tasked with overseeing national security programs, investigate the PRISM and Upstream programs and provide an unclassified report.[39] The board issued its report in the summer of 2014, finding that the program raised concerns related to the "incidental collection" of US persons' communications.[40]

The Section 702 authority was also the subject of litigation and controversy before the PRISM and Upstream programs were revealed in July 2013. In fact, a group of litigants filed suit challenging the constitutionality of Section 702 on the day it was enacted.[41] The suit was ultimately defeated in early 2013 when the US Supreme Court held that the individuals could not challenge the law because they had not shown that their communications would be collected pursuant to Section 702.[42] Another suit was brought by the Wikimedia foundation challenging the Upstream collection program.[43]

Executive Order 12333

Another series of new stories published since the summer of 2013 included revelations of surveillance programs conducted by the NSA and other intelligence services outside of the United States.[44] Some of the programs revealed are not conducted pursuant to the Foreign Intelligence Surveillance Act, but are instead authorized and defined by rules adopted under Executive Order 12333 (and its progeny), a presidential order that governs activities of the Intelligence Community.[45] Certain surveillance activities conducted under 12333 will be the subject of another report by the Privacy and Civil Liberties Oversight Board.[46]

REFORM ON TWO FRONTS: DOMESTIC & INTERNATIONAL

There have been concurrent efforts both in the United States and in Europe over the last few years to reform surveillance authorities and other

privacy laws. These efforts have been motivated, in part, by the surveillance revelations of summer 2013 and the subsequent backlash against the NSA and other intelligence services, as well as the companies involved.

Domestic Surveillance Reforms in the U.S.

The domestic surveillance reform efforts in the United States proceeded on two fronts: in the executive and legislative branches. Congress began by holding a series of hearings following the revelations in 2013, and proceeded to consider many intersecting and overlapping reform proposals. Ultimately, this effort resulted in the passage of the USA FREEDOM Act in June 2015.[47] During the same period, the President announced a plan to impose new restrictions on the Intelligence Community's collection programs.[48]

USA FREEDOM Act

Congress began to develop NSA reform bills soon after the revelations in the summer of 2013.[49] Many different proposals were made, but the majority of reform efforts were focused on three issues: (1) ending bulk collection of Americans' telephony metadata under Section 215 of the Patriot Act; (2) increasing transparency of surveillance activities through public reports and audits; and (3) improving oversight and transparency of the Foreign Intelligence Surveillance Court process.[50]

By 2014, the USA FREEDOM Act had been introduced by a bipartisan coalition of legislators, including leaders in both the House and Senate Judiciary Committees, and was seen as the best option for NSA reform in Congress.[51] However, Congress was unable to reach consensus on the Freedom Act before the end of the 2014 session.[52] But in 2015 Congress successfully passed the bill and the President signed it into law, despite efforts by leading lawmakers to block reform.[53]

The Freedom Act included a number of significant changes to surveillance programs and oversight mechanisms, but the central component of the law is a reformulation of Section 215.[54] The law bans bulk collection under Section 215,[55] instead requiring that the government base an application for "call detail records" on a "specific selection term."[56] In order to obtain a CDR order, the government must submit the application to the FISC and show that (1) it has "reasonable grounds" to show that the CDRs related to that specific selection term are "relevant" to an investigation,

and (2) it has a "reasonable articulable suspicion" that the selection term is "associated with a foreign power engaged in international terrorism."[57] If the FISC grants the application, then the government can order a company to provide CDRs within "two hops" of the specific selection term.[58]

In addition to the changes to Section 215 and the prohibition on bulk collection, the Freedom Act also includes provisions imposing new disclosure requirements for significant FISC opinions and orders, creating a panel of amici curiae to provide the FISC with assistance on legal and technical matters, and addressing some concerns about the targeting of United States persons under Section 702.[59] The law addressed some, but not all, of the concerns related to bulk collection by the NSA following the 2013 surveillance revelations.

PPD-28

The President spoke on January 17, 2014, to address the government's use of electronic surveillance and the privacy impact of its signals intelligence programs.[60] In the speech, President Obama introduced a new policy directive, PPD-28, requiring members of the Intelligence Community to develop and implement new privacy protections for their surveillance programs.[61] The PPD is binding upon executive branch agencies but it does not create a right of action enforceable in court.[62]

The focus of PPD-28 was to direct reforms that ensure signals intelligence programs are designed to "take into account that all person should be treated with dignity and respect, regardless of their nationality or wherever they may reside, and that all persons have legitimate privacy interests in the handling of their personal information."[63]

The Directive includes six sections, the last two concerning reports and jurisdictional effects and the first four outlining policy guidance, limitations, and rules for signals intelligence.[64] The first section requires that all signals intelligence collection be "conducted consistent with" four principles: (1) executive branch authorization (2) purpose limitation and consideration of privacy and civil liberties impact, (3) prohibition on collecting foreign private commercial information for competitive advantage, and (4) narrow tailoring of collection activities.[65] The second section imposes limitations on the use of signals intelligence collected in bulk, namely that such information may only be used for six listed purposes: espionage, terrorism, weapons of mass destruction, cybersecurity, threats to armed forces, and transnational crime.[66] The third section requires an annual review of signals intelligence

policies and procedures by all Intelligence Community leaders in light of the PPD-28 principles.[67] And finally the fourth section requires that all Intelligence Community agencies develop and adopt safeguards to protect the personal information of any person (regardless of nationality) collected through the signals intelligence programs.[68]

The first annual reports on progress with the PPD-28 directives were released in February of 2015.[69] The report outlined, in particular, new procedures adopted by the NSA, the FBI, and the CIA.[70] The procedures largely mirrored the rules established in PPD-28, but also establish rules for retaining personal information collected and limiting dissemination of that information absent consent.[71] In general, the CIA's procedures are less restrictive than the NSA's.[72] The FBI procedures also state that the agency will apply the rules outlined in PPD-28 to the collection programs authorized by Section 702.

