National Security: The Achilles Heel of Transatlantic Data Flows

Laura E. Gardner[1]

The close relationship between the United States and the European Union has long been evidenced both in their sizable trade relationship and in their close cooperation on a variety of security issues. As the digital economy has taken on increasing prominence, the transatlantic flow of data has also grown, with the amount of data flowing cross-border between the United States and Europe currently assessed to be the highest in the world.[2]

The flow of data between the United States and Europe, however, has encountered a significant obstruction. In regulating data flows, the United States and Europe have taken divergent approaches, reflecting their different philosophical approaches and different historical experiences. In the European Union, privacy is viewed as a core democratic value that must be safeguarded even at the expense of other values.[3] In the United States, privacy does not enjoy such a privileged position, and privacy law focuses on seeking the appropriate balance, weighing the value of data protection against potential consumer and other harms.[4] One such potential harm being taken into account in data protection and privacy debates is potential harm or threats to national security.

Despite the growing significance of transatlantic data flows to the economies of the United States and the European Union, the divergent approaches to seeking balance between national security interests and data protection interests currently threatens the continued growth of the transatlantic digital trade relationship. The revelations by Edward Snowden in 2013 that the United States had engaged in extensive surveillance and collection of data, including of EU citizens' data, cast a spotlight on the differences in the U.S. and European approaches. The United States and the European Union must now coordinate their existing frameworks for the transfer of data from the European Union to the United States in order to restore trust and facilitate the free flow of data.

This paper will begin with a brief description of the respective approaches to data protection taken in the European Union and the United States, as well as the legal framework for transfers from the European Union to the United States. Following this background will be a description of the challenging legal landscape that has emerged following the Snowden

---

[1] Bosch Fellow, 2014-2015. Views expressed in this paper are those of the author and do not reflect the official policies or positions of the Bosch Foundation, the author's Bosch Stage Institutions, or the U.S. Government.

[2] Joshua P. Meltzer, *The Importance of the Internet and Transatlantic Data Flows For U.S. and EU Trade and Investment* (2014).

[3] Paul M. Schwartz and Daniel J. Solove, *Reconciling Personal Information in the United States and the European Union*, 102 California Law Review 877 (2014).

[4] *Id.* at 877.

revelations, and potential next steps towards finding an appropriate balance between protecting security interests and protecting citizens' data in order to facilitate the continued growth of transatlantic digital trade.

Overview of Data Protection Framework

Data Protection in the European Union

The processing and protection of personal data in the European Union is currently governed by European Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data (the Data Protection Directive), which was adopted on October 24, 1995 and implemented through national laws in each of the EU Member States.[5] The Data Protection Directive has two objectives: that EU Member States protect the fundamental rights and freedoms of natural persons, in particular their right to privacy with respect to the processing of personal data, and that Member States neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection of such personal data.[6]

Advances and growth in technology and its global use have resulted in changes in the way that personal data is collected and processed since the adoption of the Data Protection Directive and Member States' implementing laws; additionally, the divergent national interpretations of and differing enforcement approaches to the Data Protection Directive have proved challenging. Due to these challenges, the European Commission proposed a draft new General Data Protection Regulation on January 25, 2012, which would seek to reform the current data protection rules to account for technological advances and to reduce fragmentation among the EU Member States.[7] The Data Protection Regulation remains subject to debate, discussion, and revision ("trilogues" among the European Commission, European Parliament, and the European Council to discuss each entity's views on the language in the draft Data Protection Regulation and seek to reach consensus will take place in Summer 2015).[8]

For the time being, however, the Data Protection Directive remains in force. In addition to protecting personal data being processed in the European Union, the Data Protection Directive sets the rules for transfers of personal data from EU Member States to "third countries" outside the EU. The Commision may find that a third country ensures an

[5] DLA Piper, *Data Protection Laws of the World*, 5; Data Protection Directive
[6] Peter Hustinx, *"EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation"*, 9.
[7] DLA Piper, *supra* note 5, at 5.
[8] Press Release, European Council, Data Protection: Council Agrees on a General Approach, June 15, 2015.

adequate level of protection, making an "adequacy decision" which will allow transfers to be made freely from the European Union to that third country under Article 25 of the Data Protection Directive.[9] Additionally, personal data may be transferred to a third country which has not been determined to have adequate protections if: additional safeguards such as appropriate contractual clauses or binding corporate rules are put into place to protect privacy, if a set of the Commission's "standard contractual clauses" are put into place to protect the data being transferred, or the data being transferred falls under an exemption.[10]

