Domesticating the "Foreign" in Making Transatlantic Data Privacy Law[*]

Bilyana Petkova[**]

Abstract

Research shows that in the data privacy domain, the regulation promoted by frontrunner states in federated systems such as the United States or the European Union generates races to the top, not to the bottom. Institutional dynamics or the willingness of major interstate companies to work with a single standard generally create opportunities for the federal lawmaker to level up privacy protection.

This article uses federalism to explore whether a similar pattern of convergence (toward the higher regulatory standard) emerges when it comes to the international arena, or whether we witness a more nuanced picture. I focus on the interaction of the European Union with the United States, looking at the migration of legal ideas across the (member) state jurisdictions with a focus on breach notification statutes and privacy officers. The article further analyses recent developments such as the invalidation of the Safe Harbor Agreement and the adoption of a Privacy Shield. I argue that instead of a one-way street, usually conceptualized as the EU ratcheting up standards in the US, the influences between the two blocs are mutual. Such influences are conditioned by the receptivity and ability of domestic actors in both the US and the EU to translate, and often, adapt the "foreign" to their respective contexts. Instead of converging toward a uniform standard, the different points of entry in the two federated systems contribute to the continuous development of two models of regulating commercial privacy that, thus far, remain distinct.

Introduction

One of the defining values of federalism is "the framework it creates for… ongoing negotiation of disagreements large and small".[1] In making space for conflicts to unravel on the (sub)-state level, be that after a centralized solution has been adopted or before one has emerged, federalism provides both institutionalized spaces for

[*] For their helpful comments and constructive advice, I am indebted to the participants in the Privacy Law Scholars Conference held in Amsterdam in October 2015, as well as to my colleagues from the Information Law Institute of New York University where a second version of this article was presented in November 2016.

[**] Postdoctoral Fellow in Residence, New York University and Visiting Fellow, Yale Information Society Project.

[1] Cristina M. Rodríguez, *Negotiating Conflict Through Federalism: Institutional and Popular Perspectives* 123 YALE LAW JOURNAL 6 (2014) at 2097.

contestation and facilitates integration[2] in heterogeneous polities. Federalism explains the incremental local and state efforts aimed at changing national policy in the United States (U.S).[3] In the European Union (EU), evidence for a different bottom-up approach to federalism is the way Member State law found a secure pathway into European law through the general principles of EU law in the reasoning of the Court of Justice of the European Union (CJEU).[4] While federalism has come to be studied primarily either in the domestic settings of the U.S. or the EU,[5] it has also been evoked as a theoretical principle that can underpin the constitutionalization of international law.[6] However, little attention has been paid so far to how internal constitutional rules in federated systems promote policy innovation and how these internal innovations travel across borders. In this article, I use insights from federalist studies to argue that a pattern of convergence (toward the higher data privacy[7] regulatory standard) might emerge when it comes to the domestic settings of fully-fledged federations like the U.S. or in quasi-federated entities like the EU. In contrast, I show that when the analysis moves to the international arena, we witness a more nuanced picture. Instead of a one-way street, usually conceptualized as the EU ratcheting up data privacy standards in the U.S., the influences between the two blocs are mutual. Such influences are conditioned by the receptivity and ability of domestic actors in both the U.S. and the EU to translate, and often, adapt the "foreign" to their respective contexts. Instead of converging toward a uniform standard, the different

[2] Id. *See also* Heather K. Gerken & Ari Holtzblatt, *The Political Safeguards of Horizontal Federalism*, 113 MICHIGAN LAW REVIEW 57, 85 (2014), arguing the benefits of extraterritorial state laws that facilitate understanding of "otherness" and trigger nation-wide debates.

[3] Heather K. Gerken, *Windsor's Mad Genius: The Interlocking Gears of Rights and Structure*, 95 BOSTON UNIVERSITY LAW REVIEW 587, 602 (2015), offering a process-based interpretation of the landmark same-sex case; as Gerken explains, instead of saying anything about the constitutionality of state laws on gay marriage, the Supreme Court in *Windsor* invalidated only a federal statue, thus leaving the battle to unravel on the state level by "clearing the channels of political change", at 606.

[4] XAVIER GROUSSOT, GENERAL PRINCIPLES OF COMMUNITY LAW (2006). *See* also Koen Lenaerts, *Interlocking legal orders in the European Union and comparative law*, 52 THE INTERNATIONAL AND COMPARATIVE LAW QUARTERLY 4 (2003).

[5] This is without prejudice to the fact that the EU is not a federation and at most, displays some federal elements in its legal structure. Whereas a multitude of European scholars prefer to threat the EU as a *sui generis* polity, comparative legal analyses have shown the benefits of adopting a federalist framing for the EU, *see* ROBERT SCHÜTZE, FROM DUAL TO COOPERATIVE FEDERALISM. THE CHANGING STRUCTURE OF EUROPEAN LAW (2009).

[6] For a helpful summary, *see* Dirk Hanschel, *German Federal Thinking and International Law*, 2 GOETTINGEN JOURNAL OF INTERNATIONAL LAW 4 (2012); *See also* Elisabeth Zoller, *Aspects internationaux de droit constitutionnel: Contribution à la théorie de la federation d'Etats'*, 294 RECUEIL DES COURS DE L'ACADÉMIE DE DROIT INTERNATIONAL 39 (2002-I).

[7] Alongside the established right to privacy in Art. 7, the European Charter of Fundamental Rights (EU Charter) includes a separate right to data protection in Art. 8, Charter of Fundamental Rights of the European Union, OJ 2012 C-326/391. Herewith, I use the term 'data privacy' when referring to Arts. 7 and 8 of the EU Charter and when comparing them with the US regime.

points of entry in the two federated systems contribute to the continuous development of two models of regulating commercial privacy that remain thus far distinct.

The article proceeds as follows: in Part I, I briefly discuss the "trading up" logic and its limits; Part II recaptures the legacy of the defunct Safe Harbor agreement[8] as a stepping stone for the development of a distinctly American model of commercial privacy regulation. I show how the US model is being reinforced by modified state initiatives originating on both sides of the Atlantic: breach notification laws and corporate privacy officers. Part III discusses the EU model of data privacy in the light of the *Schrems*[9] judgment of the CJEU. I demonstrate that a different modification of state breach notification laws and the institute of a privacy officer have found their way into the new EU General Data Protection Regulation (GDPR).[10] Part IV analyzes the post-*Schrems* environment by referring to some of the main features of the Privacy Shield[11] and other recent developments that reaffirm the influence of the US model of regulating commercial privacy. Finally, in Part V I offer tentative concluding remarks.

I. Is there "trading up" in data privacy standards?

Ever since David Vogel coined the term "California effect" in 1995,[12] many have asked themselves, including Vogel, to what extent policy convergence toward a more stringent regulatory standard is really possible.[13] Vogel's theory of "a race to the top" (the "California effect") is based on the premise that trade liberalization triggers

[8] Commission Decision (2000/520/EC) 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, O.J. 2000, L 215/7.

[9] Case C-362/14 *Maximillian Schrems v. Data Protection Commissioner*, ECLI:EU:C:2015:650 (6 October 2015).

[10] Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), O.J. 2016, L 119/1.

[11] Commission Implementing Decision (2016/1250) of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield, C/2016/4176, O.J. 2016, L 207.

[12] DAVID VOGEL, TRADING UP CONSUMER AND ENVIRONMENTAL REGULATION IN A GLOBAL ECONOMY (1995).

[13] DAVID VOGEL, THE POLITICS OF PRECAUTION. REGULATING HEALTH, SAFETY, AND ENVIRONMENTAL RISKS IN EUROPE AND THE UNITED STATES, (2012). A detailed examination of whether and to what extent stringency translates into greater privacy protection is beyond the scope of this article; *see* Robert Gelman, *Does Privacy Law Work* in TECHNOLOGY AND PRIVACY: THE NEW LANDSCAPE, (Philip E. Agre & Marc Rotenberg, eds. 1997).

stricter standards developed in jurisdictions with a large market share, which forces private companies in other jurisdictions with weaker standards either to meet the higher standard or to sacrifice a large portion of their exports. There are two key components to this argument.[14] The first is that rules move to a higher level. The second is that this process is driven by export-oriented firms that do not want to have different rules in their home market (since different rules drive up production costs vis-à-vis domestic competitors).

