UNIVERSITÀ DEGLI STUDI DI TRENTO
Dipartimento di Sociologia
e Ricerca Sociale

The Formation of Transnational Movements?

Sidney Tarrow

DIPARTIMENTO DI SOCIOLOGIA E RICERCA SOCIALE

QUADERNO 4

Università degli Studi di Trento

Dipartimento di Sociologia e Ricerca Sociale

The Formation of Transnational Movements?

Sidney Tarrow

Anno 2017

Collana: Quaderni del Dipartimento di Sociologia e Ricerca Sociale (Online)

Anno: 2017

Segreteria di Redazione:
quaderni.dsrs@unitn.it

ISSN 2465-0161

Università degli Studi di Trento
Dipartimento di Sociologia e Ricerca Sociale
Via Verdi, 26 – 38122 Trento – Italia
Tel.: 0461 281322-281329
Fax: 0461 281458
www.unitn.it/sociologia

The Formation of Transnational Movements?

Sidney Tarrow

Abstract

Scholars and legal practitioners have long found profound differences between the privacy practices of Europe and the United States. This has produced incompatible regimes of regulation, causing serious normative and political issues, which culminated in the passage of the "Safe Harbor" agreement in 2000, which was meant to govern the exchange of commercial information across the Atlantic. But after 9/11, the gaps between Europe and America shrank as both Europe and the United States adopted increasingly intrusive security measures. This convergence came to a head with the Snowden revelations spying in 2013. One effect was the liquidation of "Safe Harbor" by the European Court of Justice; a second was the passage of a new – but still untested – EU General Data Protection Regulation in 2016; but a third was greater interaction and increased collective action on the part of European and American privacy advocates. This convergence may be producing incentives and resources for the formation of a transnational movement to protect privacy. This paper employs a "political opportunity structure" framework to understand how international events between 9/11 and the Snowden revelations securitized the monitoring of commercial and personal electronic communications, increasing inclination of nationally-and-regionally-based privacy advocacy groups to come together.

The 2017 Mauro Rostagno Lectures in Contentious Politics, Department of Sociology and Social Research, University of Trento

Sidney Tarrow, Emeritus Professor of Government and Visiting Professor in the Law School at Cornell University, Università degli Studi di Trento

On October 5, 2015, The Court of Justice of the European Union (CJEU) ruled that the United States' "Safe Harbor" agreement, which had regulated the transfer of data of European origin to the United States since the turn of the century, was invalid. The ruling came when an Austrian privacy advocate, Max Schrems, brought a case to the Irish High Court against Facebook, which maintains its European data center in Ireland, where Internet regulation is lax and taxes are low. Schrems claimed that his privacy had been violated by the U.S. National Security Agency's mass-surveillance programs which had been revealed by whistle-blower Edward Snowden in 2013. The weak and underfunded Irish data protection agency held that it had no authority to monitor what Facebook did with the data it transferred from Europe to the U.S and the Irish High Court referred the dispute to the CJEU, which decided that the Safe Harbor agreement was incompatible with EU laws and conventions. The following year saw the passage of a new and more robust EU data protection directive and efforts to create a new and stronger transatlantic regime of privacy protection.

This story illustrates three things that will guide the analysis that follows:

First, firms like Facebook, and their ability to move data quickly across borders, constitute a "close interaction" between Europe and America.

Second, Europeans have a different concept of privacy than Americans and maintain more robust institutional structures to regulate privacy rights. These differences lie at the heart of "incompatible regimes" of privacy in different European and anglo-saxon countries.

Third, the increasing securitization of the Internet and the Snowden affair that exposed it have been a spur for the "contentious challenges" like the Schrems case. The thesis of this paper is that the growing convergence between European and American privacy practices are laying the groundwork for a transatlantic movement to protect privacy.

On both sides of the Atlantic, privacy advocates have attempted from the beginning of the Internet to achieve a more vigorous protection of personal data. But it was only after the massive growth of surveillance after 9/11 and its exposure by Snowden and others that a truly transnational movement began to form in defense of privacy. Not only that: In recent campaigns, firms and non-state actors have been increasingly found on the same side of the conflict, as in the recent dispute between Apple and the FBI after the San Bernardino terror attack,[1] adding financial and political heft to the marginal power of privacy groups.

This double convergence has created a much more complex network of interaction than a simple "intergovernmental network" (Raustiala 2002) or even than the "governance triangles" described by Kenneth Abbott and Duncan Snidal in their work (2009).[2] I believe it is leading to the formation of a sustained, interactive transnational privacy movement across the Atlantic, defining such a movement as a sustained network of organizations and individuals united across borders against common challenges and proposing common solutions to these challenges. If this is the case, then we can expect American and European privacy activists to eventually merge into a single – perhaps more robust – network of opposition to governments' intrusion on personal communications.

I will begin with some theoretical reflections on the relationship between globalization and complex internationalization before turning to the difficulty of forming a transnational movement on behalf of privacy, and then turn to the changes in the field of privacy since the Snowden revelations of 2013, and finally to the changing role of civil society actors in challenging public policy.

I. GLOBALIZATION AND ITS CORRELATES

During the 1990s, globalization and the information revolution seemed to many scholars and publicists to be an inexorable force reducing the power and sovereignty of states. This work came on the heels of a generation of research on interdependence, triggered by Robert Keohane's and Joseph Nye's book, *Power and Interdependence*, published ahead of its time ([1979] 2001). Some scholars and many publicists saw globalization as synonymous with interdependence, but the two phenomena are analytically separable. As Michael Zürn writes,

> The notion of globalization differs from that of interdependence in that it refers to qualitatively different conditions. Whereas the notion of interdependence refers to a growing sensitivity and vulnerability between separate units, globalization refers to the merging of units (2002:235).

This is a crucial difference, for while states foster interdependence through treaties, contracts, and the formation of intergovernmental networks, they have naturally resisted "the merging of units."

Some realists – like former President Nicolas Sarkozy of France – think states are still the only important actors in governing economic communications. With classical Gallic *suffisance,* Sarkozy told an e-G8 summit that "Nobody should forget that governments are the only legitimate representatives of the will of the people in our democracies. To forget this is to risk democratic chaos and anarchy" (quoted in Mansell 2012: 148). On the opposite extreme, advocates argue that the Internet is "ungovernable" because of its global reach. As John Perry Barlow put it;

> Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather"[3]

Between these polar positions, many observers see globalization leading to the growth of consensus-based quasi-institutions by diverse groups of government, private sector, and civil society stakeholders. In this spirit, Kal Raustiala sees globalization producing "transgovernmental regulatory cooperation", both through classical internationalist mechanisms like treaties and through informal networks (2002:14). "Champions of transgovernmentalism," he writes,

> agree that the information revolution and globalization are changing world politics and international law. But they believe the state is resilient and will remain the centerpiece of the international system. The state increasingly exercises its power, however, in a disaggregated, flexible fashion that echoes the complexity of the world around it (Raustiala 2002:19).

Kenneth Abbott and Duncan Snidal find that non-state actors are central to this "disaggregated, flexible" structure. In the 39 transnational regulatory schemes they studied in what they called "the governance triangle," they found that NGOs were principal actors in seven of them and were active participants in thirteen others. Indeed, NGOs took the lead in establishing many of these schemes

and stimulated many others (2009: 50; 56).[4] Henry Farrell and Abraham Newman go further: they have developed a framework they call "the new politics of interdependence," which they characterize as the construction of "cross-national layers" of policy agreements which have the potential to transform domestic institutions and, in turn, transform global rules (2014).

Where do social movements fit within these frameworks? As Milton Mueller and his collaborators write, in transnational policy networks "contentious political actors of *all* types cluster around authoritative institutions seeking influence" (Mueller et al., 2007: 269). This would produce a structure that is close to what I called, in *The New Transnational Activism,* "complex internationalization." In such a structure, international institutions serve as a kind of "coral reef" in whose interstices non-state actors advocate, meet others like themselves from other venues, and form transnational coalitions.[5] Enthusiasts for "globalization from below" hoped that advocates would quickly organize across borders around the international frameworks that states and international institutions were creating to regulate global exchanges.

But transnational movements are hard to create and even more difficult to sustain. The national social movements at their base are primarily oriented to domestic structures of opportunity and are inhibited by cultural and political differences from sustained interaction at the transnational level. In addition, most of them depend on intermittent events to bring them together, like the meetings of the major international financial institutions. Even in Europe – where internationalization is most advanced – most movements continue to be oriented to domestic issues, mobilize against national targets, and come together only when European and international institutions provide them with occasions to do so.

These inhibitions on the formation of transnational movements are particularly great when it comes to the defense of privacy. When Colin Bennett wrote his landmark book, *The Privacy Advocates* a decade ago, there was not yet a sustained and unified transnational privacy movement (Bennett 2008). Tech firms like Apple, Facebook, and Google had gained footholds in both Europe and America, but most of the advocacy groups active in the general area of privacy were lodged on one side or another of the Atlantic. Bennett found that most of the organizations that combine their efforts around transnational privacy issues were not *privacy-centered*, but were only *privacy-explicit* or *privacy-marginal* (Bennett 2011). When the Snowden revelations burst upon the world in 2013, these advocates had not – at least not yet -- formed a sustained transnational social movement and the different privacy regimes in Europe and America impeded their collective action.[6] Privacy is "a thousand miles wide and an inch deep," quipped Bennett, noting the "risk that an ideologically thin network is more amenable to temporary campaigns rather than long-term strategic partnerships" (2008: 193). Rather than building a cumulative movement, privacy advocates went from episode to episode.