"[PPD-28] requires that all Intelligence Community agencies develop and adopt safeguards to protect personal information."

Judicial Redress Act

Congress has now begun to consider proposals that would provide access to US courts for certain foreign individuals who have been subject to government surveillance. The Judicial Redress Act of 2015, currently pending before Congress, aims to amend the Privacy Act to extend certain privacy safeguards to non-US persons.

The significance of the Judicial Redress Act in the US-EU relations is that the passing of the bill is a precondition for the adoption of the so-called "EU-US data protection Umbrella Agreement."[73] The Agreement covers the cooperation and data transfers between American and European law enforcement agencies.

The need to extend privacy safeguards to non-US persons arises from the concern that personal information transferred from the European Union to the United States lacks adequate privacy protection. That is because the Privacy Act, as adopted in 1974, defined an "individual" entitled to protection under the Act as "a citizen of the United States or an alien lawfully admitted for permanent residence.[74] The definition reflected the reality of the time, which was that there was little information about non-US persons maintained by US federal agencies.

Most US privacy laws that were enacted subsequent to the Privacy Act of 1974 do not maintain this distinction.[75] Moreover, US federal agencies

have routinely made extensive demands on European companies and European government agencies for the personal information of European citizens. The request that the US Privacy Act be updated to reflect the fact that personal data on E.U. citizens is now routinely stored by US federal agencies followed directly from the practices initiated by US agencies.[76] According to the Electronic Privacy Information Center's analysis of the Judicial Redress Act, it does not provide for adequate safeguards.[77]

Both the EU and the US are using the Judicial Redress Act as a talking point to prove that the US has made significant improvements to provide judicial redress for non-US persons. This is perfectly reasonable and understandable from the American perspective. Independent academic experts, human rights and consumer groups in the US however, warned European officials about the flaws of the bill.

The House has already voted and passed the bill, now it is pending before the Senate. It is not clear at this point if European negotiators intent to request amendments to the Senate version of the bill.

DATA PROTECTION CHALLENGES IN THE EU

Schrems case

One of the most impactful developments in EU-US relations recently has been the Schrems case and the invalidation of Safe Harbor.

The Safe Harbor Framework is an industry-developed self-regulatory approach to privacy protection.[78] Coordinated by the Department of Commerce, the Safe Harbor program allows US companies to self-certify privacy policies in lieu of complying with legal requirements for the processing of data of Europeans. The Safe Harbor arrangement was developed in response to the European Union Data Directive, a comprehensive legal framework that established essential privacy safeguards for consumers across the European Union.[79] The Federal Trade

Commission has been tasked with overseeing Safe Harbor compliance, but only "sanctions" companies by proscribing them from future misrepresentations when they make false representations.

Max Schrems, an Austrian citizen, has been a Facebook user since 2008. As is the case with other subscribers residing in the EU, some or all of the data provided by Mr. Schrems to Facebook is transferred from Facebook's Irish subsidiary to servers located in the United States, where it is kept. Mr. Schrems lodged a complaint with the Irish Data Protection Commissioner, taking the view that, in the light of the revelations made in 2013 by Edward Snowden concerning the activities of the United States intelligence services (in particular the National Security Agency), the law and practices of the United States offer no real protection against surveillance by the United States of the data transferred to that country. The Irish authority rejected the complaint, on the ground that in a decision of 26 July 2000 the Commission considered that, under the "safe harbor" scheme, the United States ensures an adequate level of protection of the personal data transferred.

"The law and practices of the United States offer no real protection against surveillance by the United States."

Following Advocate General Bot's opinion, the CJEU struck down Safe Harbor because EU personal data transferred to the United States does not receive the same legal protection in the United States as it does in Europe. Specifically, according to the European standard, the level of protection should be "adequate"[80] and "essentially equivalent."[81]

As a consequence of the ruling, the European Union and the United States are facing an uncomfortable dilemma both domestically and internationally. Both jurisdictions should update their respective privacy laws to provide adequate privacy safeguards for people regardless of nationality. On top of that the two parties have legal and practical hurdles with international relations. On the one hand, the biggest challenge for the EU is to tackle the issue that national security is in theory a member state competence. And on the other hand, the US should introduce significant changes in its domestic laws and international commitments to ensure the continuation of data flows.

In the aftermath of the Schrems decision and the elimination of Safe Harbor, industry groups have advocated aggressively for new rules permitting trans-border data flows and emphasizing the potential economic consequences of delay. These pressures are likely to have a profound impact

on US-EU privacy negotiations going forward.

Other CJEU decisions of note: the right to be forgotten and data retention

The jurisprudence of the CJEU includes privacy related cases that are although less dominant in shaping international relations between the EU and the US, but they have also altered the European data protection and privacy landscape.

The two landmark privacy rulings of 2014 are the Google v Spain[82] case and the invalidation[83] of the Data Retention Directive.[84]

The Google versus Spain case has been the most misunderstood and widely debated European case in the United States.

The European Court of Justice ruled in *Google v. Spain* that European citizens have a right to request that commercial search firms, such as Google, that gather personal information for profit should remove links to private information when asked, provided the information is no longer relevant. The Court did not say newspapers should remove articles. The Court found that the fundamental right to privacy is greater than the economic interest of the commercial firm and, in some circumstances, the public interest in access to information. The European Court affirmed the judgment of the Spanish Data Protection Agency which upheld press freedoms and rejected a request to have the article concerning personal bankruptcy removed from the website of the press organization.

In the second case, involving a group called Digital Rights Ireland, the Court declared the Data Retention Directive invalid after, a long legal battle, on the ground that "it entails a wide-ranging and particularly serious interference with the fundamental rights to respect for private life and to the protection of personal data, without that interference being limited to what is strictly necessary."

