**Linkage Politics in an age of Multi-level Governance:**

**Surveillance in the Transatlantic Relationship**

By

Henry Farrell and Abraham Newman

**Abstract:**

The rise of globalization increasingly blurs traditional distinctions between “high” and “low” politics, as issues that were previously negotiated discretely become entangled with one another. Despite such blurring of boundaries, we know that the extent of explicit political connections between issues vary. A significant existing literature focuses on how states may intentionally tie policy areas together in order to enhance cooperation. In this article, we argue that this literature fails to incorporate another important set of changes in world politics – the rise of complex governance, in which an increasing number of non-state actors work to shape the international political agenda. Building on recent historical institutional research, we develop an argument for how such non-state actors may employ issue linkage to alter the dynamics of international negotiations. We assume that the extent of political discretion enjoyed by heads of state to negotiate and implement international agreements can vary across issue areas. When policy domains are linked, so too are different political configurations, each with its own structures of barriers of cooperation or points of leverage. This means that actors, whether state or private, may use issue linkage to exploit *heterogeneity of political discretion across different issue areas* to increase their influence over policy outcomes*.* We examine our theory in the hard case of international cooperation over intelligence and data exchange. Our findings speak to a number of critical debates in international relations including the role of non-state actors in diplomacy and the important intersection of the subfields of international political economy and security brought on by globalization.

Please email comments to aln24@georgetown.edu

The rise of globalization increasingly blurs traditional distinctions between policy and issue areas. Communication networks provide the backbone of e-commerce and an opportunity for cyberattacks; international banking facilitates both global investment and terrorist financing; trade in goods makes consumer products cheaper but can help fund civil wars and human rights abuses. This has important consequences for global politics, as issues that were previously negotiated as separable discrete packages become entangled with one another and distinctions between “high” and “low” politics become harder to sustain.[[1]](#footnote-1) Despite such blurring, we know that the extent of explicit political connections between issues vary. In other words, policy-makers sometimes actively couple issues together, while at other times they work to keep them distinct.[[2]](#footnote-2) In this paper, we seek to address the factors that promote or hinder issue linkages in an age of globalization and to understand how such linkages affect global politics.

A significant literature on negotiations and regime interaction focuses on how states may intentionally tie policy areas together in order to enhance the chance of cooperation.[[3]](#footnote-3) Research, for example, has demonstrated that broadening the agenda may dilute blocking constituencies and create package deals, enhancing the spoils of working together.

In this article, we argue that this literature fails to incorporate another important set of changes in world politics – the rise of complex governance in which an increasing number of non-state actors may work across jurisdictions in order to shape the international political agenda.[[4]](#footnote-4) Non-state actors may potentially disagree with individually or collectively held state policies and may look to link issues strategically in order to achieve their goals.[[5]](#footnote-5) As Keck and Sikkink (1999) observed two decades ago, disputes between non-state actors and states involve issue linkage just as surely as do disputes among states. Yet we do not have any specific theories of how non-state actors may use issue linkage in order to press against states, or how states may use issue linkage to out maneuver non-state actors, where they disagree.

In this article, we set out such a theory, integrating Keck and Sikkink’s claims with theories of procedural politics to understand how issues may become linked, or alternatively remain separate in an age of interdependence.[[6]](#footnote-6) Much of the work on linkage politics assumes that institutional barriers to cooperation are homogenous across issue area. Building on recent work inspired by historical institutional approaches, however, we emphasize how the extent of political discretion enjoyed by heads of state to negotiate and implement international agreements can vary across issue areas.[[7]](#footnote-7) When policy domains are linked, so too are different political configurations, each with its own structures of barriers of cooperation or points of leverage shaping the relative influence of different actors. Influence maximizing actors will typically want to maximize their own discretion, while using available constraints to minimize the discretion of others with different priorities. This means that actors, whether state or private, may use issue linkage to exploit *heterogeneity of political discretion across different issue areas.*