Data Protection in the United States

There is no single comprehensive law governing the protection of data in the United States. The United States instead has a patchwork of federal and state laws that govern the protection of data. A variety of these laws are sectoral in nature, governing the use of financial or health information, or applying to activities using personal information such as telemarketing. The Federal Trade Commission is active in this sphere, and relies on its authority to enforce broad consumer protection laws in order to prohibit unfair or deceptive practices involving the disclosure of, and security procedures for protecting, personal information, as well as to enforce more targeted privacy laws protecting financial and health information, information about children, and credit information .[11] [12]

Data Transfers from the European Union to the United States

In determining whether the United States provided an adequate level of protection, the Working Party on the Protection of Individuals with regard to the Processing of Personal Data initially concluded that "the current patchwork of narrowly-focussed sectoral laws and voluntary self-regulation [in the United States] cannot at present be relied upon to provide adequate protection in all cases for personal data transferred from the European Union."[13] Consequently, the United States Department of Commerce and the European Commission negotiated an agreed benchmark standard of protection in the form of the Safe Harbor

---

[9] European Commission, *Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU,* 2, November 27, 2013.

[10] European Commission, 20, *Frequently Asked Questions Relating to Transfers of Personal Data from the EU/EEA to Third Countries*. Data may also be transferred if it falls within one of the six derogations listed in the Data Protection Directive, including the data subject's providing unambiguous consent to the proposed transfer, or the transfer is necessary for the protection of the vital interests of the data subject.

[11] Ieuan Jolly, *Data Protection in the United States: An Overview*, Practical Law, Thompson Reuters.

[12] Federal Trade Commission, *Privacy Enforcement and Safe Harbor: Comments of FTC Staff to European Commission Review of the U.S.-EU Safe Harbor Framework*, November 12, 2013.

[13] Working Party on the Protection of Individuals with Regard to the Processing of Personal Data (Article 29 Working Party), European Commission, *Opinion 1/99 concerning the level of data protection in the United States and the ongoing discussions between the European Commission and the United States Government*, adopted by the Working Party on January 26, 1999.

Principles. In July 2000, the European Commission adopted Decision 520/2000/EC3[14] recognizing the Safe Harbor Privacy Principles and the related Frequently Asked Questions (together Safe Harbor) as providing adequate protection, thus allowing personal data to be transferred from the European Union to those U.S. companies and entities that self-certified their compliance with Safe Harbor.

Companies self-certifying that they comply with the Safe Harbor are certifying their compliance with seven principles: notice, choice, onward transfer, security, data integrity, access, and enforcement.[15] Only U.S. organizations that are subject to the Federal Trade Commission's jurisdiction, or U.S. carriers or ticket agents that are subject to the jurisdiction of the Department of Transportation, may participate in Safe Harbor.[16] This requirement provides the "teeth" of Safe Harbor, subjecting a company's self-certification and subsequent self-regulation of its compliance to potential enforcement actions, as a "failure to comply with [its] self-regulation must also be actionable under Section 5 of the Federal Trade Commission Act prohibiting unfair and deceptive acts or another law or regulation prohibiting such acts.[17]

Safe Harbor in the Wake of the Snowden Revelations

National Security as an Exception to Digital Trade under Safe Harbor

Under Safe Harbor, extensive amounts of personal data have been transferred from the European Union to the United States, allowing U.S. companies such as Google and Facebook, among many others, to grow their presence in the EU. In late September 2013, 3,246 companies had self-certified their compliance with Safe Harbor.[18] European companies and data controllers could be reasonably confident that the data they were transferring to the United States was being "adequately protected" given the protections of the self-certification to the seven principles set out in Safe Harbor and enforcement mechanisms of Safe Harbor.