The Court ruled that by adopting the Data Retention Directive, the EU legislature has exceeded the limits imposed by compliance with the principle of proportionality…although the retention of data required by the directive may be considered to be appropriate for attaining the objective pursued by it, the wide-ranging and particularly serious interference of the directive with the fundamental rights at issue is not sufficiently circumscribed to ensure that that interference is actually limited to what is strictly necessary.

It is not yet clear what impact the Digital Rights Ireland decision

will have on national data retention laws. Nevertheless, in many European member states, the respective Constitutional Courts have struck down domestic laws concerning data retention.[85] The European Union is also currently in the midst of the enacting broader privacy reforms in an update to the General Data Protection Regulation and a possible new data retention framework cannot be ruled out, having in mind the recent developments with the European refugee crisis and the Paris attacks.

LIBERTY AND OTHER CASES CHALLENGING NSA AND UK SURVEILLANCE

In Europe, besides the Court of Justice of the European Union, the key forum for privacy and human rights in general is the European Court of Human Rights (ECHR).

There are currently parallel cases before the ECHR arguing that the United Kingdom violated freedom of expression and the right to private life set out by Article 8 and 10 of the European Convention on Human Rights.[86]

The applicants complain that (1) the statutory regime in relation to the interception of external communications and metadata is incompatible with the Convention, and they allege (2) that they are very likely to have been the subjects of generic surveillance by Government Communications Headquarters and/or the United Kingdom security services.

The applicants of the most relevant cases are journalists and civil society organizations. The unlawful intercepting of the communications of such entities breaches more than just the fundamental right to respect for private life. It constitutes a violation of freedom of expression and might result in chilling effect. "The interception and exploitation of journalistic communications in this manner, in the absence of proper safeguards, may undermine the confidentiality of journalistic sources, materials and information, a necessary and basic precondition for press freedom in a democratic society."[87] As the Court acknowledged in TASZ v Hungary, non-governmental watchdog organizations have similar role in society to journalists.[88]

THE FUTURE OF INTERNATIONAL PRIVACY RELATIONS

The next phase of privacy regulation will depend on developments in international relations concerning commercial and law enforcement data transfers, as well as trade negotiations and other agreements concerning surveillance powers and the use of encryption. Europe and the United States are already engaged in a range of trade and diplomatic negotiations centered on privacy issues, and the NSA surveillance revelations will continue to be a key component of those negotiations. The dynamic has shifted as a result of the surveillance revelations and the recent decisions of the European courts, but other future events may shift the balance further in either direction.

US-EU REVISITING AGREEMENTS

Safe Harbor 2.0

The next steps in EU-US privacy relations will be centered around Safe Harbor, and the level of adequacy of the American legal system to provide privacy and data protection safeguards for US and non-US persons.

After the judgment, US and EU officials immediately resumed the previously-suspended negotiations over the "safe harbor" agreement.[89] But now the dynamic had changed. Any new revisions must be made in accordance with the requirements laid down by the CJEU in the Schrems decision. Regardless of criticisms coming from civil society, academia and industry leaders the parties are still committed to achieve a "Safe Harbor 2.0" by the end of January 2016.[90] This deadline has come from the Article 29 Working Party of the European Union, consisting of European data protection officials and the European Data Protection Supervisor. As a response to industry requests, the Working Party issued a position paper on data transfers under Safe Harbor and other alternative mechanisms to offer certainty to some degree[91] The Working Party concluded that "transfers that are still taking place under the Safe Harbour decision after the CJEU judgment are unlawful." Moreover, the opinion states that "if by the end of January 2016, no appropriate solution is found with the US authorities and depending on the assessment of the transfer tools by the Working Party, EU data protection authorities are committed to take all necessary and appropriate actions, which may include coordinated enforcement actions."

The European Union has no authority over national data protection

authorities in a sense that the EU could stop them from taking enforcement actions. Max Schrems decided not to wait for the outcome of the negotiations; instead, he took further legal actions to move the case forward.[92] Schrems filed complaints with data protection officials in Ireland, Belgium and Germany to block Facebook's data transfers to the US in order to "ensure that this very crucial judgment is also enforced in practice when it comes to the US companies that are involved in US mass surveillance."[93]

Umbrella Agreement

The US and EU are also in the midst of negotiating a so-called "Umbrella Agreement," a framework for transatlantic data transfers between US and EU law enforcement agencies. The proposed goal of the Agreement is to provide data protection safeguards for personal information transferred between the EU and the US. The negotiations over this agreement will provide yet another opportunity for US and EU counterparts to spar over the recent issues of surveillance revelations and new EU privacy restrictions.

On September 8, 2015 European and US officials announced that they have concluded an agreement on data protection for transatlantic criminal investigations.[94] The EU Justice Commissioner stated, "Once in force, this agreement will guarantee a high level of protection of all personal data when transferred between law enforcement authorities across the Atlantic."[95] Despite the announcements, neither US officials nor their European counterparts made the official text of the Agreement public. Instead, it was first made public by Statewatch.

After a Freedom of Information request, the European Commission made the document accessible but US officials still have not released it under similar Freedom of Information procedure.

According to an independent analysis of the Agreement, in its current form, do more harm than good for Europeans. It does not provide for adequate safeguards but violates the EU Charter of Fundamental Rights.[96] After the horrible Paris attacks, further law enforcement cooperation and intelligence sharing agreements are on the horizon.

As we mentioned earlier in Section 2.1.3, the finalization and signing of the agreement depends on adoption of the Judicial Redress Act 2015, which will be a part of the Schrems/Safe Harbor negotiation process.