The existence of official data protection authorities in Europe and their absence in the United States makes collaboration across the Atlantic difficult for advocacy groups. Bennett argues that "[t]he growth of official data protection authorities can have the effect of crowding out the policy space for nongovernmental advocacy groups" (2008: 35). For example, in Germany, an early organization, the *Deutsche Vereinigung für Datenschutz*, "declined in importance as the network of German data commissioners… became institutionalized" (ibid.). In the United States, in contrast,

the absence of public authorities with responsibilities for privacy has left more policy space for civil society groups to develop.

This difference is reinforced by the greater charitable giving in the United States. Groups like the ACLU and the Electronic Frontier Foundation (EFF) enjoy far more foundation funding than their European counterparts, as well as getting more support from private citizens and corporations. For example, in its 2015 annual report, EFF listed its support from foundations as $998,659, from individuals as $4.7 million, and from individuals donating through foundations at $2.2 million. In contrast, in its 2014-15 financial statement, Privacy International, the London-based international privacy organization, lists total charitable funding as £1,343 million and individual donations as £137 thousand.[7]

But the biggest differences appear to revolve around the greater power of organized business in the United States than in Europe. For example, the first draft of the US Privacy Act had a provision for a privacy protection commission that would have resembled what eventually appeared in Europe, but it was removed after hard lobbying by business interests. In her exhaustive study of congressional committee hearings on privacy, Regan found that debates that began around the value of personal privacy almost inevitably ended up aimed at other policy priorities and supported those whose interests would be curtailed by privacy protections (1995: 210).

Securitization

What has been the effect of the increasing securitization of global exchange since 9/11? Studies of post 9/11 security policy have focused on the effects of what Kim Lane Scheppele calls "the international state of emergency" on civil liberties and on speech, both online and offline (Scheppele 2004). The more surveillance, the argument holds, the greater the threat of repression, and thus the higher the obstacles to contentious political action. Scholars like Rosa Brooks have found a disturbing "trickle-down effect" of post 9/11 national security policies (Brooks 2014). Even policy areas distant from national security have experienced a "spillover effect" from 9/11 to the militarization of the police, the diffusion of the state secrets doctrine into civil law, and the securitization of immigration practices.

But when word began to leak out that American security agencies were tapping into the Internet to troll through millions of email messages and web browsing, and as Europe began to adopt ever more intrusive surveillance techniques, the situation changed. As the extent of American – and, to a lesser extent, European – practices of electronic surveillance became known, the resulting threat became part of a transnational opportunity structure with two major axes: Europe's increasingly assertive court system and a network of transatlantic advocates who were increasingly aware of each other's activities and began to operate in tandem against threats to privacy. In the next part of this paper, I will summarize the major differences between the U.S. and the E.U. privacy regimes that existed at the turn of the century and which left holes in the "Safe Harbor" agreement.

II. TWO PRIVACY PROTECTION REGIMES

Privacy is an abstract and a much-disputed term. In his landmark study, *Privacy and Freedom,* Alan Westin argued that "Few values so fundamental to society as privacy have been left so undefined in social theory or have been the subject of such vague and confused writing by social scientists" (1967: 7). Priscilla Regan divides privacy concerns into three sectors: information privacy, which "involves questions about the use of personal information collected by organizations;" communication privacy –which "involves questions about who can legitimately intercept discussions between two parties"; and psychological privacy issues, which involves "questions about the degree and type of probing utilized in determining individuals' thoughts and attitudes" (1995: 5).The most capacious definition I have found comes from Steven Shiffrin, who writes that "privacy refers to a zone of intimacy in which human beings can live flourishing lives without the intrusion and scrutiny of others" (2016:13).

When we turn to how the value of privacy is conceived in different parts of the world, we find a fundamental difference: In countries with written constitutions, like the United States, privacy is seen as a civil liberty, with reference to specific national constitutional guarantees, such as the Bill of Rights. But elsewhere, "claims about privacy as a 'human right' tend to be made in more universalistic terms and derived from certain inherent human rights by virtue of our humanity, rather than our citizenship" (Bennett 2011:130). As Abraham Newman notes, the American and EU systems are extreme cases on a continuum of regulatory systems (2008a:23; Whitman 2004).

The simplest way to characterize these two regimes is to say, with Orla Lynskey, that the European model is an "omnibus" regime in which data protection rules are applied to both public and private actors in a sector-neutral way, and are enforced by independent supervisory authorities. In contrast, the American model is a "sectoral regime with different legal frameworks applicable to the public and private sector, in which the private sector "is governed by a mixture of ad hoc legislative initiatives, industry self-regulation, and market forces" (Lynskey 2014:15-17).[8] This creates a different opportunity structure for both states and civil society groups in Europe and America.

The EU Data Protection Regime

The most distinctive feature of the European regime is its comprehensive nature and the fact that it is buttressed by a spectrum of national authorities and, since the passage of the Data Protection Directive in 1995, by a European data protection supervisor (Long and Pang Quek 2002). The origins of the system were national groups of privacy activists and lawyers who "formed the core of domestic policy networks involved in developing legislation" (Newman 2008a:108). "Coming to prominence in the wake of the peace and student movements of the 1960s," writes Abraham Newman, "these activists soon turned their attention to the more general societal implications of computer technology" (ibid.). Out of these efforts grew data protection authorities in a number of EU member states, which were delegated authority to regulate the use of personal information in their countries. They were movement activists within the state, much like the "state feminists" who helped animate the women's movement in the United States (Banaszek 2009).

A key turning point came in 1989, when the French national data privacy authority (CNIL), threatened to block data transfers between FIAT's corporate offices in Italy and France because it held that Italy lacked adequate regulations to guard the privacy of French data (Newman 2008a:114). A second was the controversy surrounding the creation of the Schengen agreement to permit the mutual policing of national borders, when the French, German and Luxembourg data privacy authorities argued that sharing police information with Belgium – which then had a weak privacy regime – would violate their regulations (ibid., p. 115).

As the boundaries of individual European economies began to erode with the approach of the single market, these national agencies began to work together to play a critical role in promoting data privacy at the European level (Newman 2008a:11). As Newman writes,

> These agencies had a dual motivation: the belief that all Europeans deserved basic privacy protection and a desire to protect their regulatory authority from assault during the creation of the internal market….Fearing that firms would relocate their data processing operations to countries without data privacy rules, regulators in countries such as France and Germany formed transgovernmental networks to lobby for European action (ibid.).

The EU's Privacy Directive that resulted from this convergence "forced reforms that strengthened privacy protection and civil liberties within the member states and created a structured system of oversight for the entire region" (ibid).[9] The pre-existing national authorities remained in place to monitor business practices in their countries and consider complaints from citizens who felt their rights had been abused but their interests and concerns were represented at the European level by what was called the "Article 29 Working Party" – an institutional interest group that serves as an advisory body to the EU's Data Protection Supervisor and issues opinions on changes in data protection practices.

The passage of the European Privacy Directive was slow, halting and left open numerous veto points at which regulation-shy European and American business groups aimed their critiques. As Priscilla Regan wrote of the capacity of European and American business to influence the shape of the Privacy Directive; "There are three primary reasons why the European-based strategy was successful:" The timing of the directive, the complexity of the process, and its length [which] provided business associations with the opportunity to organize on both sides of the Atlantic" (Regan 1999: 200). These drawn-out processes led to ambiguities in the wording of the Directive, to confusion about its implementation, and to conflicts between the strict regime of data in Europe and different regulatory regimes in other parts of the world. But because national data authorities had the leverage to obstruct the free flow of data across national boundaries, they were able to bring about a shift in the scale of data protection from the national to the European level and the sheer market power of the European economies helped convince Europe's trading partners to adopt similar data privacy regulations (Newman 2008a:116).

But market power was not limited to Europe. The most persistent conflicts arose between the EU – with its developing regional data protection regime -- and the United States, where no such institutions existed and where the lobbying power of private interests heavily outweighed the norm of privacy (Regan 1995). The market power of American firms and the strength of market-oriented ideology led the United States government to resist acceptance of European norms for the

protection of privacy and to propose a stopgap measure to allow transatlantic exchange of data to grow – Safe Harbor.

The US Data Protection Regime

If the European data protection regime is an "omnibus" one, the American one is sectoral, confusing, and market-oriented. It is sectoral because it is composed of different regimes of privacy protection for different parts of the economy; it is confusing because it is fragmented, ad hoc, and targeted to cover specific sectors and concerns; and it is market-oriented because "Americans tend to be more trusting of the private sector and the free market to protect personal privacy – fearing more the invasion of privacy from the state and not the market" (Long and Pang Quek 2002:331).