This personal data of EU citizens was being transferred under the assumption that it would be adequately protected under Safe Harbor, but that assumption was completely undermined in 2013, with the revelations by Edward Snowden that United States intelligence agencies had been engaging in widespread surveillance and data collection,

[14] Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce.
[15] Alvaro Puig, *Trans-Atlantic Privacy Protection,* Federal Trade Commission Business Blog, March 9, 2015.
[16] U.S. Department of Commerce, *Welcome to the U.S.-EU and U.S.-Swiss Safe Harbor Frameworks.*
[17] U.S.-EU Safe Harbor Principles.
[18] *Communication from the Commission to the European Parliament and the Council, supra* note 9.

impacting both U.S. citizens and European citizens, whose data had been transferred to the United States under the protections of Safe Harbor. Citizens in the European Union were outraged by the revelations of widespread surveillance, with the strongest reactions coming from German citizens[19], and data protection authorities in many EU Member States followed suit in expressing their outrage, including the declaration by German data protection authorities that the widespread surveillance indicated a strong likelihood that the Safe Harbor principles were being violated.[20]

Although the U.S. government's widespread surveillance and data collection were widely seen as an indication that Safe Harbor had failed in its efforts to protect data, the data collection and surveillance were in fact consistent with the terms of Safe Harbor, which provides a national security exception to the principles of data protection. As the Commission itself noted in its Communication on the Functioning of Safe Harbor, "the exceptional processing of data for the purposes of national security, public interest or law enforcement is provided under the Safe Harbour scheme."[21] Safe Harbor provides that "adherence to these Principles may be limited to the extent necessary to meet **national security**, public interest, or law enforcement requirements."

U.S. intelligence agencies had clearly collected data in furtherance of their missions, including the protection of national security, so could argue that their data collection activities fell within the national security exception to Safe Harbor. But the outrage that met Snowden's disclosures indicated that the belief that these actions were "necessary" to meet national security requirements was not universally shared, and particularly seemed inconsistent with the European Union's perspective on which actions might be necessary to meet national security requirements. As the Commission noted in its Communication on the Functioning of Safe Harbor, "the large scale access by intelligence agencies to data transferred to the US in the context of commercial transactions was not foreseeable at the time of adopting the Safe Harbour." Implied in this statement is that the surveillance went beyond the scope of the exception as envisioned by the Commision when Safe Harbour was adopted; given the reaction to the disclosures of surveillance, particularly in Europe, it seems plausible that few European leaders had envisioned that the protection of national security interests could entail large-scale collection of EU citizens' data.[22]

---

[19] *ARD-Deutschlandtrend: Bürger trauen Obama und den USA nicht mehr,* Spiegel Online, November 8, 2013.
[20] Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, *Entschließung der 89. Konferenz der Datenschutzbeauftragten des Bundes und der Ländern am 18./19. Mai März 2015 in Wiesbaden Safe Harbor bietet keinen ausreichenden Schutz für den Datentransfer in die USA*, March 19, 2015.
[21] *Communication from the Commission to the European Parliament and the Council, supra* note 9.
[22] Steven Erlanger, *Outrage in Europe Grows Over Spying Disclosures,* The New York Times, July 1, 2013.

However, the national security exception is not unique to the Safe Harbor framework; similar exceptions are built into a variety of different trade agreements, and their appropriate scope has often been subject to debate.

> National security is the Achilles' heel of international law. Wherever international law is created, the issue of national security gives rise to some sort of loophole…"[23]

National security exceptions are found in a variety of multilateral trade agreements, perhaps most significantly in the World Trade Organization's General Agreement on Tariffs and Trade (GATT), which includes a national security exception allowing a WTO member to opt out of its requirements under the trade agreement when that WTO member considers it to be necessary to protect its essential security interests. Although the scope of national security exceptions is subject to debate (and the varied language used to describe national security exceptions in different agreements leads to different results), the scope is generally quite broad and deference is given to the country using the national security exception in interpreting whether the national security exception applies.

In determining whether the U.S. surveillance programs appropriately fall within the national security exception of Safe Harbor, the first threshold question is whether the interests that the United States was seeking to protect are appropriately termed national security interests, and that question is easily answered in the affirmative.[24] However, the question remains whether these particular actions were "necessary" as required by the exception ("to the extent necessary to protect national security interests") given their unprecedented scale. In particular, the Article 29 Working Party has queried whether "the seemingly large-scale and structural surveillance of personal data that has...emerged can still be considered an exception strictly limited to the extent necessary."[25] It is clear from public outcry, particularly in the European Union, that the public also doubts whether this scale of surveillance is truly "necessary." Nevertheless, given the deference generally given to a state's own interpretation of the national security exception, the U.S. intelligence agencies' assertion that these actions are necessary is likely to be sufficient evidence that these actions fell within the national security exception of Safe Harbor.