1. "Trading up" in domestic settings

The "trading up" logic, primarily economic, can be reinforced by additional legal considerations and in the case of data privacy, has some explanatory value in domestic settings. In a federation like the U.S., for the sake of consistency and uniformity in the treatment of consumers, but also in order to avoid legal challenges in potential cross-border lawsuits, some major US interstate businesses prefer to voluntarily adopt the higher state standard[15] of data privacy. Such willingness on the part of interstate companies to comply with the higher standard has led to the fast uptake of breach notification rules in the U.S. When a breach of personal information affects residents of US states that do not have a "harm threshold" (establishing that no notification is needed unless there is certain harm for the consumer) as well as residents of states with lower or no such "harm threshold", most businesses provide notice to all affected individuals even though they might not be legally obliged to do so.[16] In the U.S., the willingness of major interstate companies to work with a single standard generally creates opportunities for the federal lawmaker to step in and level up (sector) privacy protections at a cost that is less than what is generally assumed. When the Dormant Commerce Clause[17] or statutory preemption challenges get limited for a period of time, legal spillovers between the US states further facilitate norm diffusion and create windows of opportunity for the federal lawmaker.[18]

---

[14] Many thanks to one of my anonymous reviewers for pressing me on this point.
[15] Bilyana Petkova, *The Safeguards of Privacy Federalism*, 20 Lewis & Clark Law Review 2 (2016).
[16] Id, at 611-612.
[17] In EU law, Art. 34 TFEU can be understood as the functional equivalent of the Dormant Commerce Clause. The Dormant Commerce Clause under US constitutional law prohibits states from passing legislation that discriminates against one state in favor of another or improperly burdens interstate commerce. *See* Pike v. Bruce Church, Inc., 397 U.S. 137, 141-42 (1970).
[18] Bilyana Petkova, The Long-Term Promise of Privacy Federalism, Part I, TECHNOLOGY & MARKETING BLOG (Sept. 1, 2015) http://blog.ericgoldman.org/archives/2015/09/the-long-term-promise-of-privacy-federalism-part-1-guest-blog-post.htm.

Similarly in the EU, albeit most likely not prompted by businesses but by expert networks of administrative civil servants, frontrunner states like Germany and France have demanded the institutionalization of a high degree of data protection throughout Europe.[19] As Gregory Shaffer has shown, since "access to their markets was important, [in the 1990s] these member states exercised considerable leverage in the negotiation of EU liberalization rules. They would have blocked a requirement of free transferability of data without concomitant data privacy protection requirements."[20] And more recently, when during the protracted negotiations for the GDPR that will enter into force in 2018 influential voices in Germany expressed concerns over the possible lowering of standards,[21] the rapporteur for the European Parliament (EP) committed to counter any such attempts.[22]

2. "Trading Up" globally

However, even if structural incentives might be in place, the trading up of consumer protection or standards of fundamental rights is far from automatic. When it comes to data privacy, although companies may initially save on the costs of developing technologically differentiated products or services, they can also decide to adapt to the diversified legal context on a cost-benefit analysis.[23] And policy inertia may prevent the federal lawmaker from acting before a window of opportunity closes. Things become more complicated on an international scale if there is no central authority that can impose legally binding rules: then the interaction of pivotal states

[19] Abraham Newman, *Building Transnational Civil Liberties: Transgovernmental Entrepreneurs and the European Data Privacy Directive*, 62 INTERNATIONAL ORGANIZATION 1 (2008).
[20] Gregory Shaffer, *Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of US Data Privacy Standards*, 25 YALE JOURNAL OF INTERNATIONAL LAW 1, (2000). As Shaffer notes: "…the enactment of the EU General Data Protection Directive of 1995 reflected the high standards of protection already adopted by some of the Member States at the time and was in accordance with then Article 100 (a) (3) of the Treaty Establishing the European Community which mandated that harmonization measures "concerning health, safety, environmental and consumer protection" needed to complete the internal market shall take as a base a "high level of protection…", at 11.
[21] Johannes Masing, *Herausforderungen des Datenschutzes* [Challenges in Data Protection], 2305 NEUE JURISTISCHE WOCHENSCHRIFT 11 (2012).
[22] Jan Philipp Albrecht, *No EU Data Protection Standard Below the Level of 1995*, 1 EUROPEAN DATA PROTECTION LAW REVIEW 3, (2015).
[23] *See Licra et UEJF v. Yahoo! Inc.* and *Yahoo! France T.G.I. Paris*, (2000) and discussion in JACK L. GOLDSMITH, & TIM WU. WHO CONTROLS THE INTERNET? ILLUSIONS OF A BORDERLESS WORLD, (2006). More recently, in enforcing the so-called "right to be forgotten", Google chose not to delist search results on its google.com domain but only on its European domains. Currently, the French Data Protection Authority (CNIL) has demanded that Google delists results on all of its domain names, and Google has appealed the case in court. *See* CNIL, 'CNIL orders Google to apply delisting on all domain names of the search engine', at: www.cnil.fr/en/cnil-orders-google-apply-delisting-all-domain-names-search-engine.

and regional organizations *de facto* sets the tone for global standards. Further, Vogel has focused on transnational businesses but has largely excluded from his analysis other important actors. International relations theorists and political scientists have sought to predict the effects of globalization, pointing out that not just market share but also institutional dynamics matter for the influence of one regulatory model over another.[24] In federated or multilevel systems such as those of the U.S. and the EU, states and localities—through state legislatures, national organizations of state officials, other state-level administrative institutions and the courts—also play a significant role as conduits of international and/or foreign law.[25] A skeptic of the influence exerted by industry interests in the trading up of data privacy standards, Newman has placed particular emphasis on the Trans-european network of experts formed by national Data Protection Authorities (DPAs) that significantly pushed for the institutionalization of a European model of data privacy in the 1990s.[26] More recently in the U.S., intergovernmental actors like the state Attorney Generals are also having an impact in the promotion of the US model of privacy regulation, described in more detail below.[27]

In his later work, Vogel observed the post-1990 continuous rift in risk regulation between Europe and the U.S. when it came to food safety, air pollution and chemical and hazardous substances. For him: "…[w]hile California [and the U.S.] formerly served as a vehicle for the 'export' of more stringent American environmental standards to Europe [i.e. in the 1970s], more recently [they have] become an 'importer' of several more risk-averse and comprehensive regulations from Europe."[28] As a frequent regulatory first-mover on the national level, California is often believed to be a "vehicle for the dissemination of European regulatory policies

[24] Taking transatlantic financing as a case study, scholars of interdependence have argued that where the EU managed to forge a coherent regulatory apparatus, it was able to alter global regulatory dynamics, forcing concessions from the US authorities. "However, this did not mean that EU regulators systematically won, and US regulators lost, reversing the previous power relationship [in which the US took the lead]. Instead, it lead to an ongoing process of accommodation and iterated institutional change between the two regimes." Henry Farrell and Abraham Newman, *Domestic Institutions Beyond the Nation State: Charting the New Interdependence Approach*, 66 WORLD POLITICS 2 (2014) at 342.
[25] See Judith Resnik, *Law's Migration: American Exceptionalism, Silent Dialogues, and Federalism's Multiple Ports of Entry*, 115 YALE LAW JOURNAL 7, (2006) at 1643.
[26] *Supra* note 19.
[27] *Supra* note 15; *See also* Danielle K. Citron, *Privacy Enforcement Pioneers: The Role of State Attorneys General in the Development of Privacy Law,* NOTRE DAME LAW REVIEW (forthcoming 2016).
[28] Vogel, *supra* note 13, at 16.

within the U.S."[29] However, while the potential for a "Brussels effect", or global export of European regulatory standards, might still be there,[30] I argue that instead of spreading a more stringent, precautionary, EU-type of data privacy regulation in the U.S., the EU-US Safe Harbor arrangement on personal data transfers from EU Member States to US companies has so far helped affirm the approach to commercial privacy favored in the U.S. The same is true so far for the successor to Safe Harbor, the Privacy Shield. In the next section I show that, if anything, the US model has been reinforced by market-oriented, nudging strategies of disclosure, such as the breach notification rules first pioneered by California. Further, that model is made workable by adapting the role of a corporate chief privacy officer (CPO), which originated in German law.