Putting these two modifications to the existing literature – the role of non-state actors and heterogeneity of political discretion across different issue areas – together offers a set of alternative empirical expectations in which state[[8]](#footnote-8) and non-state actors have new possibilities to use domestic rule setting structures to reshape bargaining dynamics in international negotiations. For example, it may allow non-state actors to connect issue spaces that *all relevant states* would prefer to see disconnected and as a result unsettle the reversion point of negotiations prior to the policy linkage. Such linkage politics are most likely to occur when non-state actors can activate domestic political structures that differ across issue spaces. Alternatively, states may seek to link issue areas with different levels of political discretion so as to conduct a negotiation in either a more or less permissive environment.

This also helps explain how new knowledge can have consequences for international politics. As constructivists have argued, the emergence of new knowledge through more or less exogenous processes can demonstrate potential linkages between areas that were hitherto disconnected.[[9]](#footnote-9) New knowledge hence provides a key basis for political entrepreneurialism, allowing actors to forge new linkages and hence reshape the underlying assumptions of politics.[[10]](#footnote-10) However, our arguments would suggest that entrepreneurs can only take advantage of issue linkage when there is substantial heterogeneity of political discretion between the relevant issue areas. This heterogeneity is what allows actors to exercise new forms of political influence by constraining other actors that previously enjoyed a high degree of discretion. Our argument, then, provides an important explanation for variation in effect of new knowledge on political dynamics.

We apply this analysis to a “hard case,” international cooperation over intelligence and surveillance, asking what happens when an external shock of new knowledge (in this case, the revelations made by Edward Snowden) opens up the possibility for greater issue linkage. Given the stakes involved in intelligence sharing, traditional accounts of international relations would expect that “high politics” would prevail, leaving little room for influence by non-state actors. More standard issue linkage accounts would predict that states promoted linkage in order to facilitate agreement or to mitigate potential negative spillovers between the affected issue areas. As we show, none of these logics appear to have prevailed. Instead, non-state actors used the Snowden revelations to activate new political constraints that existed across issue areas and thus shifted the negotiation dynamic.

Our findings have important implication for a number of literatures. First and foremost, we connect a growing literature on complex governance to work on international negotiations.[[11]](#footnote-11) The latter has tended to focus on states and state preferences, creating an unnecessary theoretical blind spot, particularly as sub-state and non-state actors come to influence such diplomatic interactions in empirically demonstrable ways.[[12]](#footnote-12) Second, the paper helps build the foundation for a more fine-grained understanding of the role of domestic institutions in international politics. While a considerable literature has focused on variation between regime types, more and more evidence suggests the importance of variation within them.[[13]](#footnote-13) Our work highlights how even across policy streams, important international decision-making processes can be shaped by the shifting configuration of domestic institutional structures. Third, we contribute to research on issue linkage, by reviving classic debates on substantive linkage, in which policy sectors become conjoined by substantial knowledge of tangible inter-relations between them, and underpinning them with a sharper understanding of the underlying mechanisms. While the literature has focused primarily on tactical quid pro quo exchanges, the changing reality of global politics demands greater attention to such substantive linkages, which are an increasingly important strategic resource for actors looking to influence policy outcomes.[[14]](#footnote-14) Finally, the intersection of information markets and commercial exchange with national intelligence demonstrates the increasingly intertwined nature of economic and security issues. Our detailed empirical evidence captures the shifting nature of cooperation and conflict, highlighting how political economy and security often work in tandem in ways that are underexplored in the scholarly literature, as well as providing potential insights to policy-makers searching to understand the politics of surveillance in a digital age.

*Issue Linkage and Interdependence*

A substantial literature focuses on the ways that issue linkage can transform global politics. This body of work has already examined how economic and security issues get combined with consequences for international cooperation. There are two major approaches in the field – bargaining approaches, which invoke rationalist models, and knowledge based approaches, which invoke constructivist ideas. Both tend to stress the importance of state preferences.