American policy-makers were not immune to the need for privacy protection. Between 1965 and 1988, Priscilla Regan counted 71 congressional hearings in the field of information privacy and 70 on communications privacy (1995: Appendix A and B).[10] The Electronic Communications Privacy Act of and the Stored Communications Act of 1986 imposed restraints on the government's access to information,[11] but Congress created no central institution to process claims that privacy was being abused.[12] In the meantime, in the growing realm of the Internet, where private firms began to retain and market the information of individual users, citizens' personal data remained unprotected.[13]

Instead, the Office of Management and Budget (OMB) and the Federal Trade Commission (FTC) and the Federal Communications Commission (FCC) were tasked with enforcing specific privacy laws, while entire sectors of the economy depended on the "self-regulation" of private actors. "Under this form of private-public regulation, publicly announced corporate policies and industry codes of conduct are backed by the FTC and state-level enforcement [but only] in response to private civil actions for damages or injunction relief" (Long and Pang Quek 2002: 333).

There is no simple reason for *why* the American privacy regime became so fragmented, dispersed, and ineffective, but we can trace *how* it happened: it was the result of a policy-making process in which abstract principles clashed with the interplay of interests, and in which the most well-placed interests "quietly" prevailed (Culpepper 2011). Regan's authoritative work shows the difficulty of getting effective privacy legislation through Congress, the unwillingness of the courts to enter this policy area, and the ultimate dominance of private interests over the ideal of privacy (Regan 1995). This was the market-oriented regime with which the United States, which was emerging as the most powerful actor in digital communications, faced an international system that was increasingly moving in a "European" direction, leading to the Safe Harbor Agreement in 2000.

III. FROM SAFE HARBOR TO PRIVACY SHIELD: TRYING TO BRIDGE THE GAP

The European Union's 1995 Data Protection Directive was not the first international instrument intended to monitor and control the unregulated diffusion of private data. Two early instruments from the OECD and the Council of Europe "were designed to harmonize data protection policy and force those without appropriate safeguards to pass equivalent legislation" (Bennett and Grant 1999: 12; also see Rotenberg and Jacobs 2013). But because neither instrument created

enforcement mechanisms, neither was particularly successful. It was largely in response to these failures and to the growth of commercial exchange in the 1990s that the European Union had negotiated the European Data Protection Directive between 1990 and 1995. The Safe Harbor agreement was a side agreement which relaxed the strict data protection regulations required of Europe's other trading partners.

Safe Harbor, which followed by five years the passage of the directive, fit loosely within the boundaries of Abbott and Snidal's "governance triangle" – but it failed to reconcile the deep differences between the American and European systems of data protection:

First, it was negotiated between an international institution – the European Commission – and a department of a national state – the Department of Commerce. The asymmetrical nature of this exchange gave the agreement an unstable character from the beginning.

Second, it depended for its implementation on the firms that signed up for it, which were responsible for self-monitoring the protection of the data sent to the United States by their opposite numbers in Europe.[14]

Third, and most important, the discussions were largely couched in political-economic terms (Long and Peng Quek 2002), and had nothing to say about the biggest thorn in its side after 2001: the growing interest of America's intelligence agencies in trolling through masses of personal data for evidence of terrorist activity. With the passage of the US Patriot Act in early 2002,[15] "the United States," as Henry Farrell and Abraham Newman write in a spirited *Foreign Affairs* article, "began to exploit interdependence, deliberately using its economic power as an instrument of national security" (2016:125).

We can best understand the vulnerability of the agreement to the national security spillover if we recall the basic distinction in Keohane and Nye's work between matters of national security and matters of less import. In *Power and Interdependence,* Keohane and Nye made three cardinal assumptions:

- *first,* where questions of national security and state sovereignty are concerned, the center of gravity of policy-making gravitates to the highest levels of the executive;
- *second,* when multiple channels connect societies below the inter-state level, informal ties develop between governmental agencies below the state-to-state level;
- *third,* when there are no clear or consistent hierarchies of military and nonmilitary issues, a plurality of domestic actors is legitimized to participate in world politics.

But in times of international crisis, sectors of activity that nominally lie outside of the security sector can be "securitized". While it continued to be managed by domestic actors below the highest levels of the state, Safe Harbor was subversively securitized. Given the changing balance of commercial exchange and security in European-American relations after 2001, it was likely that the agreement would come a cropper.

From Snowden to Schrems

That likelihood became virtually inevitable after 2013, when the Snowden revelations made it all but certain that the National Security Agency had been amassing the data of Europeans in its almost obsessive drive to "collect everything."[16] Already in 2013, an Irish NGO – Digital Rights Ireland

–contested the Irish government's data retention law in the CJEU and the court declared the Directive invalid (Lynskey 2014: 163-165). Even before the Schrems decision came down, the Article 29 Working Party "had gone so far as to declare that the implementation of the Data Retention Directive was unlawful" (Reidenberg 2014:597).

The Schrems case made clear that what had been negotiated as a commercial agreement was being undermined by security methods. In his filing before the Court, Schrems argued that, "in the light of the revelations made in 2013 by Edward Snowden concerning the activities of the United States intelligence services (in particular the National Security Agency, the NSA), the law and practice of the United States do not offer sufficient protection against surveillance by the public authorities of the data transferred to that country."[17]

The Court agreed, maintaining that "The United States safe harbour scheme …enables interference, by United States public authorities, with the fundamental rights of persons."[18] The Court held that "legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life" and "compromises the essence of the fundamental right to effective judicial protection, the existence of such a possibility being inherent in the existence of the rule of law."[19]

The Court could not have known if Schrems' personal account was being hacked by the NSA, but there was plenty of evidence that the United States government was surveilling communications between foreigners and Americans. In 2007, Congress had passed the Protect America Act (PAA), which gave the NSA the power "to monitor all the phone calls or emails it wanted to, foreign or domestic," regularizing a practice that had gone on *sub rosa* since soon after 9/11 (Greenberg 2016:148). A year later, the provisions of the law were incorporated into the FISA Amendments Act (FAA), "a more comprehensive modification of the law" (ibid., p. 150).[20] Tested by a case brought by YAHOO! in June, 2008, the FISA Review Court held that companies had turn over their computer records of Internet traffic to the NSA when required to do so (ibid, p. 167), a decision that legitimized the PRISM surveillance program that was later exposed by Snowden.[21]

At a stroke, the European Court ended Safe Harbor and led to the negotiation of a successor in 2016, "Privacy Shield." After intense and arduous negotiations, the text of the new agreement was released in February, 2016, and went into force on August 1st of that year. Secretary of Commerce Penny Pritzger called the agreement a tremendous victory for privacy for individuals, and businesses on both sides of the Atlantic", one that would "help grow the digital economy by ensuring that thousands of European and American businesses and millions of individuals can continue to access services online." But neither privacy advocates nor the EU's Article 29 Working Group wree convinced. One immediate impact was that the Irish Data Protection Commission filed a second suit ("Schrems II") in the Irish High Court to determine whether the "standard contractual clauses" used by Facebook to authorize the transfer of personal data to the U.S. post-Safe Harbor provide adequate protection for E.U. citizens. That case is still under consideration.

Securitization Crosses the Atlantic

Even before 9/11, European governments were under pressure to respond to the terrorist threat with enhanced surveillance regimes too. Soon after 9/11, the growing threat led American and European security experts to create a High Level Contact Group to lay the groundwork for a more formal EU-US deal on privacy, which "over time tilted the EU's balance away from what they saw as excessive privacy concerns and towards national security" (Farrell and Newman 2014: 11). The final agreement "remade the regulatory bargain over security and privacy within the EU" (pp. 13-14).

But it would be wrong to see this shift in emphasis from rights to security in Europe only as the result of American pressure. Although there was an initial disagreement within the EU after 9/11 between civil rights-oriented officials and security officials, the latter eventually came to dominate negotiations, passing a series of new laws and engaging in practices that compromised the aspirations of the European Charter of Rights. Europeans have tightened the privacy regime that was installed in 1995 in at least four ways:

- First, In 2006, the EU adopted a new Data Retention Directive[22] which applied to traffic and location data in order to make it available to law enforcement (Lynskey 2014:161-3. By requiring service providers to store data and maintain a surveillance database for law enforcement, the directive transformed the private sector into agents of law enforcement. In effect, writes Joel Reidenberg, "Europe has turned online intermediaries into sheriffs" (2014, p. 601).
- Second, European intelligence services are afforded privileged rights of access to data. In the UK, France, Sweden and the Netherlands, information can be intercepted without a court order and warrantless wiretapping seems to be much more widespread than in the United States (ibid., 594).
- Third, there has been a gradual process of what Colin Bennett and Charles Raab call "function creep." This is the tendency to find new uses and applications for retained data unrelated to the purpose for which the data was originally collected (Bennett and Raab 2003: 139; Kreuder-Sonnen 2016: ch. 3).
- Fourth, individual countries have adopted increasingly stringent controls on information. Both the French DGSE and the British GCHQ have been collecting international email traffic of Google and Yahoo and – in the latter case – "capturing all data entering or existing the UK through fiber-optic cables" (Ibid., 2014: 592). The greatest convergence can be seen in the UK's recent adoption of an "Investigatory Powers Act" which gives the British government the legal authority to carry out mass surveillance.[23]

With each new terrorist outrage, European public opinion became increasingly unconcerned with Europe's historical commitment to privacy. In Brussels, objections to increased surveillance from national data protection authorities and from Article 29 Working Party fell on deaf ears.[24] According to Joel Reidenberg, Europe has become a "data surveillance state" in the same sense as the United States. Reidenberg fears that "government data surveillance law in Europe and the United States has reached a turning point for the future of information privacy online" (2014, p. 583).[25] Even if his fears are exaggerated, the question raised by this growing convergence is this:

will it lead to a positive or negative effect on the potential formation of a trans-Atlantic privacy movement?