II. The Legacy of Safe Harbor

The enactment of the 1995 General Data Protection Directive (the 1995 Directive)[31] by the EU signaled a significant Transatlantic legal and policy divergence. While both the U.S. and the EU recognize the eminence of Fair Information Principles (FIPs) for regulating data privacy, the EU opted for a comprehensive statutory scheme that extended substantive protection to the public and private sphere based on the FIPs. Importantly, the EU Directive mandated each EU Member State to designate one or more independent public authorities that would be responsible for monitoring the application of the national law implementing the Directive on their territory – the DPAs. Instead, in the U.S., various statutes protect different types of data to a differing extent, depending on the sector. Different federal and state agencies have enforcement powers under these statutes.[32] Further, the 1995 Directive (and now the newly enacted GDPR) contains a provision that requires an "adequate" level of data protection to be ensured in non-EU countries that process the data of EU citizens.[33] Since the provision created a domino effect, whereby many

[29] *Id.*
[30] Anu Bradford, *The Brussels Effect*, 107 NORTHWESTERN UNIVERSITY LAW REVIEW 1, (2012).
[31] 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, OJ 1995 L281/31.
[32] For a useful summary, see Paul M. Schwartz, *The Value of Privacy Federalism*, in SOCIAL DIMENSIONS OF PRIVACY: INTERDISCIPLINARY PERSPECTIVES at 324 (Beate Roessler & Dorota Mokrosinska eds. 2015).
[33] *See* Article 25 of the 1995 Directive.

other countries started enacting comprehensive data privacy statutes to meet the EU law criteria, the perception was one of the EU ratcheting up standards worldwide. About thirty states, among them Canada, Israel and other members of the Organization for Economic Cooperation and Development, enacted EU-like statutes.[34] When it became clear that the US did not meet the "adequacy" standard under EU law, US privacy advocates, empowered by the reach of the Directive, hoped that the then Clinton administration would follow suit and would also adopt a baseline privacy statute. However, this did not happen, largely because the U.S. preferred to treat data privacy as a side matter to its e-commerce strategy.[35] Instead, in the face of strong opposition from the European Parliament and some EU Member States' DPA's, the Safe Harbor arrangement came into being.[36]

Enacted after long negotiations between the U.S. and the EU, Safe Harbor ended up being neither an international treaty, nor a bilateral agreement but rather two unilateral acts.[37] The US put forward a condensed version of the Directive's FIPs and fifteen frequently asked questions interpreting the FIPs, which the European Commission then approved in a decision[38] declaring adequacy for the US companies that would voluntarily self-certify with the US Department of Commerce to comply with the Safe Harbor framework. These principles were notice, choice, onward transfer, access, security, data integrity, and enforcement. Clearly, in substance, Safe Harbor was not a copy of the Directive but rather a hybrid solution: only companies

[34] *Supra* note 30.

[35] David Bach & Abraham L. Newman, *The European Regulatory State and Global Public Policy: Micro-Institutions, Macro-Influence*, 14 JOURNAL OF EUROPEAN PUBLIC POLICY 827, 831 (2007), at 833-834. This is not to say that the 1995 Directive did not have any impact on developments in the US. The reports commissioned by the European Commission for examining the level of protection in different sectors in the US might well have helped trigger the enactment of the Health Insurance Portability and Accountability Act of 1996, see Shaffer, *supra* note 20 at 25-26. Similarly, for the enactment of the Children's Online Privacy Protection Act (COPPA) in 1998, CHRIS HOOFNAGLE writes: "It seemed especially laissez faire to Europeans that children were subject to the same regime and roles as adults", FEDERAL TRADE COMMISSION LAW AND POLICY, (2016) at 193.

[36] Henry Farrell shows that during the negotiations of Safe Harbor, Commission officials from Directorate-General Internal Market who perceived the high EU standards as inflexible and wanted to overturn them, managed to find external allies from the U.S. Farell is adamant in emphasizing the constructivist overtone of the negotiations, where neither the EU nor the US fundamentally changed their preferences but benefited from a process of "policy learning". *See Constructing the International Foundations of E-Commerce: The EU-U.S. Safe Harbor Arrangement*, 57 INTERNATIONAL ORGANIZATION 2 (2003).

[37] This arrangement differs from the format adopted for the US-EU PNR agreement, which was signed as an international agreement. *See* Agreement between the United States of America and the European Union on the use and transfer of passenger name records to the United States Department of Homeland Security (PNR agreement), OJ L 0215, 11/08/2012 p. 5 –14. As international agreements, unlike the Privacy Shield, PNRs cane be challenged by the European Parliament. On the EU-Canada PNR, *see* Opinion of Advocate General Mengozzi A-1/15, ECLI:EU:C:2016:656.

[38] *Supra* note 8.

who fell under the jurisdiction of the Federal Trade Commission (FTC) could self-certify, which excluded entire sectors like financial services, insurance industries and air carriers over which the FTC does not have jurisdiction.[39] Most notably, the principle of use limitation[40] enshrined in the 1995 Directive became folded into the Safe Harbor principle of choice;[41] and the FTC's enforcement powers based on Section 5 of the FTC Act, which prohibits unfair or deceptive practices in or affecting commerce were soon interpreted as a fallback option because of the FTC's limited resources and wide-ranging responsibilities in other areas of consumer protection. Thus, instead of being entrusted to an independent data protection authority as postulated by the EU Directive, data privacy under the Safe Harbor scheme was to be enforced mainly through private dispute-resolution mechanisms. Finally, although the EU DPAs were encouraged to communicate violations to the FTC, the US companies that joined the scheme were thought generally immune from the enforcement remit of the EU Member States' protection authorities.[42]

Three major studies have evaluated Safe Harbor's effectiveness, in 2001, 2004 and 2008.[43] The first study came a year after the framework was established and found that only 41 US companies had enrolled and that these demonstrated "an abysmal level of implementation". Safe Harbor did not set any vetting mechanism around who can self-certify. Moreover, companies did not post their privacy policies online (in implementation of the Notice principle) and many of those that did, used corporate privacy policies that were opaque, ambiguous, and often difficult to locate, or they also diluted the substance of the principles; others were still certified after their membership had lapsed. The later studies similarly identified serious gaps in implementation, and found the dispute settlement procedures wanting. In 2010 the Düsseldorfer Kreis, the group of German state data protection authorities, voiced its

[39] Under Section 5 of the FTC Act banks, savings and loan institutions, as well as federal credit unions and air carriers are excluded from FTC jurisdiction, *see* U.S.C. § 45(a)(2).
[40] That principle postulates that data cannot be further processed in ways incompatible with the original purposes for collection.
[41] "Participants must allow individuals to choose whether their personal information will be disclosed to a third party or used for a purpose other than that for which it was collected.", *supra* note 8.
[42] DPAs were able to suspend a particular transfer under a narrow set of circumstances, *see* Art. 3.1b, *id.*
[43] Independent Consultant Study Report for the European Commission, *The Functioning of the US-EU Safe Harbor Privacy Principles* (September 21, 2001); Jan Dhont, Maria Asinari and Yves Poullet. *Safe Harbour Decision Implementation Study*, EUROPEAN COMMISSION, DIRECTORATE GENERAL INTERNAL MARKET AND SERVICES, (April 19, 2004); Chris Connolly, *The US Safe Harbor - Fact or Fiction?*, (Galexia, December 2, 2008). See also WORLD PRIVACY FORUM, *The US Department of Commerce and International Privacy Activities: Indifference and Neglect* (November 22, 2010).

concerns and issued a decision requiring German exporters of data to the US through the Safe Harbor framework to actively check that companies in the US importing data actually comply with the Safe Harbor Principles. To sum up, assessed from an EU law standpoint, the Safe Harbor compromise has far from managed to harmonize the US approach to data privacy with that of the EU.