Data Localization and the Microsoft Case

Another emerging international privacy issue is at the core of a case brought by Microsoft in US Court. In that case, Microsoft is challenging the government's attempt to access customer emails stored in the European Union, on a Hotmail server in Ireland. The case raises the controversial issue of data localization and national jurisdiction. It shows the significance of that case that a foreign government, Internet service providers, tech companies, media outlets, NGOs and academic scholars have felt the urgency to weigh in whether in the form of amicus briefs or op-eds or other publications.[97]

In December 2013, the US government served a search warrant on Microsoft seeking access to customer emails stored in Dublin, Ireland, where Microsoft maintains a data center. Microsoft opposes the government's demand on the grounds that the government cannot force American tech companies to turn over customer emails stored exclusively in overseas company data centers. Meanwhile, the government has argued that emails you store in the cloud cease to belong exclusively to you.[98]

According to Department of Justice, the US government has the right to demand the emails of anyone in the world from any email provider headquartered within US borders.

Data localization has been proposed as a partial solution to the parallel problems of government surveillance, data breaches, and differing levels of data protection across countries. Some groups strongly oppose data localization as possible threat to the future of the Internet, but others see it as an attractive solution to the privacy regulation problem.

Data localization in a summary is the concept of having IT businesses store their data in the country they operate in rather than on servers anywhere. Governments around the world have proposed bills and policies that attempt to create "national" internets. Lawmakers usually argue that such measures will ensure the data's safety and boost the economy due to the required expansion of local IT infrastructure.[99] On the other hand, data localization is associated with censorship, antidemocratic governments' increased control over their respective residents, forced jurisdiction and possibly harming innovation.

As to facilitating the data driven economy, the recently published text of the Trans-Pacific Partnership trade agreement takes the view to generally ban data localization with a narrow exception. It says that no TPP country "shall require a covered person to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory."

But of course the whole purpose of such trade agreement explains why TPP includes provisions that prohibit unreasonable limitations on the cross-border transfer, storage, and processing of data, which are intended to help establish a global framework for the free flow of information in the growing digital economy.[100]

It is fair to say that neither forced data localization nor the complete ban thereto is a proper solution to data flow related current and emerging challenges. According to our view, a high level, globally recognized and internationally enforceable privacy and data protection standard will be necessary to provide adequate fundamental rights protection.

EMERGING INTERNATIONAL PRIVACY ISSUES

Other emerging privacy issues underscore the impact of global connectivity and the consequences of trans-border data flows and openness. One issue that has emerged once again is the fight over encryption and government access to private communications. The other important and emerging issue is the concern over cybersecurity, data breaches, and the threat of identify theft. Yet ironically there is an inherent contradiction between the proposed policy solutions to these two problems: improving cybersecurity requires that we make data less accessible, while limiting the use of encryption requires that we make data more accessible.

First, it is almost every government's limitless wish to adopt new, intrusive and unjustified surveillance laws, possibly in fast track procedures without proper professional and social debate. The alleged reason behind this policy is the fear of terrorism. This fear serves as a basis for increased law enforcement and intelligence activities without presenting proves to the efficiency of these measures. In most cases, the level of intrusiveness and the lack of procedural guarantees constitute a violation of constitutions and human rights.

In the meantime, governments argue for building "backdoors" or "golden keys" into products for law enforcement and antiterrorism purposes which in fact results in security vulnerabilities that can be exploited by the same "terrorists we are afraid of."

In our view, both policies are mistaken and unlawfully curtail fundamental rights. On top of that, the above mentioned two policy goals are pursued by the same stakeholder groups even though these ideas absolutely contradict each other.

As we said, surveillance and anti-encryption efforts are not new to the public discourse, but this unfortunate trend has been strengthening since the refugee crisis and the Paris attacks both in Europe and in the United States.

More and more European countries introducing new surveillance laws, collection of biometrics and other measures allegedly aiming at securing public safety. Member states themselves fail to provide adequate privacy and data protection guarantees while the European Union is in the midst of the huge privacy related reform and the adoption of the General Data Protection Regulation.

There is a growing concern how the two policy directions will affect each other and which direction will prevail. Human rights organizations will have to follow closely during the upcoming months.

In the Zakharov case, the European Court of Human Rights has come out against blanket surveillance.[101] The most important finding of the ruling that the complainant is considered a victim of a violation of the European Convention on Human Rights without proving that he was subject to specific surveillance, since those were all secret. Based on "the fact that [the surveillance] affected all users of mobile telephone communications, the Court considered it justified to have examined the relevant legislation not from the point of view of a specific instance of surveillance of which Mr Zakharov had been the victim, but in the abstract."[102]

An additional layer to the issue is the reaction of governments to the use of social media by radical groups to organize and promote their message, and attempts by governments to control this use.

THE ROLE OF TRADE AGREEMENTS

From a human rights perspective, it is unfortunate that trade agreements will most likely determine the future of Internet governance, including online privacy. Therefore, globally binding standards would be necessary to ensure adequate safeguards for the right to private life and data protection.

adopted, is going to be as binding as any other trade agreement. Its enforceability is stronger than human rights conventions' thereof. Trade agreements affect countries beyond the ones that are currently involved in negotiations. Countries that are not signatory parties will likely be asked to accede to the given agreement as a condition of bilateral trade agreements

There is today a growing consensus on both sides of the Atlantic, supported by human rights advocates, consumer groups and business leaders, that privacy and data protection are fundamental human rights. Nevertheless, the enforcement of these rights is going to be endangered if provisions of unfolding trade agreements will prevail.

There are a few important and controversial trade agreements the US is currently negotiating. Among others, the Trans-Pacific Partnership (TTP), the Transatlantic Trade Investment Partnership (TTIP) and Trade in Services Agreement (TISA) have created debates between decision makers and also resulted in protests.[103]

Due to the territorial scope of this paper one would think that TPP is not relevant since current TPP countries are as follows: US, Japan, Australia, Peru, Malaysia, Vietnam, New Zealand, Chile, Singapore, Canada, Mexico and Brunei Darussalam. Nevertheless, signatories of trade agreements overlap and eventually impact each other.