---

[23] Hannes L. Schloemann and Stefan Ohlhoff, *"Constitutionalization" and Dispute Settlement in the WTO: National Security as an Issue of Competence*, 93 Am. J. Intl. L. 424, 426 (1999).

[24] Contrast the United States' invocation of the national security exception of GATT for the Helms-Burton secondary boycott of Cuba and the Massachusetts selective purchasing law against Burma, where the United States argued in part that these measures served U.S. security interests because they responded directly to human rights violations. These invocations demonstrate a broader interpretation of U.S. "security interests" than that which might be used to defend the U.S. surveillance programs at issue under Safe Harbor.

[25] Article 29 Data Protection Working Party, *Letter to Vice President Viviane Reding, Commissioner for Justice, Fundamental Rights and Citizenship, European Commission*, August 13, 2013.

Questions of interpretation and compliance with Safe Harbor are determined under U.S. law; the legality of these mass surveillance programs is still being reviewed in U.S. courts.[26] However, these U.S. courts are not examining the specific question of whether these surveillance programs violated Safe Harbor through the collection of EU citizens' data or whether the programs' surveillance activities were exempt from Safe Harbor requirements because they were necessary to protect national security. And though U.S. law governs questions of interpretation of Safe Harbor, there are also pending questions regarding the interpretation of EU law in light of the mass surveillance programs.

The Snowden Revelations as Evaluated under EU Law

Even if we assume that the surveillance programs do fall within the national security exception to Safe Harbor, the Safe Harbor national security exception and the Safe Harbor principles themselves may be inconsistent with EU law. An Austrian law student, Max Schrems, has brought various claims against Facebook starting in 2013, charging that the United States failed to provide the adequate protection required under the EU Directive for personal data transferred outside of the European Union.[27] Mr. Schrems argues that Safe Harbor has *never* provided adequate protection of personal data transferred outside the European Union, and that the revelations made by Snowden regarding the scope of U.S. surveillance have demonstrated that Safe Harbor is "even more illegal".[28] The Schrems case raises both the question of whether the Safe Harbor agreement, with its national security exception that the Snowden revelations have shown to be an extensive exception, is consistent with EU law, and whether EU Member States have the authority to re-evaluate the European Commission's adequacy decisions.

Although Safe Harbor itself is governed by U.S. law, the adequacy decision through which Safe Harbor was adopted by the European Union is governed by EU law, and it is this adequacy decision that has been called into question in the Schrems case. Schrems has argued that a determination that a third country provides an adequate level of protection must take into account current EU jurisprudence. Specifically, the Charter of Fundamental Rights of the European Union[29] (the EU Charter)'s protections of the right to privacy and data protection must be adequately protected in a third country in order for that country to be considered as having adequate level of protection to allow for EU citizens' data to be transferred to that country. Evaluating whether a third country meets these standards will

[26] The U.S. Court of Appeals for the Second Circuit ruled that the surveillance programs were overbroad and not authorized by statute. Similar questions are currently under consideration in the U.S. Courts of Appeals for the 9th Circuit and the DC Circuit. Noah Feldman, *Court vindicates Snowden, says no to secret laws*, The Morning Call, May 7, 2015.
[27] Europe Versus Facebook, "PRISM" Complaints against Facebook, Apple, Skype, Microsoft and Yahoo!
[28] Gail Crawford, *Snowden's Legacy: Safe Harbor under fire at the CJEU*, Latham & Watkins: Global Privacy & Security Compliance Law Blog, March 26, 2015.
[29] Charter of Fundamental Rights of the European Union, December 18, 2000.

necessarily include a review of current jurisprudence as to the scope of these EU Charter protections.

The recent Digital Rights ruling[30] on the EU Data Retention Directive provides some additional information on the scope of EU Charter's Articles 7 and 8, which protect the right to privacy and data protection, in the context of data collection and surveillance. The EU Data Retention Directive required telecommunications service providers to retain significant amounts of data on the use of all forms of telecommunications by all individuals within the EU, to be used by law enforcement agencies for investigations into serious crime or terrorism (and with no detailed regulation of access to and use of the data by those law enforcement agencies).[31]

In this Digital Rights judgment, the Court of Justice of the European Union (CJEU) held that the EU Data Retention Directive interfered with the rights to privacy and data protection set out in the EU Charter. The CJEU found that some level of interference with these rights is permissible if justified by enumerated objectives set out in the Charter, including the objective of protecting public safety, and the CJEU did find that there was a public safety justification for the restrictions on the rights of privacy and data protection contained in the Directive.