1. Reinforcing the FTC-model

Although it is difficult to disentangle the causal mechanisms of internal from that of external factors, from a US perspective, the Safe Harbor arrangement has contributed to the development and reinforcement of a properly American, market-driven model of data privacy that allows for policing of privacy violations at the fringes. I will call this the FTC-model after the name of the Federal Trade Commission, which has gradually become the primary enforcement mechanism for commercial privacy in the US.[44] On the one hand, there is no "omnibus" or comprehensive federal statute that protects data privacy in the U.S. and adoption of such is nowhere in sight.[45] On the other hand, in the US constitutional protections remain very constrained.[46] The most significant features of the FTC-model are therefore the framing of privacy as a consumer protection and not as a fundamental rights issue, as well as the preponderance of an agency-based rather than judicial enforcement. Thus, the majority of FTC enforcement actions end in settlements and consent decrees[47] with dubious deterrent power.[48] However, in spite of initial

[44] Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUMBIA LAW REVIEW 3 (2014).
[45] The Obama administration did not manage to pass baseline protection for consumer privacy in 2012 and in 2015. *See, e.g.*, Administration Discussion Draft: Consumer Privacy Bill of Rights Act of 2015, White House, at: https://www.whitehouse.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf, last accessed on September 15, 2016.
[46] Under the Fourth Amendment to the US Constitution, American constitutional law affords to the individual limited privacy protections from the government but not against private actors. As interpreted by the Supreme Court, the Fourth Amendment places no judicial restriction on information shared with a telephone provider, a bank, a search engine, or any other third party to which information was made available, albeit for different purposes. *See* United States v. Miller, 425 U.S. 435, 443 (1976); Smith v. Maryland, 442 U.S. 735, 741–42 (1979).
[47] *Supra* note 44, arguing that companies look to settlement agreements to guide their decisions.
[48] Farhad Manjoo, *Another Tech Company Finds the FTC Looking Over Its Shoulder*, N.Y. Times Bits Blog, May 8, 2014 commenting on a case when the FTC found Google in violation of a consent decree and concluding that "If you do the math, the agency's fine represented about 0 percent of Google's income that year". *See also* DANIEL J. SOLOVE & PAUL M. SCHWARTZ, CONSUMER PRIVACY AND DATA PROTECITON (2015) at 167. Solove & Schwartz did the math in an editors' note, verifying Manjoo's statement.

contestation, Safe Harbor reconfirmed and further expanded the FTC's enforcement jurisdiction in the area of commercial privacy. The agency mobilized its enforcement toolkit, historically directed at false advertising.[49] Further, the number of companies that self-certified had grown exponentially from 41 to over 4000 at the time of invalidation of the Safe Harbor framework in 2015,[50] thus giving the FTC the possibility to monitor businesses' activities based on their privacy policies. Finally, the concerns stemming from the Safe Harbor evaluation reports strengthened the hand of the FTC to pursue high-profile enforcement actions.[51] Arguably, the Agency focuses on "strategic enforcement": instead of pursuing each and every individual complaint, it carefully selects cases that can be structurally significant.

The FTC-model is best captured in Chris Hoofnagle's rich historical analysis of the agency's role in data privacy; market-oriented, this model relies on nudging strategies and does not exclude regulatory guidelines[52] when these compliment economic incentives and self-regulation in the private sector; enforcement is designed based on experiments with stick and carrot strategies to cajole businesses into privacy-friendly strategies. The FTC is, however, often urged to act under Section 5's unfairness prong only if there is "harm" (implying economic damage and thus very difficult to prove in the case of "free" data collection services) or when it can show a specific intent to defraud under the FTC Act's deception prong (again, difficult to use against companies that craft increasingly comprehensive and ambiguous privacy policies).[53] Ultimately, the FTC-model is exclusively dictated by a Law & Economics mindset and considerations of efficiency.

2. Plugs to the FTC model: the role of German and Californian initiatives

Part of Safe Harbor were "verification procedures regarding the attestation and assertions businesses make about their privacy policies, which may include self-

[49] *Supra* note 35, HOOFNAGLE.
[50] *See* Section III.
[51] *In the Matter of Google*, FTC File No. 1023136 (2011); *In the Matter of Facebook*, FTC File No. 0923184 (2011); *In the Matter of MySpace* LLC, FTC File No. 1023058 (2012).
[52] The FTC's rulemaking authority is considered too burdensome as a procedural matter and as a result, almost not used at all. *See supra* note 48, DANIEL J. SOLOVE & PAUL M. SCHWARTZ, at 161. Another feature of the model is the so-called "revolving door phenomenon". It is not uncommon that former FTC-commissioners join industry; most recently, former FTC-Commissioner Julie Brill joined Hogan Lovells Privacy and Cybersecurity practice.
[53] However, as Hoofnagle argues, Section 5 of the FTC Act requires neither of the two tests, *see supra* note 35, at 119-141.

assessments".[54] Since a corporate officer must sign off such self-assessments, the rise of the privacy officer in the corporate culture of many American technology companies became facilitated by Safe Harbor. The US 1974 Privacy Act also makes stipulations for privacy officers in the handling of data by federal agencies covered by the act,[55] but the institutional uptake of this institute by the US private sector does not seem to have been widespread at all in the 1980s. The voluntary spread of the institution of a relatively independent chief privacy officer (CPO) in major US firms now is described as crucial in responding to consumers' expectations for data privacy:[56] the US CPO's responsibilities involve an ongoing engagement with regulators, ranging from pre-product launch to the development of strategic risk management programs to training personnel within the firm.

The data protection officer was originally a creation of the German Data Protection Act of 1977, which required private companies to employ such officers. The importance of the institute rose with the German Federal Data Protection Law of 2001 implementing the 1995 EU Directive.[57] As amply documented by Bamberger and Mulligan, many of the German CPOs made the transition to the necessities of the emerging information society by developing a growing sensitivity to the need for a market of "privacy-enhancing technologies".[58] Further, some of the CPOs believed that economic disincentives for the development of such a market could be overcome through "risk of punishment by the market," reinforced by the exposure of breaches of confidence in the media and the fact that privacy must ultimately find allies with a market interest.[59] Under the shadow of Safe Harbor, the shift to a market logic professed in Germany appealed to US corporate culture. However, the insights from German law were adapted to fit the US context: unlike in Germany, US CPOs are neither mandated by law, nor is there any indication of their independence.

---

[54] Ira S. Rubinstein, *Privacy and Regulatory Innovation: Moving Beyond Voluntary Codes*, I/S A JOURNAL OF LAW AND POLICY FOR THE INFORMATION SOCIETY, (2010) at 391.
[55] Francesca Bignami, *The US Legal System on Data Protection in the Field of Law Enforcement: Safeguards, Rights and Remedies for EU Citizens*, STUDY FOR THE LIBE COMMITTEE OF THE EUROPEAN PARLIAMENT (May 2015), at 13.
[56] KENNETH A. BAMBERGER & DEIRDRE K. MULLIGAN, PRIVACY ON THE GROUND: DRIVING CORPORATE BEHAVIOR IN THE UNITED STATES AND EUROPE, (2015).
[57] *Id* at 208-214. "Indeed, where CPOs were in place within firms, their role was largely seen as low-level, bureaucratic, and inward looking….It would take a suite of new developments, prompted in large part by legislative reform and adjustment taken after the enactment of the [1995] European Data Protection Framework…to catalyze the firm behaviors described by today's leading CPOs."
[58] *Id* at 210.
[59] *Id,*

Further, Silicon Valley has significantly enabled and further complimented the FTC-model. To begin with, in California, state officials streamlined the dynamic created by Safe Harbor that professed to protect data privacy through a voluntary code of conduct. In 2012, California's Attorney General Kamala Harris entered into an agreement with major industry players, such as Google, Microsoft, Apple, Amazon.com, Hewlett-Packard, Research-In-Motion and later Facebook, requiring these companies to adopt privacy policies for their mobile applications (apps) in order to comply with California's Online Privacy Protection Act (CalOPPA) – the first piece of legislation that required online services to adopt privacy policies in the US. [60] The adoption of a privacy policy in mobile applications leapt from 19 percent in 2011 to 72 percent in 2013, while Harris, interpreting broadly CalOPPA, made sure to commence enforcement actions against those companies that had not yet put such policies in place.[61] Other states followed suit, gradually converting the existence of a privacy policy into the norm rather than the exception for doing business online. [62]

This approach is not only consistent with but has also strengthened the FTC's model of an agency that polices the data privacy market for gross market failures. For the rest, consumers are presumed to read and understand well the privacy policies that companies are required to make transparent and visible (Notice) in order for individuals to make up their minds when shopping for products and services on the internet (Choice).[63] In addition, California has released best practice guides on health care providers and cyber security for small-to-medium businesses, and sponsored workshops with stakeholders on how to deal with compliance. As noted by Danielle Citron in a recent study on the role of State Attorneys General in data privacy in the U.S., one of the key ways in which these executive state officials try to influence corporate behavior is through persuasion and informal agreements.[64] In terms of persuasion, some states like California have provided advice on compliance to