Bargaining approaches typically examine how issue linkage helps resolve the difficulties that rational states have in reaching agreement with each other.[[15]](#footnote-15) When issue linkage is connected to choice of forum, it can become a source of asymmetric bargaining strength, providing opportunities for forum shopping and changing states’ fallback options.[[16]](#footnote-16) Here, issue linkage can potentially work through three distinct mechanisms. First, by widening the set of issues that are up for negotiation, credible forms of issue linkage increase the potential gains from agreement, and hence the likelihood that states will indeed agree.[[17]](#footnote-17) Package deals expand the win-set for the parties involved and help bribe or drown out concentrated voices of opposition. Second, issue linkage can increase the credibility of cooperative arrangements, by raising the costs of defection.[[18]](#footnote-18) Third, issue linkage can lead to ‘regime integration’ as states focus on the potential negative effects of no coordination.[[19]](#footnote-19) Under this account, issue linkage is driven by the fear of potentially negative spillovers rather than the prospect of benefits to cooperation.

Knowledge based accounts – most prominently Haas (1980) – alternatively argue that scientific knowledge plays a key role in determining issue linkage. Haas distinguishes between mere ‘tactical’ linkage, in which states link two unconnected issues either to increase the chance of a deal or to provide bargaining leverage, and ‘substantive’ linkage, in which states come to link together previously disconnected issues because their consensual knowledge has changed so as to identify hitherto undiscerned connections.[[20]](#footnote-20) This account tends to blur together the issues being linked and the procedural politics associated with the issues, concentrating instead on the expansion of knowledge. Here again, state’s preferences are key to explaining how issue areas become linked – but rather than involving purely strategic considerations, they involve a mixture of bargaining and changing knowledge. Under this account, advances in scientific understanding (or, perhaps, broader understandings of relevant causal relationship) create opportunities for state actors to combine issue areas.[[21]](#footnote-21) Ultimately, however, state preferences determine whether such opportunities become activated. Specifically, changes in knowledge will lead to the connection of policy areas, when knowledge changes identify benefits to negotiating states of bringing the policy areas together.

These accounts all agree that state preferences drive issue linkage. They disagree over whether preferences are shaped by states’ collective desire to reach a deal, their collective and/or individual need to demonstrate credibility, their collective fear of negative spillover effects in the absence of coordination, or their individual desire to maximize their bargaining strength and hence influence over any agreement.

This focus makes them valuable for explaining negotiation outcomes in forums where states exclusively dominate, including a variety of negotiations touching on the relationship between security and economics, or where non-state actors hover in the background. For example, Gowa and Mansfield (1993, 1997) and Poast (2012) argue that economic relations can help secure alliances. Davis (2009) argues that the relationship between trade and peace will depend on domestic structures – where foreign policy makers are relatively autonomous, they will be able to secure alliances through trade-based side payments, but where they are subject to domestic business influence, they may instead be obliged to use their military influence to try to extract economic concessions from allies.

However, such accounts are less well fitted for explaining outcomes across issue areas where states rub shoulders with non-state actors in civil society or in the business world in determining institutional outcomes. While they explain how states may be constrained by the need to appeal to domestic interest groups, they do not treat these interest groups, or other actors, as bargainers themselves. In many situations, this will miss out on crucial dynamics of policy change.

With the rise of greater economic exchange and international communication, the state has lost its monopoly control over many channels of diplomacy.[[22]](#footnote-22) Instead, a range of alternative actors from domestic regulators through NGOs to corporations can engage with each other and international organizations directly, without state mediation. Non-state actors play an increasingly important role in security (where the high politics of inter-state conflict increasingly blurs into the activities of non-state actors and political economy (where informal and semi-formal arrangements among businesses, non-state actors and sub-state regulators are beginning to crowd out formal treaty negotiations between states).[[23]](#footnote-23) Moreover, in many instances key international disagreements are not simply those between heads of state but between a more complex array of actors, including states arguing with non-state actors or collections of sub-state and non-state actors vying against one another.