The CJEU then examined whether the restrictions were proportionate, using a strict level of review in light of the nature of the rights impacted and the nature and seriousness of the infringement of those rights and of the objective pursued. Due to the broad scope of the data collection, the nearly unlimited access to data provided to law enforcement agencies, and the lack of sufficient safeguards, the CJEU found that the EU Digital Retention Directive was overreaching, and the EU Digital Retention Directive was invalidated, effectively prohibiting mass surveillance in the European Union.

The mass surveillance and collection programs in the United States can be closely analogized to those authorized under the EU Digital Retention Directive, as the U.S. programs also allowed the retention of significant amounts of data and were not subject to detailed regulation of access to and use of the data by the agencies collecting the data.[32] Although a public objective (public safety in the case of the EU Digital Retention Directive,

---

[30] Digital Rights Ireland v. Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality, and Law Reform, Commissioner of the Garda Síochána, Ireland, the Attorney General, Judgment of the Court (Grand Chamber), April 8, 2014, In Joined Cases C-293/12 and C-594/12.

[31] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

[32] Oversight of the surveillance programs, including by the Foreign Intelligence Surveillance Court, has been criticized as being inadequate. Evan Perez, Secret Court's Oversight Gets Scrutiny, The Wall Street Journal, June 9, 2013.

national security for the U.S. data collection programs) provides the justification for these data collection programs, they fail tests of proportionality.

Although the CJEU did not look at third countries' programs analogous to the EU Digital Retention Directive, if such data collection is overreaching in the European Union, then such data collection of EU citizens' data in third countries would similarly overreach and threaten the EU Charter's protections of privacy and data protection. While the CJEU does not have jurisdiction to allow it to evaluate surveillance programs in place across the world, the European Commission's adequacy decisions to allow for transfer of data can take into account CJEU jurisprudence and take into account whether data being sent to third countries will receive the same protections that such data is accorded in the European Union - including taking into account the EU Charter's protections and the CJEU's related finding that these protections are violated when data is subject to mass surveillance and collection by governments, and law enforcement agencies in third countries have unfettered discretion to review and use such data.

The Irish High Court did look to the EU Charter in responding to Schrem's allegations that Safe Harbor fails to provide adequate protection to EU citizens.[33] The judge stated that the "Snowden revelations demonstrate a massive overreach on the part of the security authorities, with an almost studied indifference to the privacy interests of ordinary citizens. Their data protection rights have been seriously compromised by mass and largely unsupervised surveillance programs."[34] However, the Irish High Court did not decide whether Safe Harbor provides adequate protection, instead referring the case to the CJEU, with the request that the CJEU answer the question of whether the Irish data protection authority has independent authority to review European Commission adequacy decisions - and specifically whether the Irish data protection authority has authority to review the Safe Harbor adequacy decision.

But as the CJEU continues to consider this specific question of the division of authority within the European Union[35], the larger question remains of whether Safe Harbor could possibly meet the adequacy standards of the EU Directive if it continues to contain a national security exception which we now know provides the legal loophole through which U.S. intelligence agencies can undertake widespread surveillance and data collection,

---

[33] Schrems v. Data Protection Commissioner, High Court of Ireland, 2013 765 JR, June 18, 2014.
[34] *Id.*
[35] The Advocate General's nonbinding opinion was originally scheduled to be released on June 24, 2015, but was delayed and no new date has been set. The CJEU decision will be made following the Advocate General's opinion, and is expected by October. Although the Advocate General's opinion is non-binding, it could strongly influence the ultimate CJEU decision. It is worth noting that although the question presented to the CJEU is the relatively narrow question of the competency of data protection authorities to reevaluate adequacy decisions made by the Commission, the CJEU may choose to issue an opinion on a broader question of the continuing adequacy of Safe Harbor.

failing to demonstrate proportionality and potentially undermining the protections of the EU Charter.

And what is the path to reform of Safe Harbor? This paper will provide a brief analysis of the feasibility and possibilities of three potential avenues for reform: revision of Safe Harbor to limit the national security exception; closer cooperation on intelligence collection in order to ensure that U.S. intelligence agencies' surveillance efforts are appropriately limited in scope; and ensuring avenues for EU citizens to seek redress for overreaching by U.S. intelligence agencies.