IV. AN EMERGING TRANS-ATLANTIC PRIVACY MOVEMENT?

Until recently, European and American groups were slow to organize across the Atlantic to contest restrictions on privacy. Even as dedicated an activist as Simon Davies of Privacy International admitted as much when he wrote that the privacy movement faces its greatest challenge in the international realm: "The idea "Think global, act local' has become a *modus operandi* for the privacy community," he wrote in 1999,

> but it is an approach that may ultimately undermine privacy reform. While international business possesses the market power and the global incentive to mobilize against the regulation of data diffusion at the international level, most activists are occupied fighting fires on domestic turf" (Davies 1999:259).

That this situation is changing can be seen from a comparison of conflicts over encryption between the early 1990s and the current period.

From Clipper Chip to "Security For All"

In 1993, the Clinton Administration announced that it would make available a new cryptographic device, the "Clipper Chip," which was purported to protect private communications from hacking while allowing the government to obtain the "keys" to the encryption upon presentation of a legal authorization. The underlying algorithm for Clipper Chip, what was known as "Skipjack," had been developed by the NSA. Skipjack was classified as secret on national security grounds, preventing independent evaluation of its capacity to ensure the encryption of private messages.

In August 1994, Matt Blaze, a cryptography expert working at Bell Laboratories, published a paper, "Protocol Failure in the Escrowed Encryption Standard," which exposed fatal flaws in Clipper Chip and Skipjack.[26] Sensing the danger of the government's capacity to use the system to infiltrate private communications, a coalition of privacy groups, including the Electronic Privacy Information Center (EPIC) the EFF, sent an electronic petition – something new at the time – to the U.S. government, opposing Clipper Chip. Eventually signed by over 50,000 people, the petition, added to Blaze's paper, led the government to back down from the scheme.[27]This was one of the first episodes of collective resistance to threats of government intrusion on private communications and it had a dramatic effect on the tech sector. First, it gave rise to a vigorous online discussion among tech experts, but more important, it brought together a coalition of privacy groups and tech firms.[28] Observe, however, that it took place *only* within the United States and that all of the groups signing the letter denouncing the dangers of Clipper Chip were American.[29]

Now fast forward to January 2016, when a group of 200 activists, digital rights experts, companies and organizations called on the Obama administration and other world leaders to oppose any "back doors" to encryption. It circulated a petition, "Security for All," which read, in part,

> We urge you to protect the security of your citizens, your economy and your government by supporting the development and use of secure communications tools and technologies, rejecting policies that would prevent or undermine the use of strong encryption, and urging other leaders to do the same.[30]

Like the 1994 petition, the signatories included American stalwarts like the American Civil Liberties Union, EPIC, and the EFF. But more important, the letter was organized by a transnational coalition, "Access Now," which did not exist in 1994, and included signatories from forty different countries. Access Now is a coalition that has organized two "Crypto-Summits", the first in Washington DC in July 2015, and the second in Silicon Valley in March 2016. It organizes an annual conference, what it calls "Rights.con".[31]Table 1 shows how the debate over encryption and its challenges has become more global, and the role of transnational NGOs in the mobilization of a transnational coalition to protect it from state interference.

Table 1: Organizations That Signed the "Security For All" letter, by Origin

Geographic location	*Number of organizations*	*Percentage*
Europe	61	33%
North America	56	30%
Asia	25	14%
Central and South America	21	11%
Africa	5	3%
Oceania	4	2%
International*	11	6%
NA**	2	1%
Total	185	100%

Source: "An Open Letter to the Leaders of the World's Governments Signed by Organizations, Companies, and Individuals, January 10, 2016. https://www.securetheinternet.org/

Notes: * Organizations were coded as "international" when they were either located on more than one continent of were found to have member organizations in more than one country and a decentralized governance structure. ** Organizations were coded "NA" when no geographic information could be found for them.

Access Now is not the only transnational group that has been carrying the banner of support for digital rights across borders. For example, in the field of intellectual property rights, in the 1990s American policy was essentially written by "rights holders" – big companies that claimed to own the materials they produced. But by 2012, Susan Sell writes, "a transnational coalition of engineers, academics, hackers, technology companies, bloggers, consumers, activists and Internet users defeated the rights holders" (Sell 2013: 67). As Sell concludes: "The ability of Insider/Outsider

coalitions comprised of 'rooted cosmopolitans' to shift from lower…to higher (for example, bilateral, plurilateral, multilateral, transnational levels and back again for coordinating protest is a powerful political resource (ibid., p. 80).

In 2011, Colin Bennett – who was originally skeptical of the existence of a transnational privacy movement (see above) – began to sense the possibility of an integrated privacy network emerging. "The environment," he wrote

> now involves a complicated network of private and public sector actors who engage in overlapping domestic and international regimes…. Some advocates wish to build a more coherent transnational activist network, which not only uses official means of advocacy and redress, but also engages in a broader "politics of privacy", publicly exposing overly intrusive practices and even "outing" the organizations that are responsible for them (Bennett 2011:126-127).

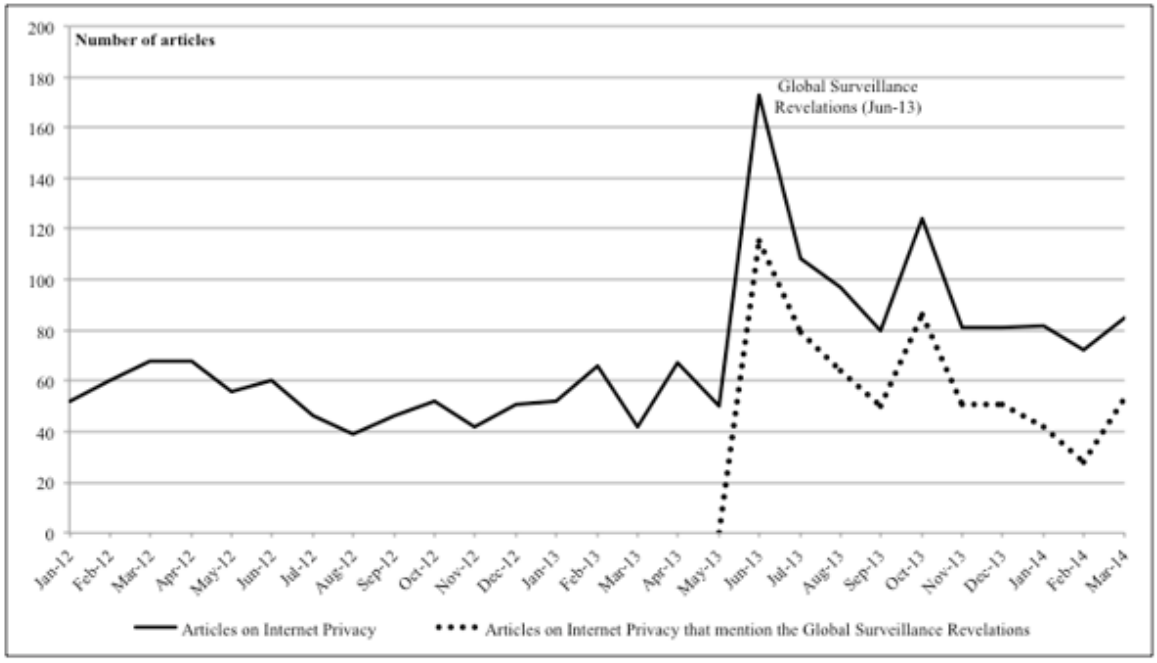
It was the growing evidence of the extent of the US's – and, to a lesser extent, the UK's -- scooping up enormous amounts of private digital communication that led to growing concern with the dangers of state surveillance and with growing evidence of the creation of a sustained transnational movement. This takes us to "the Snowden effect."

Enter Snowden

Edward Snowden was not a traditional social movement activist; on the contrary, when he decided to reveal his findings in 2013, he was a paid contractor of the NSA with no connection to any social movement organization. But in the Internet age, the very meaning of social movements has begun to shift, from organizations that use communications media as a mechanism to publicize their claims to small groups of activists for whom communication is their fundamental function (Bennett and Segerberg 2012). Snowden's exploits, using his own digital skills to expose the NSA's secret surveillance programs, may simply be the ultimate extension of this trend.

A young scholar, Agustin Rossi, has done the most systematic work demonstrating the increase of interest in surveillance during and after the Snowden revelations. Using print editions of the main newspapers in the largest EU members – France, Germany, Italy, Spain, and the UK, Rossi carried out a search for news and opinion pieces on Internet privacy or on the EU's General Directive on Privacy Regulation from January, 2012 to March 31st, 2014, when the European Parliament voted on the Regulation. Rossi found that Snowden's global surveillance revelations tripled the salience of Internet privacy issues covered in the press and allowed pro-privacy advocates to push for privacy-strengthening rules. Figure One reproduces Rossi's general findings for the five national sets of newspaper articles he analyzed.[32]

Figure 1: Salience of Internet Privacy Issues in the Five Biggest EU Countries, January 2013- March 2014



Source: I am grateful to Agustin Rossi for allowing me to reproduce this graphic from his "Internet Privacy in the European Union and the United States," Unpublished PhD Dissertation, European University Institute, September 2016, p. 42.