[60] CALIFORNIA BUSINESS & PROFESSIONS CODE SECTIONS 22575 (2004).
[61] The FTC has never gone so far as to say that not having a privacy policy is a deceptive or unfair practice. *Supra* note 44, at 599.
[62] Under US federal law, only a few sectors of the economy must have a privacy policy, including financial institutions, healthcare providers, and websites collecting information about children under thirteen, *id*.
[63] Daniel P. O'Brien & Doug Smith, *Privacy in Online Markets: A Welfare Analysis of Demand Rotations*, FTC BUREAU OF ECONOMICS WORKING PAPER No. 323 (2014).
[64] Informal agreements are known as Assurances of Voluntary Compliance or AVCs: companies promise to follow, or go beyond, the applicable legal mandates. For a critical assessment, *see supra note* 27, Danielle K. Citron: "Violators incur no obligations, fines, or penalties unless the attorney general files a lawsuit on the substantive violation and wins. In other words, noncompliance can only be punished if offices file a formal complaint".

companies before the commercial rollout of new technologies and have further established "task forces with business leaders, advocacy groups, and experts in the hopes that participants will reach consensus on data practices". Although the posting of privacy policies gives the FTC and State Attorneys General the possibility to pursue companies for broken promises, it is noteworthy that the content of such privacy policies remains unregulated in the U.S. Recent initiatives however, again in California, might be gradually changing the *status quo*.[65]

Be that as it may, the "Notice and Choice" approach as a whole is widely found wanting: numerous behavioral studies have shown that consumers mistakenly perceive the existence of privacy policies as a sufficient guarantee of compliance with such policies.[66]

However, another significant plug to the FTC-model, again prompted by California, is what became the breach notification statute. The basic logic behind this type of legislation is again market-driven: companies that do not want bad publicity enhance their data security measures in order to avoid leaks that can potentially cause identity theft. This reputational incentive is emphasized in the Californian breach notification bill, which specifically requires that certain major breaches be announced in the press. Although, since California passed the first such statute in 2002 the debate on "who" needs to be notified "when" for "what" is ongoing,[67] key here is that this is a performance metric for the company, so businesses are rewarded by not having to give notice if things are gong well. Forty-seven states, the District of Columbia, and several territories now have some variation of breach notification laws in place. Some of the US states require only that the consumer be notified "without due delay" or "as soon as reasonably practicable" after a breach is detected, whereas a handful set precise time limits: for instance, Ohio, Rhode Island, Vermont and Washington require notification to residents of their states within 45 days of the breach. Other states have inserted provisions requiring that the Attorneys General or other state agencies be notified too, depending on the scale of the breach, and/or in certain states depending on a harm threshold, as noted in the previous section.[68] At first sight,

---

[65] *Id.*

[66] Idris Adjerid, Alessandro Acquisti & Laura Brandimarte, *Sleights of Privacy: Framing, Disclosures, and the Limits of Transparency*, Proceedings of the Symposium on Usable Privacy and Security – ACM (2013).

[67] Paul M. Schwartz & Edward J. Janger, *Notification of Data Security Breaches*, 105 MICHIGAN LAW REVIEW 5 (2007).

[68] Data Breach Charts, *Baker Hostetler* (2015)

breach notifications share an affinity with the EU model of data privacy in that they are mandatory in most states and required by statute; further, a data privacy regulator oversees them and can sometimes impose fines and sanctions. However, the insufficient deterrent effect of the rather symbolic fines imposed by both the FTC and the Attorneys General[69] perpetuates the lack of a market for privacy that could render meaningful choice to the consumer. This approach differs from the EU aspirations of policing data privacy violations through more robust fines, as recently espoused in the GDPR: after 2018, both DPAs and the national courts in the EU will be able to set in place "a system which provides for effective, proportionate and dissuasive penalties"[70] that can amount to up to 4% of the annual worldwide turnover for undertakings.

III. The *Schrems* judgment of the Court of Justice

Even if the Safe Harbor arrangement can be seen as a catalyst for the development of some data privacy protections where none existed before, and as a boost to the US FTC-model, it has justifiably attracted many critics in both the US and the EU over the years. From a European law perspective, it had multiple deficiencies connected with its inability to overcome the problems associated with self-regulatory schemes. However, it was not before the Snowden revelations that the arrangement finally became the subject of reforms in the EU.[71] Even though Snowden exposed that the sharing of data held by private companies for national security purposes under the PRISM program was a blatant violation of Safe Harbor, the renegotiations of the agreement were protracted and still ongoing when the CJEU invalidated the Decision of the Commission authorizing data transfers to the US. For

---

http://www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/Data_Breach_Charts.pdf. See also Dana Lesemann, *Once More unto the Breach: An Analysis of Legal, Technological and Policy Issues Involving Data Breach Notification Statutes*, 4 AKRON INTELLECTUAL PROPERTY JOURNAL 2 (2012).

[69] *See supra* notes 43 and 60.

[70] Art. 83(4) read in conjunction to para. 152 of the Preamble, *supra* note 10.

[71] Communication from the Commission to the European Parliament and the Council 'Rebuilding Trust in EU-US Data Flows' (COM(2013) 846 final, 27 November 2013, and 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 (COM(2013) 847 final, 27 November 2013.

present purposes, I will focus only on some key aspects of this landmark ruling regarding the EU-U.S. interaction.[72]

The main findings of the CJEU in *Schrems*[73] are a continuation of its reasoning in the *Digital Rights Ireland*[74] case where the Court previously invalidated the EU Data Retention Directive. That Directive did not permit acquisition of the content of retained data for law enforcement purposes. In the case of *Digital Rights Ireland*, although the CJEU acknowledged the blurring of the line between the so-called meta (or traffic) and content data, in view of the possibility that both present for profiling individuals, it eventually invalidated the Directive based on a proportionality balancing assessment. In the *Schrems* case however, the Court found that the essence of the right to private life is affected in the case of mass surveillance that gives the government access to the content of intercepted communications.[75] Similarly, the Court found that the essence of the right to effective judicial protection is affected by the lack of any possibility for the individual to pursue legal remedies (in order to have access to personal data relating to him or her, or to obtain the rectification or erasure of such data).[76] When the essence of a fundamental right is affected under EU law,

---

[72] For a detailed assessment, *see* Loïc Azoulai & Marijn Van der Sluis, *Institutionalizing personal data protection in times of global institutional distrust: Schrems Case C-362/14, Maximillian Schrems v. Data Protection Commissioner, joined by Digital Rights Ireland, Judgment of the Court of Justice (Grand Chamber) of 6 October 2015*, *EU:C:2015:650*, (case note), COMMON MARKET LAW REVIEW, forthcoming (2016).

[73] *Supra* note 9.

[74] Case C-293/12 and Case C-594/12*, Digital Rights Ireland Ltd. v Minister for Communications*, Marine and Natural Resources & Kärntner Landesregierung and Others, (2014).

[75] *Supra* note 9, para.94. Although the referring Irish Court and the Advocate General did not reach the same conclusions about the essence of fundamental rights being affected, both largely shared the CJEU's assessment on the incompatibility of the Safe Harbor decision with the EU Charter in what refers to the necessity of massive surveillance and the insufficiency of US oversight mechanisms such as the Foreign Intelligence Surveillance Court (FISC). See Opinion of Advocate General Bot in Case C-362/14 *Maximillian Schrems v. Data Protection Commissioner*, (6 October 2015). Some have interpreted the reforms of the US Foreign Intelligence Surveillance Act as providing for targeted instead of massive surveillance, see Peter Swire, *US Surveillance Law, Safe Harbor, and Reforms Since 2013*, at https://fpf.org/wp-content/uploads/2015/12/Schrems-White-Paper-12-18-2015.pdf (2016). This claim however remains contested; moreover, the very purpose of the US national security reform has been not to eliminate but to shift mass collection of (meta) data from the National Security Agency (NSA) to private phone companies. On FISC, see also Elizabeth Goitein and Faiza Patel, *What Went Wrong with the FISA Court*, BRENNAN CENTER FOR JUSTICE AT NEW YORK UNIVERSITY SCHOOL OF LAW, (2015). "[t]he [FISA] court provides a veneer of judicial oversight for surveillance activities…", at 51.