Post-Snowden Options for Reform

Safe Harbor Revision

Efforts to negotiate a revised Safe Harbor are currently underway, and the ongoing nature of the negotiations has also been raised in the Schrems case as a factor the CJEU should consider in its decision. The CJEU has been asked by Ireland and the European Commission to defer its decision until after the ongoing negotiations to revise Safe Harbor are completed, a task which the European Commission and the U.S. Department of Commerce are seeking to complete in Summer 2015. The negotiations to revise Safe Harbor have been ongoing since late 2013, based on a set of recommendations published by the European Commission in November 2013.[36] As Safe Harbor was approved by the European Union in 2000, a revision to update Safe Harbor is in some respects overdue, and many of the recommendations put forward by the Commission will serve to update Safe Harbor and are relatively unobjectionable. The challenges in implementing the Commission's recommendations arise in the area of security and surveillance, particularly with respect to two of the the Commission's recommendations regarding access to data by U.S. authorities.

The European Commission recommended that companies that have self-certified under Safe Harbor should include in their privacy policies information on the extent to which U.S. law allows public authorities to collect and process data which is being transferred under Safe Harbor.[37] This recommendation poses a challenge for many U.S. companies, as the data being collected and processed by U.S. law enforcement agencies is often confidential, and the requests by the U.S. law enforcement agencies to the U.S. companies requesting access to their data are themselves frequently also confidential. U.S. companies may not be able to provide a full and accurate accounting of the extent to which the data they have collected may be accessed by U.S. law enforcement agencies, and the scope of data

[36] *Communication from the Commission to the European Parliament and the Council, supra* note 9.
[37] *Id.*

collection allowed under U.S. law may also not be known to U.S. companies, as determinations regarding the scope of data collection are frequently made under the Foreign Intelligence Surveillance Act (FISA), under which hearings and determinations are confidential. U.S. companies simply lack the knowledge of the extent to which U.S. law allows the collection and processing of private companies' data by public authorities, and to the extent that U.S. companies do know to what extent their own data is being collected or processed by public authorities, they may be obligated by law not to disclose that information. Some U.S. companies have voiced their objections to the intransparency in their disclosures to public authorities, and have lobbied for greater transparency and the ability to provide some amount of disclosure to the public regarding the scope of government surveillance.[38] However, it seems clear that U.S. companies cannot currently certify the full extent of U.S. government access to data as would be required under the Commission's recommendation.

The Commission has also recommended that the national security exception to Safe Harbor be used only to the extent that it is "strictly necessary or proportionate." This language would narrow the current scope of the Safe Harbor national security exception, which currently allows any "necessary" national security exceptions to be made, without requiring a higher level of "strictly necessary" or any proportionality review. The language recommended by the Commission goes further than the language contained in the EU Directive, but does reflect the increasing focus on proportionality in EU jurisprudence (as evidenced in the EU Data Retention Directive case described above in this paper) as well as the language contained in draft versions of the Data Protection Regulation, which reflects the direction in which the European Union would like to move in terms of data protection:

> The Commission's draft EU Regulation states that "Restrictions on specific principles...and on certain related obligations of the controllers may be imposed by Union or Member State law, as far as **necessary and proportionate** in a democratic society to safeguard public security...Those restrictions should be in compliance with requirements set out by the Charter of Fundamental Rights of the European Union and by the European Convention for the Protection of Human Rights and Fundamental Freedoms."[39] The Parliament's draft language contains a similar provision limiting exceptions to those "**necessary and proportionate**" and in compliance with the human rights Charter and Convention.

Although the "necessary and proportionate" restriction is clearly aligned with both the jurisprudence of the CJEU in the Data Retention Directive case and the language that has been proposed for the Data Protection Regulation which will replace the Data Protection

[38] Richard Salgado, *Shedding some light on Foreign Intelligence Surveillance Act (FISA) requests*, Google Official Blog, February 3, 2014.
[39] *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*, Paragraph 59.