Lack of transparency is a common deficiency of trade agreements. Often civil society and the general public are excluded from negotiations completely. In most cases, the texts of the agreements have only become public through unofficial sources or leaks. The process of including only governments and industry lobbyists undermines democratic values and lead to the lack of legitimacy.

The final text of TPP's E-Commerce Chapter, which includes provisions on trans-border data flows, has become public recently. The trade agreement applies an inverse logic between trade and privacy, absolutely contrary to how a fundamental right should be addressed.

TPP recognizes "the economic and social benefits of protecting the personal information of users of electronic commerce and the contribution that this makes to enhancing consumer confidence in electronic commerce."

We agree that protecting personal information does have economic and social benefits but this does not mean a country should guarantee the protection of privacy and personal data. Instead, it should be a legal obligation arising from the nature of privacy recognized as a fundamental right.

The countries signing TPP agree that they allow the cross-border transfer of personal information by electronic means. The only reason for a party to introduce limitations to data flows is to achieve a legitimate public policy objective. However, TPP also says that measures to protect personal data in this case cannot be a disguised restriction on trade.

The TPP if adopted is going to be binding just like other trade agreements. Their enforceability is stronger than human rights conventions' thereof. Trade agreements affect countries beyond the ones that are currently involved in negotiations. Countries that are not signatory parties will likely be asked to accede to the given agreement as a condition of bilateral trade agreements with the US and other members.

Regional and global trade agreements therefore, put fundamental rights in danger and government should be held accountable for violating human rights in secret agreements to prioritize trade interests.

The Schrems decision will most likely determine the future of already existing and emerging privacy issues in a different way than it was anticipated before the judgment of the CJEU. The remaining issues include but are not limited to the going dark debate, data breaches and countries passing expansive surveillance laws.

CONCLUSION

The international debate over the protection of privacy and personal data is central across many of the current international relations areas. The resolution of these privacy debates will define the data protection and shape human rights protections for many generations. What if countries decide to impose encryption restrictions and/or mandate "golden key" backdoors? What if countries fail to provide for security of sensitive personally identifiable information? What if countries decide to pass expansive surveillance laws? What if trade agreements will override fundamental rights protections? The answers to these and other questions will determine whether national and international organizations can maintain human rights protections amidst the changing technological and political landscape.

From the perspective of the EU-US relations it is a key issue whether we anticipate legal or political answers to these dilemmas. Under the *Schrems* decision there is only one acceptable legal response which is to respect the fundamental right to privacy, and governments should adjust their policies accordingly.

From a political perspective, however, it is hard to be optimistic. What we see is that yes, countries are pushing for building backdoors into devices, yes, data breaches are accepted as everyday consequences of business conduct, yes, governments are increasing their surveillance powers and techniques and yes, trade agreements include restrictions to privacy.[104]

Therefore, there are emerging trends in the public and the private

sector as well that can endanger people's right to privacy and data protection both practically and legally. The presented legal cases have taken the right approach to protect privacy as a fundamental right.

National and international public officials, business leaders and human rights defenders have different roles in shaping the future of the Internet and privacy in particular. Transatlantic relations are one of the main scenes in the play and what happens here will certainly have a global effect. Therefore, the significance of the *Schrems* decision and its aftermath should not be underestimated.

Notes

[1] Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1155 (2013).

[2] *See* Glenn Greenwald, "NSA Collecting Phone Records Of Millions Of Verizon Customers Daily", *The Guardian*, June 6, 2013, http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order; Barton Gellman, "U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program", *Washington Post*, June 6, 2013, http://wapo.st/1LcAw6p.

[3] C-362/14, Schrems v Data Prot. Comm'r 2015 E.C.R. *Available at:* http://curia.europa.eu.

[4] *See* Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act or USA FREEDOM Act 50 U.S.C.§ 1801 note (2015); Peter Swire, "US Surveillance Law, Safe Harbor, and Reforms Since 2013", December 17, 2015, https://fpf.org/wp-content/uploads/2015/12/White-Paper-Swire-US-EU-Surveillance.pdf.

[5] Glenn Greenwald, "NSA Collecting Phone Records Of Millions Of Verizon Customers Daily", 2013.

[6] USA PATRIOT Act of 2001, Pub. L. 107–56, 115 Stat. 272, 287 (2001) (codified as amended at 50 U.S.C. §§ 1861–62 (2006)).

[7] Primary Order, In re Application of the FBI for an Order Requiring the Production of Tangible Things from [REDACTED] at 3, Dkt No. BR 13-80 (FISA Ct. Apr. 25, 2013), *Available at:* http://www.dni.gov/files/documents/PrimaryOrder_Collection_215.pdf.

[8] *Id* at iii n.1. The routing information included "session identifying information (e.g., originating and terminating telephone number, International Mobile Subscriber Identity (IMSI) number, International Mobile station Equipment Identity (IMEI) number, etc.), trunk identifier, telephone calling card numbers, and time and duration of call. *Id*.

[9] Office of the Director of National Intelligence, "DNI Announces the Declassification of the Existence of Collection Activities Authorized by President George W. Bush Shortly After the Attacks of September 11, 2001", December 21, 2013, http://icontherecord.tumblr.com/post/70683717031/dni-announces-the-declassification-of-the.

[10] Siobhan Gorman, Evan Perez, and Janet Hook, "U.S. Collects Vast Data Trove", *Wall Street Journal*, June 7, 2013, http://www.wsj.com/articles/SB10001424127887324299104578529112289298922.

[11] Report on the National Security Agency's Bulk Collection Programs for USA PATRIOT Act Reauthorization 3–5 (2011), *available at* http://www.dni.gov/files/documents/PrimaryOrder_Collection_215.pdf.