[76] *Supra* note 9, para. 95. These criteria would appear hard to satisfy under current US law. First, US law is permissive of inter-agency sharing of information when an investigation is deemed to involve a component of national security and law enforcement. Second, there are multiple exceptions from the US Privacy Act of 1974. That Act generally allows individuals rights of access and correction of personal information but only in some governmentally held records. Exceptions include "routine use", as well as general exceptions for law enforcement purposes. Combined with law enforcement's reliance on unregulated under US law practices of commercial data brokers that can package and sell to

this excludes any further balancing tests with countervailing interests.[77] The CJEU also read the provisions of the 1995 Directive – in light of the right to privacy, data protection and effective judicial protection enshrined in the EU Charter – to mean that in the Safe Harbor decision, the Commission has exceeded its competence in circumventing the independent powers conferred on the national DPAs to investigate individual complains.[78] The Court interpreted the standard of adequacy for data exchanges with third countries required by the Directive to mean "essentially equivalent".[79] Remarkably, with the *Schrems* case, the Luxembourg Court also clarified that, even if balancing were possible under the 1995 Directive, economic interests in the free flow of data cannot trump the fundamental right to privacy under the EU Charter.[80] The emphasis on fundamental rights that the Court gave in its judgment contrasts with the pragmatism[81] that the European Commission espoused in the aftermath of the judgment.

1. Reinforcing the EU-model of data privacy

The *Schrems* case was about curtailing mass surveillance but it was actually about boosting commercial privacy on the Internet; in effect, because of the centrality of the purpose limitation FIP and the comprehensive statutory protections for both public

---

the government data obtained from various sources, the gaps in protections for US citizens, and by extension, for Europeans are significant. *Supra* note 55. *See* also Chris J. Hoofnagle, *Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement*, 29 NORTH CAROLINA JOURNAL OF INTERNATIONAL LAW (2003).

[77] "The identification of an intrusion as compromising the essence of privacy meant that there was no need for a proportionality assessment under Article 52 (1.2) of the [EU] Charter.", Martin Scheinin, *The Essence of Privacy and Varying Degrees of Intrusion*, at http://verfassungsblog.de/the-essence-of-privacy-and-varying-degrees-of-intrusion-2/ (2015).

[78] *Supra* note 9, at para. 103.

[79] *Id*, at para. 73.

[80] Bilyana Petkova, *All Things Balanced? Towards an Internal Hierarchy of Values in the EU Legal Order*, 23 MAASTRICHT JOURNAL OF EUROPEAN AND COMPARATIVE LAW 3 (2016). Arguably, the European Commission has been more hesitant in establishing a hierarchy between fundamental rights and economic interests in the data privacy domain, as the CJEU pointed out in the *Schrems* case, at para. 16: "The Commission concluded in point 3.2 that whilst, '[g]iven the weaknesses identified, the current implementation of Safe Harbour cannot be maintained, ... its revocation would adversely affect the interests of member companies in the [European Union] and in the [United States]', *Id*. *See also*, paras. 66-67 where the CJEU took an issue with the fact that private operators might risk data security out of economic considerations.

[81] For a pragmatic interpretation, *see also* Christopher Kuner, "Indeed, many or perhaps even most countries around the world exempt the activities of their intelligence services from their national data protection law and lack an effective oversight structure for surveillance activities, leading one to ask how under the Court's reasoning adequate protection for data transfers can ever exist.", *The Sinking of the Safe Harbor* at http://verfassungsblog.de/the-sinking-of-the-safe-harbor-2/ (2015).

and private uses of data under EU law it was about both. The decision therefore reaffirmed the EU aspirations for data privacy. Especially after the entry into force of a binding EU Charter with the Lisbon Treaty, the EU model places an emphasis on privacy and data protection as fundamental rights that can be limited only with sufficient safeguards;[82] individual redress is central to this approach; and while the independent investigatory powers of the DPAs[83] (strengthened as they are by the possibility of imposing substantial fines to companies),[84] remain an indispensable feature of the EU model, judicial enforcement is at the apex of this approach.[85] The main criticism of this approach is that it might not realistically be sustainable in the age of digitalization and Big Data.

2. Plugs to the EU-model: the role of Californian and German initiatives

To be sure, market-oriented instruments have complimented the constitutionalization of the EU data privacy model too. Some EU Member States followed the lead of California and introduced breach notification requirements at the national level. For example, in Germany, the 2009 amendments to the Federal Act of Data Protection established a requirement on data breach notification.[86] Under the amendments, data controllers must notify data subjects and DPAs of any unauthorized access or unlawful transfer of personal data, if the incident "threatens significant harm" to the rights and protected interests of the data subjects. Since the act does not specifically define "significant harm," it has been interpreted to give companies a certain leeway in determining whether an unauthorized or unlawful activity meets the threshold.[87] In Spain, a royal decree of 2007 postulated that data controllers, as part of

[82] To be sure, interpretation of what constitutes "sufficient safeguards" allows for some play in the joints. *See* Advocate General's Opinion in Joined Cases C-203/15 *Tele2 Sverige AB v. Post-och telestyrelsen and C-698/15 Secretary of State for Home Department v. Tom Watson and Others* (2016), arguing that a general obligation to retain data under national law may be compatible with EU law when such obligation is subject to strict safeguards.
[83] ABRAHAM L. NEWMAN, PROTECTORS OF PRIVACY. REGULATING PERSONAL DATA IN THE GLOBAL ECONOMY (2008), placing particular emphasis on the DPAs in an early political science analysis of the EU and the US models of data privacy regulation.
[84] *Supra* note 70.
[85] *Supra* note 9, at paras. 61-65 where the CJEU reiterated its final authority to review Commission decisions that might endanger individual rights (via the preliminary reference procedure as triggered by national courts).
[86] Bundesdatenschutzgesetz [Federal Data Protection Act], Dec. 20, 1990, BGBl. I at 2954, as amended. § 42a.
[87] *Id.* If harm is detected, notice must be given immediately after the data is secured. Also, the notification requirements only extend to some categories of data such as bank or credit card

their security policies, should draw up a document containing notification procedures, as well as management and response to incidents related to breaches of personal information.[88] Although at first not enshrined in legislation but through a Code of Practice, Ireland also required that data controllers inform the Irish DPA of breaches that the national regulator could then decide whether to disclose to the data subjects.[89]

Ultimately, with the General Data Protection Regulation,[90] the EU took up the insights of Californian law. In the latest version of the Regulation's preamble, a broad definition of damage caused by data breaches is described as a trigger for these provisions.[91] The data controller is supposed to notify the particular data breach to the competent supervisory authority (usually, the DPA) without undue delay and whenever feasible, within 72 hours of the breach unless the controller is able to demonstrate that the breach is unlikely to result in a risk to the rights and freedoms of the individual.[92] The first version of the Regulation put forward in the Commission's proposal suggested a 24-hour period of notification, which was, however, deemed unnecessarily strict and burdensome in the version espoused by the European Parliament (EP). The risk-based approach, clearly prominent in the latest version of the Regulation, requires immediate notification only in the case of potential high risk for the data subject.[93] The standard of "undue delay" is established by taking into account "in particular the nature and gravity of the personal data breach and its consequences and adverse effects for the data subject".[94] Although inspired by US

---

information, "sensitive information," or information that is subject to professional or official confidentiality. *See* Mauricio F. Paez and Jörg Rehder, *Germany Strengthens Data Protection Act, Introduces Data Breach Notification Requirement*, at http://www.jonesday.com/germany-strengthens-data-protection-act-introduces-data-breach-notification-requirement-10-26-2009/#_edn1 (2009).

[88] *Data Breach Notifications in the EU*, European Network and Information Security Agency, at: https://www.enisa.europa.eu/publications/dbn/at_download/fullReport.

[89] *Id*. In 2010, a review group in Ireland suggested that further details be introduced under a statutory Code of Practice.

[90] Mandatory breach notification requirements, albeit limited to security breaches, which occur in the electronic communications sector were introduced already in the e-Privacy Directive, currently under review. *See* 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), 2002 O.J. (L 201) 37, 42.

[91] "A personal data breach may, if not addressed in an adequate and timely manner, result in physical, material or moral damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorized reversal of pseudonymisation, damage to reputation, loss of confidentiality of data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned.", *Supra* note 10, Preamble, para. 85.

[92] *Id,* Art. 33 (detailing what a notification should consist of).