Specifically, we expect that standard issue linkage accounts are likely to struggle in explaining the political dynamics associated with globalization in which economic and security questions blur so that non-state actors are hard to exclude from the negotiation table – financial regulation, surveillance, conflict minerals, cybersecurity, anti-money laundering and anti-terrorism measures to name a few. In such issue areas, security, economic exchange and domestic order have become increasingly intertwined. Furthermore, in these areas, states not only have to negotiate among themselves but negotiate with or circumvent a variety of non-state actors as well as actors within the government.

*Linkage Politics in an Age of Complex Governance*

While these research programs offer useful heuristics for a period in which the state dominated diplomatic relations, we attempt to build a model of issue linkage in an era of complex governance. With the rise of greater economic exchange, global transportation, digital networks, and multinational supply-chains, other actors including firms, NGOs, regulators and at times individuals have become important actors in global politics. Our goal is not to revisit the ‘new actors’ debate but understand its significance to diplomatic interactions. At the same time, we take seriously the call to explore variation in domestic institutional differences. These two insights – new actors and heterogeneous levels of political discretion by issue area – form the building block of our alternative analytic approach.

In this world, the preferences of the government remain important, but not sacrosanct in determining how different issue areas intersect. The existing literature summarized above tends to emphasize the benefits that unitary states may accrue by linking issues. But states may have a strong interest in maintaining high boundaries between those policy areas where they have the greatest freedom of action, and those policy areas where they are more constrained by domestic institutions.

At the same time, sub-state and non-state actors now exist that have access to global public policy venues and often have distinct preferences from the state.[[24]](#footnote-24) There is considerable work from a number of theoretical perspectives, which demonstrates the agenda setting power of non-state actors. Work on epistemic communities, for example, stresses the importance of technical expertise and scientific authority in forming global policy.[[25]](#footnote-25) By contrast, recent work on NGOs has highlighted the ways in which central organizations serve as gatekeepers that filter knowledge produced in an organizational ecology.[[26]](#footnote-26) Finally, a considerable body of literature suggests that non-state actors can serve as norm entrepreneurs, framing certain problems in a particular way so that they resonate with other powerful actors.[[27]](#footnote-27) Work in the neo-functionalist tradition, for example, stresses how political entrepreneurs can leverage the stresses of greater interdependence to couple distinct policy domains to one another.[[28]](#footnote-28) All of this research suggests that these new actors may be well positioned both to generate the ‘new knowledge’ necessary for substantive linkages and (which is our focus in this paper) influence their adoption by the broader international community.

Our account will not offer significant added value in cases where these actors share preferences with major states, or states are agnostic, or where domestic actors have no significant ability to bargain over internationally relevant policy questions. It will provide the sharpest contrast with existing theories in situations where the relevant states more or less share common preferences, where these preferences differ from those of significant non-state domestic actors, and where those domestic actors potentially have the necessary resources (whether access to public opinion, or mandated consultation, or law courts) to bargain over the relevant policy questions. NGOs and independent regulators, for example, may have a strong interest in breaking down barriers between policy domains so as to maximize states’ accountability to them. In other cases, they may seek to maintain separation between policy domains as to make it harder for states to strike package deals or engage in side payments that disadvantage them.