Press attention has been matched by increased funding and organization of privacy advocacy groups in both Europe and the United States. Funding growth has been greatest in the United States, where the threats to privacy have been the most extreme and have been most vividly exposed. For example, the EFF, which reported total income of $4,748 million in 2005-6, had reached an income level of over $16 million by 2014-15.[33] In the United Kingdom, Privacy International, which reported income of £487 thousand in 2010-11, had reached an income level of almost £1.6 million by 1914-15.[34] Of course, these figures come from among the most prominent privacy groups and may not be representative of the entire sector, but they are indicative of a growing interest in privacy among both the public and that foundations that sustain these groups.

Relatedly, there has been a growth in the number of adovcacy organizations defending privacy. Using the systematic source of the *Encylopedia of Associations* (EoA), Milton Mueller and his associates analyzed public interest organizations whose interests relate to the mass media, telecommunications, cable, intellectual property, privacy, and computers from 1969 through 2003 (Mueller et al, 2004:172). The most rapid growth came in the 1960s and '70s, and was mainly oriented towards "content-oriented activism." By the 1990s, however, the emphasis had shifted to the Internet and had become predominantly rights-oriented. These groups included the EEF, the Electronic Privacy Information Center, the Center for Democracy and Technology, the Internet Free Expression alliance, and the Domain Name Rights Coalition. The trend to rights-orientation

continued after the turn of the new century, with the appearance of groups such as Public Knowledge, the Center for Digital Democracy, and, more recently, Access Now (Ibid., p. 179).

Mueller and his collaborators also scanned the LEXIS-NEXIS searchable Congressional Information Service Index for hearings at which communications issues were discussed. Out of a total of 1,771 such events, the largest number (N = 227) that they identified were primarily concerned with privacy. This does not mean that privacy emerged with greater protection during these decades --on the contrary; Regan's work showed that privacy tended to evaporate in the course of congressional debates (1995); but it does mean that public interest groups interested in privacy were increasingly involved in the political process.

Greater Trans-Atlantic Connections

To the degree that an international state of emergency has expanded across the Atlantic, European and American privacy groups are increasingly facing a similar structure of opportunity and threat. Over the last decade and a half, there has been an increase in the number of privacy groups that engage in transnational issues. Already in 2004, Mueller and his collaborators noted "a series of institutional changes with transnational scope, driven by international trade concerns and foreign policy issues" (2007: 280). This led to the addition of international staff and to greater attention to international issues in groups like EPIC and the EFF. It also led to the formation of trans-Atlantic coalitions and to campaigns on internet privacy.

For example, in 2015, fourteen U.S. based civil liberties and privacy groups joined twenty European-based groups in sending a joint letter to the EU Commissioner for Justice, Consumers, and Gender Rights and to Secretary of Commerce Penny Pritzker, urging a comprehensive modernization of privacy and data protection laws on both sides of the Atlantic.[35] And in an unusual transatlantic development, American groups are also beginning to act as *amici* in court cases in Europe alongside their European counterparts. For example, in 2016, the Irish High Court accepted EPIC's application to participate in a new case about data protection rights regarding Facebooks' contractual clauses. The case follows the CJEU decision to strike down Safe Harbor in 2015. EPIC also recently joined a case before the European Court of Human concerning the activities of British and U.S. intelligence organizations.

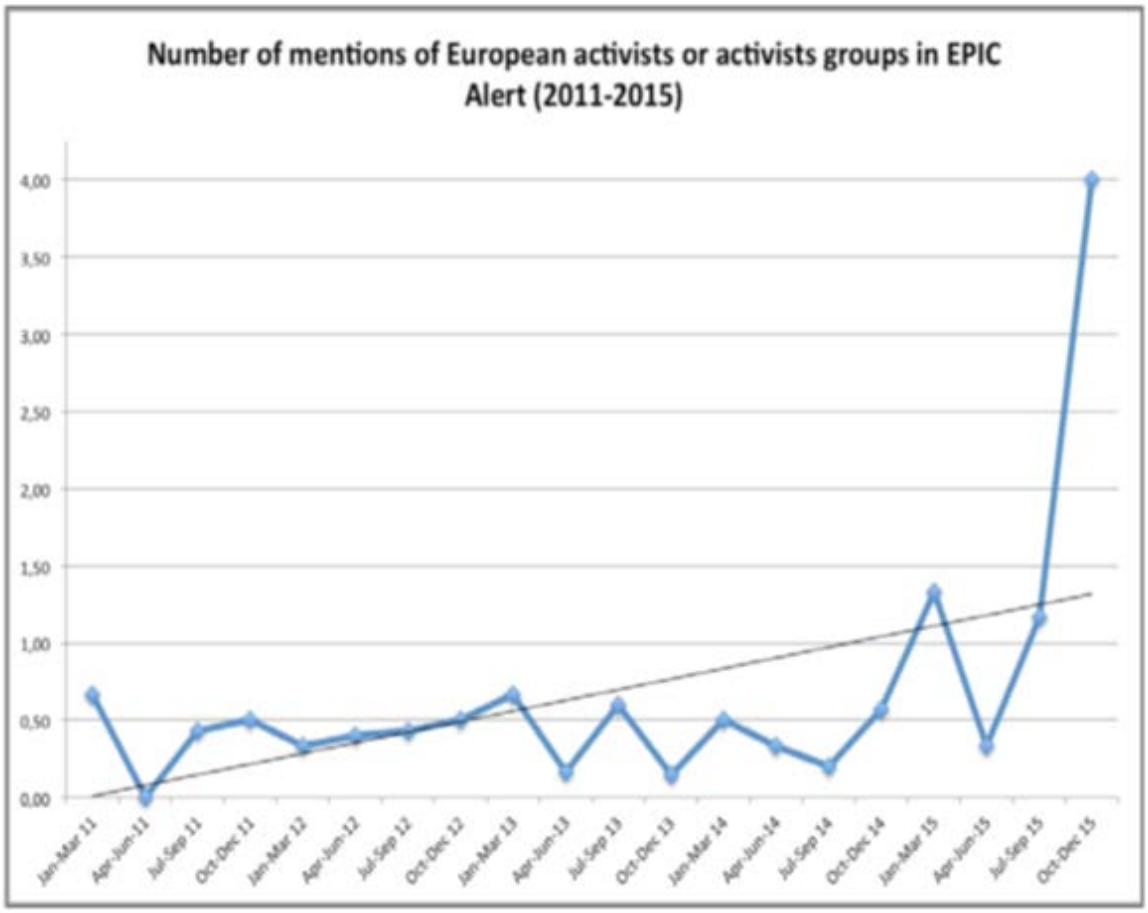
Indicative of this trend has been the creation and expansion of Access Now, which maintains eleven offices around the world, organizes the international RightsCon conference, and has dedicated activities in privacy, digital security, human rights, freedom of expression and net discrimination. Scanning the Access Now blog in August, 2016, ten of twelve postings were either international in general, or dealt with a part of the world outside the U.S.[36] Policy-oriented groups are also becoming active participants in academic conferences on privacy, both in the U.S. and in the European Union.

To probe how systematic this trend may be, Emilio Lehoucq and I collected data on the attention given to privacy issues on the other side of the Atlantic from two of the most important advocacy groups in the privacy world: EPIC, the U.S. based Electronic Privacy and Information Center, and EDRI, the Brussels-based European Digital Rights group.[37] The object of the exercise was to understand whether there has been a reciprocal growth of attention of American-based and EU-based groups to one another over time. We were also interested in the connections – if any --

between "real-world events" – like the Snowden revelations in 2013 and the dispute over Safe Harbor in 2015 – and the growth of mutual attention of European and American privacy groups to one another and to one another's concerns.