Directive, such restrictive language may not be acceptable to the United States. Specifically, the United States has historically insisted on a broad scope of flexibility in its interpretation of national security exceptions. By including a proportionality requirement, the language being used to outline the scope of the exception shifts to indicate that the use of the national security may be subject to a significantly higher level of review or analysis in order to determine whether the national security exception has been applied in a way that is "proportionate." Given the sensitivity of national security issues, it is unlikely that the United States would be willing to subject its decisions to any level of review, and particularly to the high level of scrutiny by the European Union that a proportionality test would require.

Closer Coordination on Intelligence

The outcome of these Safe Harbor negotiations is yet to be determined, but recent press reports indicate that a conclusion is expected to be reached during Summer 2015.[40] Closely connected with the Safe Harbor negotiations and happening concurrently is the negotiation of a Data Protection Umbrella Agreement between the United States and the European Union. This agreement would provide data protection for data which is transferred between the European Union and the United States for law enforcement purposes, including data being sent to the United States for the prevention, detection, investigation and prosecution of criminal offenses, including terrorism.[41] Although the negotiation of this Umbrella Agreement has received significantly less attention than the renegotiation of the Safe Harbor Agreement, it has the potential to significantly impact the balance between data protection and national security in the transatlantic context.

The goal of limiting the scope of the national security exception in Safe Harbor will likely be difficult to obtain, as discussed above, but the Umbrella Agreement offers the possibility of limiting potential access to/surveillance of EU citizens' data by developing mechanisms for closer coordination between the European Union and the United States on intelligence collection and surveillance. Increasing coordination between the intelligence agencies of the EU and the United States would help by providing EU intelligence agencies an earlier opportunity to provide input on scope and methods of surveillance and collection have been made. Additionally, by moving the dialogue on data protection in the surveillance context into the purview of intelligence agencies and out of the commercial space, it may be easier for consensus to be reached. U.S. intelligence agencies already work in concert with EU intelligence agencies on a variety of issues, and often share the same sets of objectives - which they may not be willing to discuss openly outside of the intelligence community. In the intelligence space, agencies on both sides of the Atlantic can speak more freely and

[40] Phil Bradley-Schmieg, *U.S. and EU Miss Target for Safe Harbor Renegotiation, But Remain Optimistic*, Inside Privacy: Updates on Developments in Global Privacy & Data Security from Covington & Burling LLP, June 5, 2015.
[41] European Commission, *Factsheet EU-US Negotiations on Data Protection*, June 2014.

openly about the objectives they are pursuing and potentially agree to limit their activities after an honest evaluation of the goals and the appropriate means or methods in reaching those goals.

Negotiation of a narrower scope for the national security exception in Safe Harbor has faced inherent limitations as the U.S. agency negotiating Safe Harbor - the U.S. Department of Commerce - is not a member of the U.S. intelligence community. The U.S. Department of Commerce therefore cannot make very extensive or concrete pledges to limit the range of action of the U.S. intelligence agencies. Additionally, U.S. industry would likely oppose any efforts to provide a more nuanced definition of national security, as companies would not want to be tasked with determining whether a specific deviation from the Safe Harbor principles would be "necessary and proportionate" to national security. Rather, U.S. industry would prefer that all such determinations be made by U.S. intelligence and security agencies. These determinations could be made through closer coordination between EU and U.S. intelligence agencies that can seek to work together to pursue the objective of protecting national security while also appropriately safeguarding the data of EU and U.S. citizens. There may be a greater likelihood of making progress in limiting the scope of surveillance by connecting the agencies that are engaged in that surveillance.

Redress for EU Citizens

In addition to increasing cooperation between law enforcement and intelligence agencies, the umbrella agreement currently under negotiation between the European Union and the United States seeks to set out a series of guarantees and safeguards that must always apply to data that is transferred for the purposes of law enforcement between the United States and the European Union.[42] Under the agreement, when personal data is transferred from the European Union to the United States for law enforcement purposes, it will be processed with safeguards satisfactory to both the United States and the European Union. The agreement will help to provide protection for EU citizens' data being transferred to the United States that is not otherwise covered by an agreement such as Safe Harbor.