This raises a key question: under what conditions are non-state and sub-state actors likely to exert influence? Here, we advance a novel interpretation of the relationship between issue linkage and influence, filling a gap in the existing literature. As Keohane and Nye (1987) pointed, there may be advantages to bringing together attention to sub-state actor dynamics with issue linkage, so as better to understand “the complex multi-level games that typically accompany issue-linkage in world politics.” [[29]](#footnote-29) Keck and Sikkink (1999:97) observe that:

In order to bring about policy change, networks need to both persuade and pressurize more powerful actors. To gain influence the networks seek leverage…over more powerful actors. By exerting leverage over more powerful institutions, weak groups gain influence far beyond their ability to influence state practices directly. Identifying points of leverage is crucial strategic step in network campaigns…Material leverage usually takes the form of some kind of issue-linkage…

However, there is no substantive body of work on exactly how the entrepreneurialism of non-state actors and issue linkage work together. The existing scholarship has focused on the earlier stages of the process, in which actors provide new information or use such information to frame and alter substantive debate, rather than examining the specific mechanisms through which actors can apply information, once it has become available, to exploit new forms of issue linkage. This arguably over-emphasizes the importance of new information *as such* while failing to pay attention to the specific circumstances under which new information does, or does not, allow actors to behave in entrepreneurial ways. In short, we agree with Haas that new knowledge may bring states (or in our account states and non-state actors) to focus on actual and practical ways in which issues are linked together, and on how best to deal with these linkages. However, existing work on substantive linkage still fail to tell us how actors will practically respond to these potential linkages.

To build an alternative account we move away from Haas’s (1980) reasonably sharp distinction between the logic of strategic interaction and the logic of how knowledge is generated and used. We argue that knowledge of potential links between issues potentially provides strategic resources for actors, but they must be able to leverage that knowledge politically to shape negotiation outcomes.

Specifically, we point to how different issues are often systematically associated with different institutional constellations, which in turn provide different competences or sources of influence for actors. We focus on the fact that political discretion -- the ease with which a chief of government may domestically enact an internationally negotiated agreement -- may not only vary by jurisdiction but also across issue or policy domains. Actors – whether sub-state, non-state or state, may be able e.g. to bring legal challenges, instigate regulatory investigations or enforcement, or mobilize electoral politics in order to shape policies in their preferred direction. However, their ability to do this will vary systematically from issue area to issue area. In some issue areas, they may have extensive opportunities to shape policy outcomes. In others, their competences will be limited, or even perhaps non-existent.

This in turn allows us to draw on arguments from historical institutionalism, which notes that institutional rules and dynamics vary considerably within jurisdictions by policy or issue domain, so that the rules covering specific issue areas create distinct dynamics for policy expansion or retrenchment. Differences in eligibility and funding, for example, between Medicaid and Social Security in the United States, create distinct possibilities for blocking policies in these different policy areas.[[30]](#footnote-30) Orren and Skowronek (1996) argue that owing to the fits and starts of political development, institutions within a jurisdiction often develop in a fragmented manner. Rather than viewing political systems as a natural equilibrium attempting to optimize a particular political outcome, they contend that political systems frequently contain internal contradictions and internal tensions, which they label political intercurrence. This sedimentary like structure of political institutions layered on top of one another over time creates important opportunities for political entrepreneurs to exploit tensions, bridging and linking distinct institutional components, to create new opportunities or constraints.

This is very much in line with international relations scholarship on ‘procedural politics’.[[31]](#footnote-31) Jupille (2012) describes how law making within the European Union was typically driven by differences in the respective competences of the Commission, Council and European Parliament across different issue areas. For example, rule-making concerning the environment might provide significant decision making power to the Commission and Parliament. Legislation concerning domestic security might fall under a quite different procedure, which provided the Council with a determinative role in shaping policies and laws. Unsurprisingly, this led legislative actors to fight to ensure that legislation with an ambiguous legal basis be considered in issue areas that maximized their influence, while limiting the influence of others, with the ever present threat of appeal to the European Court of Justice for a definitive ruling. Similarly, work on global financial regulation has exploited differences in domestic regulatory structures to explain state bargaining power.[[32]](#footnote-32)

Applying this procedural logic to issue linkage, we expect that actors’ decisions to seek either to link or to separate issue areas will depend on the specific decision making configurations of the issue spaces being linked. The most important aspect of issue linkage, from our perspective, is that it takes a policy or group of policies that was previously thought to be confined within one issue space, with its associated structures of decision making and influence, and imbricates it with another, making it susceptible to the structures of decision making and influence associated with that space too.