[12] *Ibid*. at v.

[13] *Ibid*. at iii–v.

[14] *Ibid*. at iii.

[15] *See* In re EPIC, 134 S. Ct. 638 (2013) (seeking mandamus review of the FISC order based on the argument that the court lacked jurisdiction to require ongoing production of all telephone metadata); ACLU v. Clapper, 785 F.3d 787 (2d Cir. 2015) (finding that the FISC order requiring production of telephone metadata exceeded the authority granted under Section 215); Klayman v. Obama, ___ F. Supp. 3d ___ (D.D.C. 2015) (granting injunctive relief); Smith v. Obama, 24 F. Supp. 3d 1005 (D. Idaho 2014).

[16] *See* In re Application of the FBI for an Order Requiring the Production of Tangible Things from [Redacted], No. Br. 13-109, 2013 WL 5741573 (FISA Ct. Aug. 29, 2013) ("Eagan Opinion").

[17] *Ibid*. at *vi.

[18] American Civil Liberties Union v. Clapper, 785 F.3d 787, 812–20 (2d Cir. 2015).
[19] Klayman v. Obama, ___ F. Supp. 3d ___, 2015 WL 6873127 at *10 (D.D.C. Nov. 9, 2015).
[20] *See* Hearing of the Senate Judiciary Committee on Strengthening Privacy Rights and National Security: Oversight of FISA (Foreign Intelligence Surveillance Act) Surveillance Programs (July 31, 2013) http://icontherecord.tumblr.com/post/57811913209/hearing-of-the-senate-judiciary-committee-on.
[21] Privacy and Civil Liberties Oversight Board, "Report on the Telephone Record Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court", January 23, 2014, http://perma.cc/FA8U-6RFJ ("*Based on the information provided to the Board, including classified briefings and documentation, we have not identified a single instance involving a threat to the United States in which the program made a concrete difference in the outcome of a counterterrorism investigation. Moreover, we are aware of no instance in which the program directly contributed to the discovery of a previously unknown terrorist plot or the disruption of a terrorist attack.*")
[22] *See* Review Group on Intelligence and Communication Technologies, "Liberty and Security in a Changing World: Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies" 104 (2013) ("*Our review suggests that the information contributed to terrorist investigations by the use of section 215 telephony meta-data was not essential to preventing attacks and could readily have been obtained in a timely manner using conventional section 215 orders.*")
[23] *See* Barton Gellman, "U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program", *Washington Post*, June 6, 2013, http://wapo.st/1LcAw6p.
[24] *Ibid*.
[25] *See* FISA Amendments Act of 2008: Hearing Before the Subcomm. on Crime, Terrorism, and Homeland Sec. of the H. Comm. on the Judiciary, 112th Cong. 27–37 (2012) (Statement of Marc Rotenberg, Executive Dir., EPIC).
[26] Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138 (2013).
[27] Privacy and Civil Liberties Oversight Board, Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act 5 (2014).
[28] *Ibid*. at vi.
[29] James Risen and Eric Lichtblau, "Bush Lets U.S. Spy on Callers Without Courts", *New York Times*, December 16, 2005, http://www.nytimes.com/2005/12/16/politics/bush-lets-us-spy-on-callers-without-courts.html?_r=0.
[30] *See* Craig Timburg, "NSA Slide Shows Surveillance of Undersea Cables", *Washington Post*, July 10, 2013, https://www.washingtonpost.com/business/economy/the-nsa-slide-you-havent-seen/2013/07/10/32801426-e8e6-11e2-aa9f-c03a72e2d342_story.html.
[31] *See* Siobhan Gorman and Jen Valentino-Devries, "New Details Show Broader NSA Surveillance Reach", Wall Street Journal, August 20, 2013, http://www.wsj.com/articles/SB10001424127887324108204579022874091732470.
[32] *Ibid*.
[33] *Ibid*.
[34] *Ibid*.
[35] 50 U.S.C. § 1881a(a).
[36] 50 U.S.C. § 1881a(c)(1)(A). These targeting procedures must be "reasonably designed" to ensure that surveillance "is limited to targeting persons reasonably believed to be located

outside of the United States" and prevent the "intentional acquisition" of communications that the government knows are purely domestic. 50 U.S.C. § 1881a(d)(1).

[37] 50 U.S.C. § 1881a(c)(1)(A). These minimization procedures must be "consistent with" those adopted for other FISA surveillance. 50 U.S.C. § 1881a(e).

[38] 50 U.S.C. § 1881a(g).

[39] Privacy and Civil Liberties Oversight Board, Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act 1 (2014), *available at* https://www.pclob.gov/library/702-Report.pdf.

[40] *Ibid*. at ii.

[41] *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138, 1146 (2013).

[42] *Ibid*. at 1155.

[43] Wikimedia Foundation v. NSA, ___ F. Supp. 3d ___, 2015 WL 6460364 (D. Md. Oct 23, 2015).

[44] *See*, *e.g.*, Barton Gellman and Ashkan Soltani, "NSA Collects Millions of E-mail Address Books Globally", *Washington Post*, October 14, 2013, https://www.washingtonpost.com/world/national-security/nsa-collects-millions-of-e-mail-address-books-globally/2013/10/14/8e58b5be-34f9-11e3-80c6-7e6dd8d22d8f_story.html; Kevin Rawlinson, "NSA Surveillance: Merkel's Phone May Have Been Monitored for Over 10 Years", *The Guardian*, October 26, 2013, http://www.theguardian.com/world/2013/oct/26/nsa-surveillance-brazil-germany-un-resolution.

[45] *See* David S. Kris and J. Douglas Wilson, National Security Investigations and Prosecutions § 2:7 (2d Tomson/West, 2012).