A key component of the umbrella agreement is the requirement that EU citizens have enforceable rights regarding the protection of their personal data. This particular issue remains an outstanding and unresolved issue in the umbrella agreement negotiations, in part because new legislation is required to provide a fix.[43] President Obama has noted this particular issue in discussing the need to reform national security in response to concerns

[42] *Id.*
[43] David Meyer, *Europeans could get data protection rights in U.S.,* Politico: Europe Edition, June 18, 2015.

raised about widespread surveillance.[44] In January 2014, Obama specifically noted three related concerns regarding the expanded efforts of U.S. intelligence agencies following September 11: that U.S. intelligence agencies have the technological capacity to access routine communications worldwide, that the government collection and storage of bulk data creates a potential for abuse, and that the legal safeguards that restrict surveillance against U.S. persons (specifically the requirement that a warrant be issued before surveillance must be undertaken) do not apply to foreign persons overseas. Although this last concern is common across the globe - Obama noted that "few, if any, spy agencies around the world constrain their activities beyond their own borders" - it is also an issue that is central to the concerns raised by the European Union regarding the collection and surveillance activities of U.S. intelligence agencies vis-a-vis EU citizens' personal data.

It is this issue - guaranteeing the rights of EU citizens to seek redress for the violations of their data protection rights - that is one of the last remaining barriers to concluding the Umbrella Agreement[45] and, given how closely the negotiations of the Umbrella Agreement are tied to the renegotiation of Safe Harbor, likely one of the last remaining barriers to conclusion of the Safe Harbor negotiations. On this issue, there seem to be few voices of opposition, with then-Attorney General Eric Holder stating in June 2014 that the Obama Administration "is committed to seeking legislation that would ensure that, with regard to personal information transfered within the scope of our proposed [Umbrella Agreement], EU citizens would have the same right to seek judicial redress for intentional or willful disclosures of protected information, and for refusal to grant access or to rectify any errors in that information, as would a U.S. citizen under the Privacy Act."[46] Google also voiced its support for the extension of the protections of the U.S. Privacy Act to EU citizens in November 2014.[47] A bipartisan bill introduced in June 2015 would provide citizens of "major U.S. allies" (including EU citizens) the right to ensure that information shared with the United States for law enforcement purposes is accurate and the ability to seek judicial recourse when that information is not accurate.[48] This bipartisan bill has been enjoying broad support of a variety of trade associations and organizations.[49] Passage of such a bill would pave the way for the conclusion of the Umbrella Agreement negotiations and provide EU citizens with a level of comfort that their data will enjoy increased protection, and that they have the avenues for recourse available to the United States.

---

[44] President Barack Obama, *Remarks on Changes to National Security Agency programs at the U.S. Department of Justice*, January 17, 2014, Transcript.
[45] *News in Brief/News Ticker: July 8th,* FTSE Global Markets, July 9, 2015.
[46] Press Release, U.S. Department of Justice, *Attorney General Holder Pledges Support for Legislation to Provide U.S. Citizens with Judicial Redress in Cases of Wrongful Disclosure of their Personal Data Transferred to the U.S. for Law Enforcement Purposes,* June 25, 2014.
[47] David Drummond, *It's time to extend the US Privacy Act to EU Citizens,* Google: Public Policy Blog, November 12, 2014.
[48] Press Release, Chris Murphy United States Senator for Connecticut, *Broad Support Lining Up Behind Murphy-Hatch Judicial Redress Act of 2015,* June 29, 2015.
[49] *Id.*

These three avenues for reform - revision of Safe Harbor; closer cooperation on intelligence collection through the Umbrella Agreement; and ensuring avenues for EU citizens to seek redress - are closely intertwined, and successful engagement on each of these is needed to effectively reform the framework for transatlantic data flows and restore trust.

Towards a Resolution

Transatlantic data flows will only continue to increase as digitalization moves beyond our computers and smartphones and into the objects we use in our daily life, with the advent of an "internet of things."[50] With the larger flows of data and increasing digitalization come new risks, including new vulnerabilities and increased ability to use remote access to cause physical destruction.[51] These new uses for data will also provide new opportunities and challenges for intelligence agencies to address these new risks as well as existing security risks. To prepare for these changes, it is vital that the European Union and the United States work to address the challenges facing the current framework for the transatlantic transfer of data now, in order to develop a framework that adequately protects both its citizens' data and our national security interests, on both sides of the Atlantic.

[50] Gitta Rohling, *Facts and Forecasts: Billions of Things, Trillions of Dollars*, Pictures of the Future: The Magazine for Research and Innovation, October 1, 2014.
[51] The President's National Security Telecommunications Advisory Committee, *DRAFT: NSTAC Report to the President on the Internet of Things*.