Where there are significant differences in the structures associated with different issue spaces, connecting them will have important political consequences. It will increase some actors’ influence over policy outcomes and decrease others. This in turn gives rise to a straightforward theory of how individual actors will decide either to try to link issues, or to keep them discrete. When actors believe that issue linkage will increase their influence over policy, by requiring that relevant policy changes be handled through procedures that give them a greater say, they will push for issue linkage. When, alternatively, issue linkage would dilute their influence (e.g. by giving increased influence to rival actors) they will oppose it. When it will have no obvious consequences (e.g. because there is no great difference in levels of influence across the two issue areas), they will be largely indifferent.

Stated more generally, if two actors, A and B, have different preferences over a policy concerning a specific issue C, the outcome will be shaped by the structures of decision making and influence associated with C. If this policy is highly politically salient (so that A and B disagree strongly over it), then the influence structures associated with C will allow the preferences of one actor or group of actors (A) to prevail, while the other (B) will be shut out. However, if new knowledge emerges that suggests that the policy potentially also involves issue D (which has substantially different associated structures of decision making and influence, which provide B with stronger influence) as well as C, then A will try to keep the issues discrete, so as to preserve its influence over the policy, by ensuring that it continues to be dealt with under the decision structures associated with C. B, in contrast, would be advantaged under the decision making and influence structures associated with D, and hence will struggle to link the two issue areas together.

This allows us to lay out reasonably clear expectations about how actors will behave after an exogenous shock to collective knowledge reveals new possibilities for issue linkage regarding a politically salient policy. First, it predicts that knowledge shocks will provide few resources for entrepreneurialism in situations where political discretion is homogenous across the issue areas. Under these circumstances, issue linkage will not result in strategic gains in influence for any actor. Second, it predicts that actors will seek to keep issue areas separate in situations where issue linkage will dilute their influence, by conjoining the issue area where the salient policy is already located with another policy area where they have less clout. Third, it predicts that actors will seek to join issue areas together, when the salient policy is located in an issue area where they have less influence, and it is now possible to join it together with an issue area where they have more influence.[[33]](#footnote-33) The key corollary of this expectation is that these actors will receive greater political leverage in the negotiation process once the issues have been linked.

To offer an initial plausibility probe of our argument, we examine international negotiation over information sharing. Over the last twenty years, there have been a series of efforts to link largely commercial disputes concerning how business should share information with each other or with governments to security concerns relating to how governments should or should not have access to this data. Given the high stakes involved in both the health of digital markets and the sharing of intelligence information, we would assume that state preferences would guide the linking or delinking of these two issues. Our detailed case study, drawing on primary sources, interviews with participants, as well as key secondary sources, demonstrates how non-state actors, most notably privacy advocates in Europe, leveraged new knowledge made available in the Snowden revelations to link economic and security issues. In doing so, they were able to activate new restrictions on political discretion and in turn generated a new negotiation dynamic. The following empirical section offers a detailed processes tracing of the interaction, contrasting our argument emphasizing non-state actors and the heterogeneity of political discretion with more conventional approaches stressing state preferences. The analytic narrative is particularly useful for theory building as it presents a hard test for non-state actors to engage in such linkage politics and it contains a number of temporal and sub-sector cases that allow us to scrutinize the competing claims.[[34]](#footnote-34)

*Transatlantic Negotiations over Digital Markets and Intelligence Cooperation*

**The Commercialization of the Internet and Digital Disputes**

When data exchange first became a transatlantic policy problem, it was interpreted in commercial terms focusing on privacy issues. In the mid-1990s, the EU introduced a comprehensive privacy law, the Data Protection Directive, in order to prevent privacy concerns from hampering European integration. However, the Directive had important external consequences, leading to fears within the US that the Directive might cripple the burgeoning e-commerce sector.[[35]](#footnote-35)