[46]*See* PCLOB, "*Examination of E.O.* 12333 Activities in 2015", 2015, *available at* https://pclob.gov/library/20150408-EO12333_Project_Description.pdf.

[47] USA FREEDOM Act of 2015, Pub. L. 114-23, 129 Stat. 268.

[48] *See* Press Release, "Presidential Policy Directive–Signals Intelligence Activities" January 17, 2014, https://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities.

[49] *See generally* Alan Butler, *Standing Up to Clapper: How to Increase Transparency and Oversight of FISA Surveillance*, 48 New Eng. L. Rev. 55, 91–100 (2013).

[50] *Ibid*.

[51] *See* Editorial Board, "A Stronger Bill to Limit Surveillance", *New York Times*, July 27, 2014, http://www.nytimes.com/2014/07/28/opinion/a-stronger-bill-to-limit-surveillance.html?_r=0.

[52] Charlie Savage and Jeremy W. Peters, "Bill to Restrict N.S.A. Data Collection Blocked in Vote by Senate Republicans", New York Times, November 18, 2014, http://www.nytimes.com/2014/11/19/us/nsa-phone-records.html.

[53] *See* Bill Chappell, "Senate Approves USA Freedom Act, Obama Signs It, After Amendments Fail," NPR, June 2, 2015, http://www.npr.org/sections/thetwo-way/2015/06/02/411534447/senateis-poised-to-vote-on-house-approved-usa-freedom-act.

[54] *See* "USA Freedom Act: What's In, What's Out", Washington Post, June 2, 2015, https://www.washingtonpost.com/graphics/politics/usa-freedom-act/; Alan Butler, "NSA Reform Moves Forward in Congress—With a Clear Prohibition on Bulk Collection But Still Missing Important Transparency and Oversight Provisions", Privacy Rights Blog at epic.org, May 14, 2014, http://epic.org/blog/2014/05/nsa-reforms-move-forward.html.

[55] Pub. L. 114-23 § 103, 129 Stat. 268, 272 (2015). The law also prohibits bulk collection

under the FISA Pen Register provision.; *See* Pub. L. 114-23 § 201, 129 Stat. 268, 277 (2015).
[56] Pub. L. 114-23 § 101, 129 Stat. 268, 269–270 (2015).
[57] Pub. L. 114-23 § 101(a)(3), 129 Stat. 268, 270 (2015).
[58] *See* Jodie Liu, "So What Does the USA Freedom Act Do Anyway?" LawFareBlog, June 3, 2015, https://www.lawfareblog.com/so-what-does-usa-freedom-act-do-anyway.
[59] *Ibid*.
[60] Remarks on United States Signals Intelligence and Electronic Surveillance Programs, 2014 Daily Comp. Pres. Doc. 30 (Jan. 17, 2014).
[61] Directive on Signals Intelligence Activities, 2014 Daily Comp. Pres. Doc. 31 (Jan. 17, 2014).
[62] Peter Swire, "US Surveillance Law, Safe Harbor, and Reforms Since 2013", December 17, 2015.
[63] *Ibid*. at i.
[64] *See generally id*.
[65] *Ibid*. at ii–iii.
[66] *Ibid*. At iii.
[67] *Ibid*. at iv.
[68] *Ibid*. at iv–vii.
[69] Office of the Director of National Intelligenve, "Signals Intelligence Reform: 2015 Anniversary Report" (2015), http://icontherecord.tumblr.com/ppd-28/2015/overview.
[70] *See* Lauren Bateman, "NSA, CIA, and the FBI Implementation of PPD-28", LawFareBlog, February 9, 2015, https://www.lawfareblog.com/nsa-cia-and-fbi-implementation-ppd-28.
[71] *Ibid*.
[72] *Ibid*.
[73] EPIC, "EU-US Data Transfer Agreement", 2015, https://epic.org/privacy/intl/data-agreement/index.html.
[74] 5 U.S.C. § 552a(a)(2); *See generally,* The Privacy Act 1974, EPIC (2015), https://epic.org/privacy/1974act/.
[75] *See, e.g.*, 15 U.S.C. § 1681a(c) (West 2015) (stating that the definition of "consumer" for purposes of the Fair Credit Reporting Act "means an individual"); 15 U.S.C. § 1692a(3) (West 2015) (stating that the definition of "consumer" for purposes of the Fair Debt Collection Practices Act "means any natural person obligated or allegedly obligated to pay any debt"); 18 U.S.C. § 2721(a)(1) (West 2015) (prohibiting under the Driver's Privacy Protection Act the disclosure of personal information about "any individual" in connection with a motor vehicle record).
[76] EPIC, "Statement of EPIC on H.R. 1428, the Judicial Redress Act of 2015", September 16, 2015, https://epic.org/foia/umbrellaagreement/EPIC-Statement-to-HJC-on-HR1428.pdf.
[77] EPIC, "EPIC Recommends Changes to Judicial Redress Act", September 16, 2015, available at https://epic.org/2015/09/epic-recommends-changes-to-jud.html.
[78] U.S. Department of Commerce, "Safe Harbor Privacy Principles", last updated January 30, 2009, http://export.gov/safeharbor/eu/eg_main_018475.asp.
[79] Directive 95/46/EC of the European Parliament and of the Council of Oct. 24, 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995, O.J. (L 281) 31, lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML.
[80] Article 25(6) of Directive 95/46/EC of the European Parliament and of the Council of 24

October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (O.J. 1995 L 281, p. 31), as amended by Regulation (EC) No 1882/2003 of the European Parliament and of the Council of 29 September 2003 (OJ 2003 L 284, p. 1) ('Directive 95/46'); Marc Rotenberg, "Letter to the Editor", New York Times, October 13, 2015, http://www.nytimes.com/2015/10/13/opinion/digital-privacy-in-the-us-and-europe.html.