In the United States fifteen years of Epic Alert, the bi-weekly online newsletter of EPIC, were coded from 2000 through 2015. Epic Alert contains articles on privacy developments in the US and around the world, reports on breaking privacy news, reviews of the latest privacy-related publications, and lists upcoming privacy conferences and events.[38] In Europe, we coded every issue of Edri-Gram, the fortnightly online newsletter of the Brussels-based group European Digital Rights, which covers similar topics to its American-based counterpart for the period 2011-2015.[39]

Figure 2: Number of Articles in Epic Alert Dealing with European Issues, 2000-2015

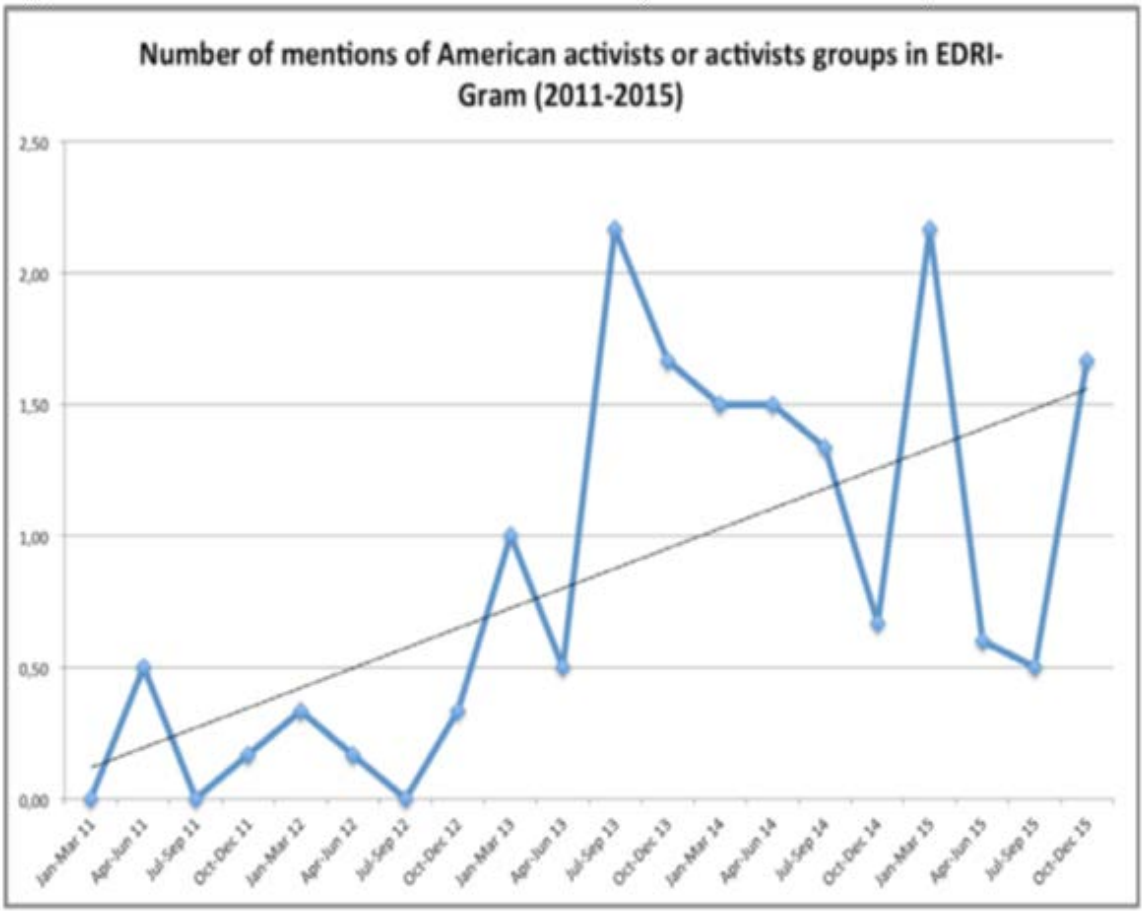


As Figure Two shows, the amount of coverage of non-US events or issues in the Washington-based *Epic-Alert* newsletter grew steadily, but moderately, during the first decade of the new century, but increased dramatically after 2012 – when Edward Snowden's revelations appeared -- and especially during the debate over the transfer of European data to the United States. A rapid inspection of these postings showed that it was the debate over Safe Harbor and the Privacy Shield that increased EPIC's attention to European developments.

Figure Three allows us to compare the Europe-based privacy group's attention to what was happening in the privacy field across the Atlantic. As Figure Three, shows EDRI's attention to the

U.S. also grew over the last half-decade, but did not follow the same trend line as that of the American group. There has been an increase in attention to American issues in this Brussels-based newsletter since 2011, but the biggest period of growth came in 2013, after the Snowden revelations became public.

Figure 3: Number of Articles in EDRi-Gram Dealing with American Issues, 2011-2015



In summary, from an intermittently-mobilized group of primarily nationally-oriented groups and a spectrum of other groups for whom privacy is only one of their concerns (Bennett 2008), as are seeing efforts to mobilize transnationally around issues like surveillance and encryption. From an opportunity structure that was sharply divided by the gaps between European and American privacy regimes, securitization is creating a submerged "coral reef" around which European and American privacy groups are mobilizing. Of course, it cannot be proven on the basis of these data that the cause of this shift is the security environment. But its timing around and after the Snowden revelations is indicative that the growth of a common security environment in Europe and America is creating a common opportunity structure for privacy groups on both sides of the Atlantic. While these findings are too fragmentary to allow us to reach firm conclusions about the potential growth of a trans-Atlantic privacy movement, there is growing evidence that such a movement is in the process of formation.

CONCLUSIONS

Part One summarized arguments from the IR literature about theimpact of globalization on the creation of transnational regulatory arrangements. The international scene has seen not only the creation of formal international institutions but a growing trend to the formation of informal transgovernmental networks. Abbott and Snidal see this trend producing a "governance triangle," which extends from states and private businesses to NGOs. They are largely correct, but their work elided what happens when close interaction clashes with incompatible regimes. The story told in this paper suggests that neither formal institutions nor side agreements like "Safe Harbor" are very good at resolving such disjunctions or laying the foundation for the creation of a transnational movement on behalf of privacy.

In Part Two, I examined the mix of opportunities and constraints in the field of privacy protection in the EU and the United States. I argued that the European regime is more unified and more protective of privacy, while the American regime is fragmentary, sectoral, and has been mainly shaped by the interests of business. Some scholars, like Rustiala, see transgovernmental networks as mechanisms to increase cooperation – or at least, to limit conflicts between states. But close interaction plus incompatible regimes produce unstable agreements and the potential for conflict. We saw this in the attempt to bridge the gap between the US and the EU privacy regimes with the Safe Harbor agreement; we will have to see whether its successor agreement – Privacy Shield – fares any better.

In Part Three, I showed how policy makers tried to bridge the gap between Europe and the United States through international agreements. Safe Harbor was never a particularly robust solution, since it only papered over the differences between Europe and America and had no provision for monitoring the intrusion of state actors into private communications. But, paradoxically, it was the securitization of transatlantic commercial communications that undercut the agreement, especially after the Snowden revelations revealed its true extent.

Part Four surveyed evidence that suggests a robust growth in the privacy advocacy sector. How are these changes affecting public policy? Demonstrating the effect of collective action on policy outcomes is one of the thorniest problems in social movement research. But if recent developments can be trusted, the developments charted in this paper may be having an effect on the EU's policies towards privacy. In December 2015, the European Commission and the European Parliament announced the General Data Protection Regulation, which replaced the 1995 Privacy Directive with binding legislation. While it is true that the new GDPR will leave wide leverage for state security agencies to penetrate privacy, it will be binding on all citizens of the EU, apply to non-members of the Union, and offer citizens a mechanism for "the right to be forgotten.[40]

When the GDPR was first proposed in 2012, it was largely seen as a mechanism aimed at ending the fragmentation and administrative burdens of the 1995 DPD and unifying the data protection regimes of the different European states. But in the course of its deliberations, spurred by privacy advocates, by the Article 29 Working Party, and by members of the European Parliament, the Commission added more robust data protection features to the regulation – precisely the opposite of the process that Regan had found in the privacy legislation she studied in the American Congress (1995).

What had happened to put steel into a legislative process that more typically leads to the watering-down of legislation? The proven weakness of Safe Harbor was one reason; the geometric growth of transatlantic digital communication was another; but the most important was the explosion of concern for the dangers of the surveillance of private communication that was triggered by the Snowden revelations and then by the Schrems case. These actions by civil society actors brought together privacy advocates, political actors, and tech firms that were pushed into a privacy-defending position that their previous behavior would not have predicted.

Securitization is a double-edged sword: while it has increased the ability of states to penetrate digital communications, it has also created a common political opportunity structure that has triggered the growth of a coalition of tech firms, privacy advocates, and institutional actors in the defense of online privacy. The data assembled in Part Four of this paper suggests that the loose network of privacy-oriented groups that Collier mapped in the last decade may be coalescing into a transnational movement, which is the only way that the power of powerful states can be effectively contested (Cole 2015).

Sources

Abbott, Kenneth W., and Duncan Snidal. 2009. "The Governance Triangle: Regulatory Standards, Institutions and the Shadow of the State." Pp. 44-88 in *the Politics of Global Regulation*, edited by Walter Mattli and Ngaire Woods. Princeton: Princeton University Press.

Banaszak, Lee Ann. 2009. "Moving feminist Activists Inside the American State: The Rise of a State-Movement Intersection and its Effects on State Policy." Pp. 223-54 in *The Unsustainable American State*, edited by Lawrence Jabobs and Desmond King. New York: Oxford University Press.

Bennett, Colin J. 2008. *The Privacy Advocates: Resisting the Spread of Surveillance*. Cambridge: MIT Press.

—. 2010. "Storming the Barricades So We Can All Be Private Together: Everyday Surveillance and the Politics of Privacy Advocacy." *Leviathan* 25:299-320.

—. 2011. "Privacy Advocacy from the Inside and the Outside: Implications for the Politics of Personal Data Protection in Networked Societies." *Journal of Comparative Policy Analysis: Research and Practice* 13:125-41.

Bennett, Colin J. and Rebecca Grant (Eds.) *1999. Visions of Privacy: Policy Choices for the Digital Age*. Toronto and London: University of Toronto Press.

Bennett, Colin J., and Charles Raab. 2003. *The Governance of Privacy: Policy Instruments in Global Perspective*. Aldershot: Ashgrate.