[93] *Id,* Art. 34.1

[94] *Id,* Preamble para. 67.

state law therefore, the European version of breach notification legislation remains substantially different. Unlike in the US, it covers non-material next to material harm, and, unlike in most of the US state bills on breach notifications, it also gives a clear indication on time limits and/or guidance on how to interpret the requirement of notifying without "undue delay".

The latest version of the GDPR also adopts the institution of a Data Protection Officer (DPO) that would play an important role in identifying and assessing data privacy risks.[95] Unlike in German law however, the mandatory appointment of a DPO under the EU Regulation is required for public authorities, but only in limited circumstances, for private companies. Similar to the practice in the US, there is no further nuancing as regards the position of DPOs within the hierarchy of the company, nor about their professional qualifications beyond "expert knowledge of data protection law and practices".[96] Both the Commission's and EP's versions were far more demanding in that respect since the requirements on DPOs in the private sector were more detailed: in the Commission's version, a DPO needed to be employed by any enterprise that has 250 or more employees; and in the EP's version when data processing is carried out, "by a legal person and relates to more than 5000 data subjects in any consecutive 12-month period; or the core activities of the controller or the processor consist of processing special categories of data…, location data or data on children or employees in large scale filing systems."[97]

Ultimately, although resembling the US approach, which relies on companies to voluntarily appoint DPOs, the EU Regulation still significantly differs from it. First, Member States like Germany are allowed to preserve or adopt requirements that go beyond the EU law floor;[98] second, if a company decides to hire a DPO, the Regulation establishes some minimum requirement on independence and exercise of

[95] *Id,* e.g. Art. 35.2 (postulating that the data controller should seek the advice of a data protection officer, where designated, in conducting impact assessments about new technologies).
[96] *Id*, Preamble para. 97 and Art. 37.5.
[97] Compare Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with regard to their Personal Data and on the Free Movement of Such Data, COM (2012) 11 final with European Parliament Legislative Resolution of Mar. 12, 2014 on the Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with regard to their Personal Data and on the Free Movement of Such Data. The final provisions of Art. 37.1b and c require that a DPO is appointed when "…the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale" or when there is large scale processing of special categories of data, *id*.
[98] *Id.*, Art. 37.4

the DPO's tasks with due regard for avoiding conflicts of interest;[99] and third, the Regulation makes it clear that the evaluation of risk is not the sole responsibility of DPOs; instead, risk-based analyses are carried out in consultation with the national DPAs which are supposed to publicize a list of the kind of processing operations that would require companies to conduct impact assessments.[100]

IV. The Privacy Shield

Often, in protecting data privacy against surveillance and for commercial purposes, the two act as interlocking gears. For example, in a high-profile case of Microsoft about the validity of a search warrant that the US government sought to obtain for both content and non-content data stored in Microsoft's data center in Ireland, many of Microsoft's competitors like Apple, Cisco, AT&T and Verizon all filed amici briefs in support of Microsoft opposing the law enforcement measure in support of Microsoft.[101] In another recent controversy, Apple was ordered to help the F.B.I access the mobile phone data of one of the suspects in a shooting in San Bernardino, California, spurring a larger debate about whether companies should create "back doors" for decrypting communication for the needs of law enforcement.[102] Again, the technology industry overwhelmingly aligned with privacy advocates[103] who opposed the measure. Since the American business community is interested in gaining consumer trust, be that in Europe or in the U.S., it can sometimes exercise pressure for raising the data privacy bar against US government surveillance and/or law enforcement.[104] However, unlike in the *Schrems* case, that pressure does

[99] *Id.*, Preamble para. 97 "..[d]ata protection officers, whether or not they are an employee of the controller, should be in a position to perform their duties and tasks in an independent manner" and Art.38.6 "The data protection officer may fulfil other tasks and duties. The controller or processor shall ensure that any such tasks and duties do not result in a conflict of interests."

[100] *Id.*, Preamble paras. 77 and 94; Art. 35.

[101] *Microsoft v. U.S., United States Court of Appeals*, Second Circuit, No. 14-2985 (2016). In July 2016, the Second Circuit unanimously ruled in favor of Microsoft, rejecting the extraterritorial application of the warrant. The case is likely going to be appealed.

[102] Amy Davidson, *The Dangerous All Writs Act Precedent in the Apple Encryption Case,* (2016), at: http://www.newyorker.com/news/amy-davidson/a-dangerous-all-writ-precedent-in-the-apple-case.

[103] Brief of Amicus Curiae Electronic Privacy Information Center (EPC) and Eight Consumer Privacy Organizations, *In the Matter of the Search of an Apple iPhone Seized during the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203,* Case No. CM 16-10 (SP), (2016).

[104] Nick Wingfield & Cecilia Kang, *Microsoft wins appeal on overseas data searches*, at: http://www.nytimes.com/2016/07/15/technology/microsoft-wins-appeal-on-overseas-data-searches.html (2016).

not stem from the law; instead, it is based on market incentives and in certain cases, on libertarian logic concerned with keeping a "small government".

The European Commission recently sought to decouple surveillance from the commercial context of transatlantic data management. On the one hand, it has replaced the Safe Harbor scheme under the so-called Privacy Shield, discussed below. On the other hand, it promoted an Umbrella Agreement supposed to ensure legal remedies for European citizens in the context of data sharing for national security purposes.[105] Despite the inherent differences between the two contexts, an attempt to further legally disentangle the commercial and the surveillance domain in data privacy handling leads to less of a "Brussels effect," not more.

The Court's findings of misuse of personal data for surveillance purposes in *Schrems* could have served as a lever for the European Commission to renegotiate ambitious terms for a Transatlantic deal on commercial exchange of data; perhaps, it could even have empowered US companies to lobby Congress for reforms in the interest of achieving real approximation of standards. Instead, the aftermath of the *Schrems* case saw minor changes to the *status quo*. Adopted on July 12, 2016, the Privacy Shield allows US companies to certify as of August 9, 2016.[106] A detailed analysis of the agreement goes beyond the scope of this article. Suffices to say here that the new hybrid agreement does not substantially differ from its predecessor – the Safe Harbor; the same seven principles are put forward.[107] The emphasis on disclosure reaffirms the FCT-model: under the Privacy Shield companies need to inform individuals of the possibility to access their data as well as to be able to obtain confirmation of any data held about them; in addition, businesses' Notice or privacy policy should also clearly indicate which US agency has investigatory and enforcement powers in case of violations and provide information about the availability of private dispute resolution mechanisms. In sum, the Notice principle bundles together five of the other Privacy Shield principles, namely: notice, choice,

[105] Agreement between the United States of America and the European Union on the Protection of Personal Information Relating to the Prevention, Investigation, Detection and Prosecution of Criminal Offences, at: http://ec.europa.eu/justice/data-protection/files/dp-umbrella-agreement_en.pdf. The agreement only becomes valid upon adoption by the US Congress of a Judicial Redress Act. The limitations of some of the suggested remedies have already been questioned. *See* Franziska Boehm, *A Comparison between US and EU Data Protection Legislation for law enforcement purposes*, STUDY FOR THE LIBE COMMITTEE (2015).

[106] *Supra* note 11. Many thanks to one of my anonymous reviewers for suggesting that I develop this section.

[107] *Id,* at Section 2.1.

access, data integrity and enforcement.[108] In preparation for certification with the agreement, companies are therefore advised to strengthen in particular their privacy policies.[109]

In terms of redress, one novelty of the Privacy Shield is that an individual should obtain response within 45 days after lodging a complaint.[110] However, redress is limited to non-monetary, equitable relief, and is thus giving little incentive to individuals to seek to enforce their rights, notwithstanding the newly introduced possibility for individuals to complain directly to their national DPAs that then need to liaise with the US Department of Commerce and the FTC in offering redress. In the absence of Privacy Shield certification, personal data transfers to the US (and generally, to third countries that do not offer an adequate level of protection) can be based on three alternative legal bases found in article 26 of the 1995 Directive that would remain unchanged under the GDPR. These are: the unambiguous consent of the data subject, Model Contract Clauses (article 26(4)) or Binding Corporate Rules (article 26(2)).[111] Given the difficulty of proving that consent is unambiguously obtained, companies may sometimes decide to choose between the two other methods but are instead strongly advised by the business community to transition to the Privacy Shield.[112] This is because under model contract clauses, it would be much easier for the individual to sue a company. Instead of centering on individual redress, the hope is that the Privacy Shield will further unlock the potential of the FTC-model,[113] prompting the Federal Commission to be more proactive and engage in

[108] Despite the different wording, there is no distinction between the data integrity requirement in Safe Harbor and the Privacy Shield. Whereas the purpose limitation FIP is mentioned in the Privacy Shield, there is no clarification of what could constitute incompatible processing purposes, *id.*

[109] The other two principles – onward transfer and security – also require little adjustment for companies that have previously certified under Safe Harbor. The security principle is flexible in as much as it does not set any concrete encryption standards. Under the onward transfer principle, onward transfers of data are contractually limited to specific purposes. This means that organizations can be held liable for third party processing. Although the principle is reinforced under the Privacy Shield, it still remains "insufficiently framed, especially regarding…scope, the limitation of purpose and the guarantees applying to transfers to Agents." *See* Article 29 Data Protection Working Party, Opinion 01/2016 on the EU-U.S. Privacy Shield Draft Adequacy Decision (April 13, 2016), at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf.