[81] Paragraph 73 of C-362/14, Schrems v Data Protection Commissioner, 2015.

[82] Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos, May 13, 2014, http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&doclang=EN [http://perma.cc/ED5L-DZRK].

[83] Joined Cases C-293/12 and C-594/12, Digital Rights Ireland Ltd v. Minister for Communication et al and Kärtner Landesregierung et al, judgment of 8 April 2014, nyr.

[84] Directive 2006/24/EC O.J. 2006 L 105/54.

[85] Hungarian Civil Liberties Union, "The never ending data retention", June 22, 2015, http://tasz.hu/node/16417.

[86] 10 Human Rights Organizations and Others v the United Kingdom (Application no 24960/15), Bureau of Investigative Journalism and Alice Ross v the UK (Application no. 62322/14).

[87] Godwin v. the United Kingdom (1996) 22 EHRR 123, [§ 39].

[88] Tarsasag a Szabadsagjogokert v Hungary (2009) Application no 37374/05, Chamber Judgment, ECtHR.

[89] European Commission, "Commissioner Jourová's remarks on Safe Harbour EU Court of Justice judgment before the Committee on Civil Liberties, Justice and Home Affairs (Libe)", October 26, 2015, http://europa.eu/rapid/press-release_SPEECH-15-5916_en.htm. European Commission, "Restoring Trust in EU-US Data Flows", November 27, 2013, http://europa.eu/rapid/press-release_MEMO-13-1059_en.htm.

[90] EPIC, "NGOs Reject 'Safe Harbor 2.0', Urge EU and US to Protect Fundamental Rights", November 12, 2015, https://epic.org/2015/11/ngos-reject-safe-harbor-20-urg.html. European Commission, "Commission issues guidance on transatlantic data transfers and urges the swift establishment of a new framework following the ruling in the Schrems case", November 6, 2015, http://europa.eu/rapid/press-release_IP-15-6015_en.htm.

[91] Article 29 Working Party, "Statement of the Article 29 Working Party", October 16, 2015, http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf.

[92] Europe v Facebook (2015), available at http://www.europe-v-facebook.org/.

[93] Europe v Facebook, "PRISM 2.0 - Complaints after the Judgment C-362/14, Europe v Facebook", December 2, 2015, http://www.europe-v-facebook.org/EN/Complaints/PRISM_2_0/prism_2_0.html.

[94] Congressman Jim Sensenbrenner's Press Release, "Judicial Redress Act Final Step in Umbrella Agreement with EU", September 8, 2015, http://sensenbrenner.house.gov/news/documentsingle.aspx?DocumentID=397867.

[95] European Commission, "Statement by EU Commissioner Věra Jourová on the finalisation of the EU-US negotiations on the data protection Umbrella Agreement", Press Release, September 8, 2015, http://europa.eu/rapid/press-release_STATEMENT-15-5610_en.htm.

[96] Douwe Korff, "EU-US Umbrella Data Protection Agreement: Detailed analysis", FREE Group, October 14, 2015, http://free-group.eu/2015/10/14/eu-us-umbrella-data-

protection-agreement-detailed-analysis-by-douwe-korff/.

[97] Andrew Woods, "Lowering the temperature on the Microsoft-Ireland case", Brookings, September 21, 2015, http://www.brookings.edu/blogs/techtank/posts/2015/09/21-lowering-temperature-microsoft-case. Sam Thielman, "Decision in Microsoft case could set dangerous global precedent, experts say", *The Guardian*, September 9, 2015, http://www.theguardian.com/technology/2015/sep/09/microsoft-federal-case-data-security-precedent.

[98] Digital Constitution, "Milestones and Documents", 2015, http://digitalconstitution.com/about-the-case/.

[99] Alexander Plaum, "The impact of forced data localization on fundamental rights", *Access Now*, June 4, 2014, https://www.accessnow.org/blog/2014/06/04/the-impact-of-forced-data-localisation-on-fundamental-rights.

[100] David M. Brown, "Trans-Pacific Partnership Would Promote Cross-border Data Transfers and Restrict Data Localization", *Data Privacy Monitor*, November 10, 2015, http://www.dataprivacymonitor.com/international-privacy-law/trans-pacific-partnership-would-promote-cross-border-data-transfers-and-restrict-data-localization/.

[101] Zakharov v Russia (2015) Application no 47143/06, Chamber Judgment, ECtHR.

[102] European Court of Human Rights, "Arbitrary and abusive secret surveillance of mobile telephone communications in Russia", Press release, December 4, 2015, http://hudoc.echr.coe.int/eng-press#.

[103] Cécile Barbière, "Parliament's opposition to TTIP arbitration on the rise", *Euractiv*, April 27, 2014, http://www.euractiv.com/sections/trade-society/parliaments-opposition-ttip-arbitration-rise-313935. Chris Johnston, "Berlin anti-TTIP trade deal protest attracts hundreds of thousands", *The Guardian*, October 10, 2015, http://www.theguardian.com/world/2015/oct/10/berlin-anti-ttip-trade-deal-rally-hundreds-thousands-protesters.

[104] Max J. Rosenthal, "How the Paris Attacks Could Lead to More Government Snooping on Americans", *Motherjones*, November 20, 2015, http://www.motherjones.com/politics/2015/11/digital-privacy-under-attack-again-after-paris. Joe Davidson, "OPM 'failures' are topic of fifth hearing on data breach", *The Washington Post*, July 7, 2015, https://www.washingtonpost.com/news/federal-eye/wp/2015/07/07/opm-failures-are-topic-of-fifth-hearing-on-data-breach/. Estelle Masse, "Access Now testifies on mass surveillance at European Parliament", *Access Now*, December 8, 2015, available at https://www.accessnow.org/access-now-testifies-on-mass-surveillance-in-the-eu-at-european-parliament/.