Bennett, W. Lance, and Alexandra Segerberg. 2013. *The Logic of Connective Action*. New York: Cambridge University Press.

Brooks, Rosa. 2014. "The Trickle-Down War." *Harvard Law and Policy Review* 32:583-602.

Chatfield, Charles, Jackie Smith, and Ron Pagnucco (Eds.). 1997. *Transnational Social Movements and Global Politics*. Syracuse: Syracuse University Press.

Cole, David. 2015. *Engines of Liberty*. New York: Basic Books.

Culpepper, Pepper. 2011. *Quiet Politics and Business Power: Corporate Control in Europe and Japan*. New York: Cambridge University Press.

Davies, Simon. 1999. "Spanners in the Works: How the Privacy Movement is Adapting to the

Challenge of Big Brother." Pp. 244-62 in *Visions of Privacy: Policy Choices for the Digital Age*, edited by Colin J. Bennett and Rebecca Grant. Toronto and London: University of Toronto Press.

Diani, Mario, and Ivano Bison. 2004. "Organizations, Coalitions, and Movements." *Theory and Society* 33:281-309.

Farrell, Henry, and Abraham Newman. 2014. "The New Politics of Interdependence: Cross-National Layering in Trans-Atlantic Regulatory Disputes." *Comparative Political Studies* 48:497-526.

---.2016. "The Transatlantic Data War: Europe Fights Back Against the NSA." *Foreign Affairs* 95(January-February):124-33.

Greenberg, Karen. 2016. *Rogue Justice: the Making of the Security State*. New York: Crown.

Hofmann, Jeanette, Christian Katzenbach, and Kirsten Gollatz. 2016. "Between Coordination and Regulation: Finding the Governance in Internet Governance." *New Media and Society* 18:1-18.

Keohane, Robert O., and Joseph S. Nye (Eds.). 2001 [1979]. *Power and Interdependence: World Politics in Transition*. New York: Addison-Wesley Pub. Co.

Kong, Lingjie. 2010. "Data Protection and Transborder Data Flow in the European and Global Context." *European Journal of International Law* 21:441-56.

Kreuder-Sonnen, Christian. 2016. "Emergency Powers of International Organizations." Unpublished PhD Thesis, Political Science, Free University of Berlin.

Long, William, and Marc Pang Quek. 2002. "Personal Data Privacy Protection in an Age of Globalization: The US-EU Safe Harbor Compromise." *Journal of European Public Policy* 9:325-344.

Lynskey, Orla. 2014. *The Foundations of EU Data Protection Law*. Oxford: Oxford University Press.

Lyon, David. 2003. *Surveillance After September 11*. Cambridge: Polity.

Mansell, Robin. 2012. *Imagining the Internet: Communication, Innovation, and Governance*. Oxford: Oxford University Press.

Mueller, Milton, Brenden Kuerbis, and Chrsitane Page. 2007. "Democratizing Global Communication? Global Civil Society and the Campaign for Communication Rights in the Information Society." *Inernational Journal of Communication* 1:267-296.

Mueller, Milton, Christiane Page, and Brenden Kuerbis. 2004. "Civil Society and the Shaping of Communication-Information Policy: Four Decades of Advocacy." *The Information Society* 20:1-17.

Newman, Abraham L. 2008. *Protectors of Privacy: Regulating Personal Data in the Global Economy*. Ithaca and London: Cornell University Press.

—. 2008a. "Building Transnational Civil Liberties: Transgovernmental Entrepreneurs and the European Data Privacy Directive." *International Organization* 62:103-30.

Raustiala, Kal. 2002. "The Architecture of International Cooperation: Transgovernmental Networks and the Future of International Law," *Virginia Journal of International Law* 43:2-23.

Regan, Priscilla. 1995. *Legislating Privacy*. Chapel Hill and London: University of North Carolina Press.

—. 1999. "American Business and the European Data Protection Directive: Lobbying Strategies and Tactics." Pp. 199-216 in *Visions of Privacy: Policy Choices for the Digital Age*, edited by Collin J. Bennett and Rebecca Grant. Toronto and London: University of Toronto Press.

Regan, Priscilla M., Colin J. Bennett, and Robin M. Baykley. 2016. "If These Canadians Lived in the United States, How Would They Protect Their Privacy?" in *2016 Privacy Law Scholars Conference*. George Washington University.

Reidenberg, Joel R. 2014. "The Data Surveillance State in the United States and Europe." *Wake Forest Law Review* 49:583-608.

Rossi Silvano, Agustin. 2016. "Internet Privacy in the European Union and the United States." in *Political and Social Sciences*: European University Institute.

Rotenberg, Marc, and David Jacobs. 2013. "Updating the Law of Information Privacy: The New Framework of the European Union." *Harvard Journal of Law and Public Policy* 36:607-252.

Scheppele, Kim Lane. 2004. "Law in a Time of Emergency: States and the Temptations of 9/11."

Journal of Constituitonal Law 6:1-75.

Sell, Susan. 2013. "Revenge of the 'Nerds': Collective Action Against Intellectual Property Rights Maximalism in the Global Information Age." *International Studies Review* 15:67-85.

Shiffrin, Steven H. 2016. *What's Wrong with the First Amendment?* New York: Cambridge University Press.

Westin, Alan. 1967. *Privacy and Freeedom*. New York: Athaneum.

Whitman, James Q. 2004. "The Two Western Cultures of Privacy: Dignity versus Liberty." *Yale Law Journal* 114:1151-1221.

Zurn, Michael. 2002. "From Independence to Globalization." in *Handbook of International Relations*, edited by Walter Carlsnaes, Thomas Risse, and Beth Simmons. London: Sage.

[1] Ellen Nakashima, "Google, Facebook and Other Powerful Tech Firms Filing Briefs to Support Apple. *The Washington Post* February 28, 2016. www.washingtonpost.com/world/national-security/google-facebook-and-other-powerful-tech-firms-filing-briefs-to-support-apple/2016/02/28/beb05460-de48-11e5-846c-10191d1fc4ec_story.html. For a list of amicus briefs and letters to the court as of March 3, go to http://www.apple.com/pr/library/2016/03/03Amicus-Briefs-in-Support-of-Apple.html.

[2] In their 2009 paper, Abbott and Snidal characterized these groups broadly and assumed that actors in each group pursue their own interests and values when they bargain for influence. Their "triangle" represents actual schemes of transnational agreements and takes in a wide variety of institutional forms, ranging from predominantly domestic state regulation to firm self-regulation, to NGO-initiated schemes, and finally to joint and multi-actor arrangements. Abbott, Kenneth W., and Duncan Snidal. 2009. "The Governance Triangle: Regulatory Standards, Institutions and the Shadow of the State." Pp. 44-88 in *the Politics of Global Regulation*, edited by Walter Mattli and Ngaire Woods. Princeton: Princeton University Press.

[3] https://www.eff.org/cyberspace-independence. For the story of how Barlow came to write his provocative paper, go to https://www.wired.com/2016/02/its-been-20-years-since-this-man-declared-cyberspace-independence/

[4] I have calculated these numbers by eyeballing "the governance triangle" in Figure 2.1 of Abbott's and Snidal's bold effort to plot the relations among states, first, and NGOs.

[5] Hofmann and her colleagues focus "on those 'critical moments' when routine activities become problematic and need to be revised, thus, when regular coordination itself requires coordination". Also see Jeannette Hofmann, Christian Katzenbach, and Kirsten Gollatz. 2016. "Between Coordination and Regulation: Finding the Governance in Internet Governance." *New Media and Society* 18: 1-18.

[6] I define "privacy advocates," with Colin Bennett, as "anybody who might challenge the processing of personal information by government or business. See Collier's "Storming the Barricades So We Can All Be Private Together" Everyday Surveillance and the Politics of Privacy Advocacy." *Leviathan* 25, 2010, p. 301. As in most social movements, it is obvious that not all advocates are transnational, and not all those who "challenge the processing of personal information" are advocates. Many are part of institutional groups and others represent political parties.

[7] The EFF's 2015 audited financial report can be found at https://www.eff.org/document/fiscal-year-2014-15-audited-financial-statement. Of the corporate foundations, $1.5 million came from a single source, "Humble Bundle."

[8] Note that the 1995 Directive is to be superseded by a new General Data Protection Regulation (GDPR) in 2018. For a brief analysis, see Courtney M. Bowman, "A Primer on the GDPR: What You Need to Know," *Privacy Law Blog*, December 23, 2015,at http://privacylaw.proskauer.com/2015/12/articles-european-union. For a comparison between the 1995 directive and the GDPR, see Orla Lynskey *The Foundations of EU Data Protection Law*. Oxford: Oxford University Press, 2014, ch. 2.

[9] A good summary can be found in Colin Bennett and Charles Raab, *The Governance of Privacy: Policy Instruments in Global Perspective*. Aldershot: Ashgrate, 2003, pp. 19, 78-80, who also provide a list of the diffusion of data protection legislation in Europe and elsewhere (p. 102), and of the agencies with authority to protect privacy in OECD countries (pp. 108-9). For a sustained analysis of the Data Privacy Directive and of the progress of data protection in Europe before the passage of the GDPR, see Abraham Newman's *Protectors of Privacy: Regulating Personal Data in the Global Economy,* Ithaca: Cornell University Press, 2008.