[110] *Supra* note 11, at Section 2.3, para. 44.

[111] *Supra* note 31.

[112] Privacy Shield Webinar by Paul Hastings, August 18, 2016.

[113] However, a lot of uncertainty remains with the new Trump administration that can effectively try to roll back on FTC's powers. *See* Wilmer Cutler Pickering Hale and Dorr LLP, "House Subcommittee Pushes FTC Overhaul, Restricting Investigations and Consent Orders", (2016) at: http://www.lexology.com/library/detail.aspx?g=26dfc6f6-3393-4b2d-b14d-24be3c00862e.

enforcement actions that not only go after companies that have falsely certified under the agreement but also against those that do not comply with their privacy policies.

In any case, the FTC-model and the EU model of judicial enforcement may soon come under tension again, since under the *Schrems* judgment, the national DPAs can submit individual complaints questioning the validity of the Privacy Shield to the EU national courts, which can eventually refer this question to the CJEU. [114] In addition, the Privacy Shield sets in motion an annual review mechanism that allows the European Commission to periodically assess the agreement's functioning and either amend, suspend or repeal it.[115]

Finally, although bulk collection for national security and law enforcement purposes is not terminated in the US, under the Privacy Shield the US government has committed to minimize it whenever possible, as well as to introduce the institute of an ombudsman to deal with complaints under this header. [116] Again, under the supplemental principles of the Privacy Shield, the focus is on disclosure: individuals should be informed of the possibility that access to their personal information can be requested by the US public authorities.

V. Concluding Remarks

In a fully-fledged federation like the U.S., or in a federating entity like the EU, and even when transferred to the international legal order, federal structure is the perennial battleground for change in a political or a legal *status quo*. Federalism illustrates the existence of different points of entry for foreign and international norms and laws. As noted by Judith Resnik, a national movement can create dynamics for the ratification of an international treaty by first seeking to enlist the support of state officials in a federation; even if ratification fails, states and localities can also directly

[114] *Supra* note 9, paras. 64-65. Individual complaints can also come to the DPAs as test cases designed by data privacy activists that can also try to challenge the agreement in direct actions for annulment before the EU General Court.
[115] *Supra* note 11, Section 6.
[116] However, the independence of the suggested institute of an ombudsperson, especially in the light of the *Schrems* judgment, was questioned by 27 privacy and civil liberties organizations, see David Bender, *Advocacy Group Letter Opposes Privacy Shield*, INSIDE PRIVACY (2016), at https://www.insideprivacy.com/international/european-union/advocacy-group-letter-opposes-privacy-shield/.

adopt the provisions of an international treaty or democratically decide to model their constitutions and statutes on foreign law.[117]

In the area of data privacy, the advent of the internet and the un-territoriality of data[118] call for responses in international law. However, before any such responses crystalize,[119] the interaction between key federal and federalizing entities like the U.S. and the EU lays down the groundwork for global data privacy standards. I have demonstrated how, through legal institutes and policy solutions first developed on the state level – breach notification statutes and data privacy officers – the U.S. and the EU are translating "foreign" law and policies to their respective constituencies. Germany and California are acting as main moderators in this continuous dialogue.

The findings of this case study offer a glimpse at the path of globalization in one concrete area of the law. I show how internal constitutional law aspects facilitate policy learning in a globalized context; the validity of the main hypothesis can be tested in other case studies. My findings show that contrary to the conventional view of the EU as a global norm shaper of commercial data privacy law and policy, on many occasions the EU has actually been a norm taker of standards and practices originating in the U.S. The different points of entry that federalism creates complicate the picture; by allowing for disaggregation of the federal entity, federal studies have demonstrated that norm formation often occurs all-the-way-down.[120] This piece adds to the mosaic of federalism by demonstrating how legal ideas also travel *across* the U.S. and the EU constitutive units. In spite of adapting to one another's regulatory insights, the U.S. and the EU contribute to the development of two so far different approaches to commercial data privacy on the Internet. Norm diffusion, often toward

[117] As Judith Resnik has shown, following US withdrawal from the Kyoto Protocol, the United States Conference of Mayors enacted a program that was endorsed, by 2006, by 200 city mayors. The program aimed to "meet or exceed the Kyoto Protocol targets" and is but one example of how states and localities in federations adapt "foreign" norms back home, *supra* note 25; Another example would be if states could directly sign on to international treaties that the federal entity rejects or is unable to join, see Ernest A. Young, *The Puzzling Persistence of Dual Federalism*, in FEDERALISM AND SUBSIDIARITY, (James E. Fleming & Jacob T. Levy, eds. 2014) (criticizing the US foreign relations preemption doctrine as unnecessarily broad). Young's argument becomes especially relevant since the GDPR gives the possibility to the Commission to decide whether separate territories within a third country fulfil the conditions of adequacy for data transfers with the EU, see Art. 43 GDPR.

[118] Daniel Halberstam, *Federalism: Theory, Policy, Law* in THE OXFORD HANDBOOK OF COMPARATIVE CONSTITUTIONAL LAW, (Michel Rosenfeld & András Sajó, eds. 2012); Heather Gerken, *Forward: Federalism All the Way Down*, 124 HARVARD LAW REVIEW 4 (2010).

[119] Stephen Schulhofer, *An International Right to Privacy? Be Careful What You Wish for*, 14 INTERNATIONAL JOURNAL OF CONSTITUTIONAL LAW 238 (2016) (arguing that an international multilateral agreement is actually not desirable as it would weaken privacy protections).

[120] Jennifer Daskal, *The Un-Territoriality of Data,* 125 YALE LAW JOURNAL 326 (2015).

the higher data privacy standard, can be facilitated either by businesses or institutional dynamics but is ultimately more likely to occur in domestic settings. On the international arena, limits to the extraterritorial effect of either EU[121] or US law[122] so far contain the predominance of each model. Thus far, EU data privacy law (at least on the books) continues to place a strong emphasis on fundamental rights and substantive protections based on a comprehensive set of the Fair Information Practice Principles. In contrast, the American experience of state leadership of privacy-friendly initiatives, in combination with the FTC, usually remains confined to treating data privacy not as a constitutional but as a consumer protection issue; the FTC-model consists of legal requirements for disclosure and a narrower, harm-based approach,[123] in line with the American political economy. However, the ongoing interaction of the two models through their interface – previously Safe Harbor, now the Privacy Shield – signifies that if there is a gradual receptivity of a version of the FTC-model by most of the EU DPAs, this may lead to a reaffirmation of the FTC approach on a global scale. Finally, judicial interpretation by the CJEU, possibly of the Privacy Shield and/or on the application of the GDPR to businesses established in the EU, will also impact the future development of international data privacy standards.

[121] Safe Harbor (and one could add, the Privacy Shield) was designed, in fact, to limit trading up effects by allowing companies to use different models in different markets and blunt the extaterritorial effects of EU law. More generally, on the extraterritoriality of EU law, *see* Joanne Scott, *Extraterritoriality and Territorial Extension in EU Law*, 62 AMERICAN JOURNAL OF COMPARATIVE LAW 1 (2014),
[122] *See supra* note 101.
[123] *See also* Chris J. Hoofnagle, *US Regulatory Values and Privacy Consequences: Implications for the European Citizen*, EUROPEAN DATA PROTECTION LAW REVIEW, forthcoming (2016).