The conflict over commercial data flows stemmed in large part from the beginnings of economic interdependence in e-commerce. While it is hard to imagine today, the Internet did not exist as a commercial space until the mid-1990s, having been limited during its early existence to research and non-commercial purposes. The release in 1994 of Netscape Navigator, one of the first commercial web browsers to allow secure and encrypted communication helped a much broader base of individuals and firms to use the Internet for business purposes.[[36]](#footnote-36)

As firms and policy-makers sought to combat the pressures of increased global competition in old-line industrial sectors, e-commerce offered the potential for innovation and job creation. Market players on both sides of the Atlantic saw the transatlantic marketplace as a key source of potential growth. As described by Ira Magaziner, the US e-commerce ‘czar’:

In 1994 … President Clinton asked me to have a Cabinet level group to look at one or two things that we might do were he to be re-elected … we … determined that something which was not on the original list we were looking at, which was the commercialization of the Internet would offer the potential to drive the world economy for the next couple of decades if we could set up the right policy environment for it. … what we believed was that if the government could resist over-regulating, over-censoring, over-taxing the Internet, that it had the potential to really drive economic growth. [[37]](#footnote-37)

This anti-regulatory emphasis in the United States, in particular, set the two jurisdictions on a collision course over privacy policy. The 1995 Data Privacy Directive included an extraterritorial clause, which prevented data transfers to jurisdictions that had weak protections. Article 25 provided that transfers could only take place to countries outside the EU if those countries provided an “adequate” level of privacy protection. Where the Commission found that a country did not have adequate protection, member states were obliged to take the necessary measures to block data flows to that country. The Commission could, however, find that a country provided adequate protection, and could also negotiate with outside countries to bring them to improve their protections and make them adequate from the EU’s perspective.

This was intended to block an obvious loophole in EU law – without such a rule it would be easy e.g. for multinational corporations to transfer personal information to a third jurisdiction with weak privacy rules and process it there. However, it also very explicitly sought to remedy this through encouraging other jurisdictions to engage in negotiations with the Commission to improve their privacy rules and standards so as to achieve adequacy. Hence, the European Union more or less explicitly sought to bring the rest of the world into closer conformance with its understanding of privacy and data protection.[[38]](#footnote-38)

While the European Union created comprehensive privacy rules that covered most market activity and included oversight by independent regulatory agencies, US privacy law followed a sectoral approach with privacy rules for some sensitive sectors but not others, where industry self-regulation prevailed. The US did not and does not have a dedicated privacy agency that provides independent oversight for privacy concerns. Ultimately, Europe did not view US rules as adequate as per the clause in the 1995 Privacy Directive. This threatened to ignite the first trade war of the digital era.

Importantly for our argument, this dispute largely bracketed related security issues. When the European Union introduced the Directive, it was concerned with preserving the Single Market and travel across national borders within the EU. Instead, it largely treated ‘data protection’ as an aspect of economic integration, dealing with it through its Internal Market directorate, and was only marginally interested in it as a human right.[[39]](#footnote-39) The 1995 Data Protection Directive warned in its pre-amble that differences in national regulations might, should they continue, “constitute an obstacle to the pursuit of a number of economic activities at Community level, distort competition and impede authorities in the discharge of their responsibilities under Community law.”[[40]](#footnote-40) Since the EU had no competences relating to national security, the Directive did not cover “operations concerning public security, defense, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law.”