[10] Milton Mueller and his associates have carried out a thorough analysis of congressional hearings on communications and information privacy in the United States. See their report "Reinventing Media Activism: Public Interest Advocacy in the Making of U.S. Communication-Information Policy, 1960-2002" at http://arifyildirim.com/ilt510/milton.mueller.pdf.

[11] 18 U.S.C, &&2510-2522 (2012) and && 2701-2712.

[12] The new Consumer Finance Protection Bureau may eventually grow into that role unless it is suppressed by the Trump administration. The CFPB was created by an act of Congress in 2011 in the wake of the financial scandals that had created the Great Recession of 2008. For a brief introduction, go to http://www.consumerfinance.gov/

[13] The most dramatic recent change was the approval by the Federal Trade Commission to prevent companies like AT&T and Comcast from collecting and giving our digital information about individuals – such as the websites they visit and the apps they use. Although the FCC has general responsibility for regulating communications, this was the first time the agency has passed protection of online communications. See Cecilia Kang, "Broadband Providers Will Need Permission to Collect Private Data," *New York Times*. October 27, 2016 at http://www.nytimes.com/2016/10/28/technology/fcc-tightens-privacy-rules-for-broadband-providers.html?_r=0

[14] As such, the agreement had more the character of a contract than an international regulation. As Lingjie Kong writes of such third-party agreements, "Such contracts do not provide a waterproof guarantee; questions remain as to the possibilities of controlling their implementation or enforcing their clauses." Kong, Lingjie. 2010. "Data Protection and Transborder Data Flow in the European and Global Context." *European Journal of International Law* 21, 2010, p. 448).

[15] A brief synopsis of this critical legislation, passed by Congress at the insistence of the Bush administration soon after the September 11th terrorist attacks can be found at https://epic.org/privacy/terrorism/hr3162.html. For the general impact of 9/11 on Americans' privacy see Lyon (2003).

[16] Former NSA director Keith Alexander was later quoted as saying; "Yes, I believe it is in the nation's best interest to put all the phone records into a lockbox that we could search." http://bigstory.ap.org/article/senators-limit-nsa-snooping-us-phone-records.

[17] Court of Justice of the European Union, Press Release No. 117/15. Judgement in Case C-362/14. Maximilian Schrems v Data Protection Commissioner, Luxembourg, October 6, 2015.

[18] The decision will be found at Curia.europa.eu/documents-JSF?number=C-362/14. For a reasonably balanced account, see Natalia Drozdiak and Sam Schechner, "EU Court Says Data-Transfer Pact With U.S. Violates Privacy." *Wall Steeet Journal,* October 6, 2015.

http://www.wsj.com/articles/eu-court-strikes-down-trans-atlantic-safe-harbor-data-transfer-pact-1444121361. A more technical, but still brief analysis will be found in "European Court of Justice Invalidates US-EU Safe Harbor," Oct. 8, 2015. http://www.natlawreview.com/article/european-court-justice-invalidates-us-eu-safe-harbor-agreement.

[19] "The Court of Justice declares that the Commission's US Safe Harbour Decision is invalid." Court of Justice of the European Union press release No. 117/15, Luxembourg, 6 October 2015, at http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf.

[20] The Protect America Act of 2007 (PAA), (Pub.L. 110–55, 121 Stat. 552, was passed as an amendment to the Foreign Intelligence Surveillance Act (FISA) that was signed into law by President George W. Bush on August 5, 2007. The act removed the requirement that the government needed a warrant for surveillance of foreign intelligence targets that were "reasonably believed" to be outside of the United States. Title VII of the FISA Amendments act of 2008 reauthorized many provisions of the Protect America Act. For this important act, go to http://www.intelligence.senate.gov/laws/fisa-amendments-act-2008.

[21] Craig Timberg, "US Threatened Massive Fine to Force Yahoo to Release Data," *Washington Post,* September 11, 2014. https://www.washingtonpost.com/business/technology/us-threatened-massive-fine-to-force-yahoo-to-release-data/2014/09/11/38a7f69e-39e8-11e4-9c9f-ebb47272e40e_story.html?utm_term=.eeb8f100a87f.

[22] Directive 2006/24/EC, art. 1, 2006 O.J> (L105) 54 EC.

[23] But note that in a recent decision, the European Court of Justice struck down the predecessor of the Investigatory Powers Act, the Data Retention and Investigatory Powers Act (DRIPA), which the court held did not meet EU standards on data retention. Owen Boycott, "EU's Highest Court Delivers Blow to UK Snooper's Charter," *The Guardian Online,* December 21, 2016. https://www.theguardian.com/law/2016/dec/21/eus-highest-court-delivers-blow-to-uk-snoopers-charter. Of course, the Brexit vote may make this decision moot.

[24] Joel Reidenberg,"The Data Surveillance State in the United States and Europe." *Wake Forest Law Review* 49 (2014), notes no. 99 and 100) references opinions of the Data Protection authorities and of the Article 29 Working party to the Data Retention Directive that give the flavor of these authorities' vigorous objections.

[25] As Lynskey cautions, in actual practice, the European "omnibus" system affords generous exceptions to data regulation for the public sector – especially where national security and police are concerned while the United States may be moving glacially towards the European model. Lynskey references the emergence of industry self-regulation in areas previously governed by market forces, and what she sees as "an increased impetus for private sector regulation." (Lynskey, 2014. The Obama administration's proposed "Consumer Privacy Bill of Rights Act" of 2015 was blocked in Congress and was criticized for not going far enough by a coalition of consumer groups. For the White House draft, go to https://www.whitehouse.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf. For an analysis of the bill and its failure to go anywhere, go to

http://www.nytimes.com/2016/02/29/technology/obamas-effort-on-consumer-privacy-falls-short-critics-say.html?_r=0.

[26] Blaze's original paper can be found at www.Crypto.com/papers/eesproto.pdf. He has written up the story for general readers in "Key Escrow from the Safe Distance," at www.crypto.com/paperrs/escrow-acsacii.pdf.

[27] This summary comes from a somewhat more detailed analysis, including the relevant documents at the time, put together by EPIC called "The Clipper Chip," available at https://epic.org/crypto.clipper/default.htm. The article, "ATT, No Joy at Clipper Flaw," was published on June 3, 1994 on the first page of the business section of the *Times*. http://www.nytimes.com/1994/06/03/business/at-at-t-no-joy-on-clipper-flaw.html.

[28] As of February 2017, a google search for "clipper chip" turned up 851,000 hits. The debate following the proposed release of the program led to an enormous outpouring of online and press analyses of what the government had tried to do and its technical failings. For a list of web-based discussions, go to the Electronic Frontier Foundation's archive, "Privacy - Crypto - Key Escrow 1993-4 (US): Clipper/EES/Capstone/ Tessera/ Skipjack" Archive. I am in debt to Cindy Cohn, executive director of the EFF for alerting me to the importance of this early case.

[29] The letter will be found at https://epic.org/crypto/clipper/crypto_experts_letter_1_94.html.

[30] James Eng, "200 Cyber Activists Urge World Leaders to Reject Encryption 'Back Doors," NBC News online, January 11, 2016 at http://www.nbcnews.com/tech/security/200-cyber-activists-urge-world-leaders reject-encryption-back-doors-n494191.

[31] https://www.rightscon.org/. The 2017 conference will be held in Brussels and will deal centrally with the issues examined in this paper.

[32] These findings can be found in Augustin Rossi's PhD thesis, "Internet Privacy in the European Union and the United States," European University Institute, September, 2016. Note that there are interesting variations among the five countries' newspapers that he studied, but these do not modify the general trend in Figure One.

[33] These figures come from audited data released by the EFF in 2006 (https://www.eff.org/about/annual-reports-and-financials), and in 2016 (https://www.eff.org/document/fiscal-year-2014-15-audited-financial-statement).

[34] The Privacy International official income figures for these years will be found at https://www.privacyinternational.org/node/102.

[35] See "EU-US Letter on Safe Harbor After Schrems." http://r.search.yahoo.com/_ylt=A0LEV76NfopXL2cAgo0PxQt.;_ylu=X3oDMTByOHZyb21tBGNvbG8DYmYxBHBvcwMxBHZ0aWQDBHNlYwNzcg--/RV=2/RE=1468722957/RO=10/RU=http%3a%2f%2fthepublicvoice.org%2fEU-US-NGO-letter-Safe-Harbor-11-15.pdf/RK=0/RS=FT_WgXqM4LBMBUmfA7iwmB79D2g-

[36] https://www.accessnow.org/issue/privacy/. The Brussels2017 Rightscon conference program will be found at https://www.rightscon.org/cms/assets/uploads/2017/02/RC2017-draft-program-v1.0.pdf.

[37] My thanks to Emilio Lehoucq, of the University of the Andes in Bogota, Colombia, for carrying out the coding of these newsletters for this paper.

[38] https://epic.org/alert/

[39] https://edri.org/newsletters/

[40] http://ec.europa.eu/justice/data-protection/reform/index_en.htmcontent/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC. http://ec.europa.eu/justice/data-protection/reform/index_en. The main legal difference between a directive and a regulation is that while the former allows each government to implement it as their parliaments decide, the latter becomes law in each country in the form in which it is handed down from Brussels.