Nevertheless, European demands caused considerable consternation among US firms and concerned US officials. In Magaziner’s description:

A lot of our companies were reacting with great concern, and coming to us in government and saying this is a nightmare, and it's going to affect our investments in Europe. … they were facing a huge investment plus that there was a risk that the normal data that they needed to operate their business with subsidiary companies and so on, would be put in danger ... They thought it was a potential disaster. [[41]](#footnote-41)

Equally, the US administration was worried that new EU rules could strangle the nascent e-commerce sector at birth. US officials were convinced that government rules would have seriously damaging consequences for e-commerce, preventing it from experimenting with new business models and responding rapidly to changing circumstances. Magaziner and other Clinton administration officials had deliberately and specifically sought to shape policy debates so as to keep the government out of e-commerce regulation. They presented a “Framework for Global Electronic Commerce,” which was intended to lay down basic principles for both the US and EU, forestalling national regulatory initiatives except in highly sensitive areas such as child pornography.[[42]](#footnote-42) The EU’s new privacy rules presented a direct challenge to this program – they were both directly relevant to e-commerce and potentially highly restrictive.

This led to an initial war of words between the EU and US over whose rules should shape the transatlantic relationship, and, by extension, emerging business sectors such as e-commerce. Magaziner hoped in the short term to build a model of self-regulation that might diffuse internationally – in 1999 he predicted that “if the privacy protections (sic) by the private sector can be spread internationally, that will become the de facto way privacy is protected, and that will diffuse this disagreement.”[[43]](#footnote-43) However, even while Magaziner and an industry group, the Online Privacy Alliance, sought to convince EU regulators that self-regulation was viable, US businesses proved slow to sign up to self-regulation, eventually prompting the US administration to put pressure on the Better Business Bureau to set up a privacy certification regime. The European Union, for its part, continued to press for large scale regulatory change in the US.

The European side of the negotiations was conducted by officials from the Commission’s Directorate-General for the Internal Market. The US negotiations were led by the US Department of Commerce, occasionally consulting with the Department of the Treasury, the Federal Trade Commission, the US Trade Representative and the Office of Management and Budget via an inter-agency process.[[44]](#footnote-44) When the two sides began negotiating in 1998, neither side was especially optimistic of success. [[45]](#footnote-45) However, to the surprise of the negotiators, the parties reached agreement on a novel form of cooperation that became known as the Safe Harbor Agreement.[[46]](#footnote-46) Under the agreement firms register as participants and, in turn, agreed to comply with a set of basic privacy principles (known as the Safe Harbor Principles) similar to those contained in the EU privacy directive.[[47]](#footnote-47) These commitments were monitored and enforced by the Federal Trade Commission with input and participation of European data privacy authorities.

Importantly, Safe Harbor contained an exemption for national security issues, largely bracketing the issue. Moreover, given the quirks of US regulatory history, public sector bodies as well as a number of key sectors including telecommunications, finance, and aviation were excluded from the agreement as they did not fall under the jurisdiction of the FTC. As a result, many key sectors related to intelligence sharing were not directly affected by the agreement.

Safe Harbor quickly became a key means through which companies with large operations in the US engaged the transatlantic marketplace. By 2004, thousands of companies had signed on to the Safe Harbor.[[48]](#footnote-48) At the same time, the transatlantic digital market place grew exponentially.[[49]](#footnote-49) US firms benefited tremendously, with IT companies like Google and Facebook winning larger market shares in many European countries than they had in the US.

Safe Harbor was neither a traditional compromise solution nor the simple recognition of another country’s rules. Instead, it created standards by which European governments could be reasonably assured that global private companies were roughly following European standards as they processed data outside of Europe. At the same time, it did not require the US to change its domestic rules for privacy. Instead, it offered an interface through which the two jurisdictions mitigated transnational institutional differences, while providing a platform for the transatlantic market. It seemed as if policy makers on the two sides of the Atlantic could have their cake and eat it too, despite the frictions posed by overlapping rules and rising economic interdependence.

Despite the apparent elegance of the solution, it did not take long for critics to emerge. As social media services exploded and ever more amounts of data were collected, privacy advocates argued that US firms were not meeting Safe Harbor standards.[[50]](#footnote-50) And equally troubling, they argued that the process for redress was not transparent, as it was difficult for European citizens to bring complaints to the FTC. The French data privacy authority, for example, claims that many more complaints were brought to the FTC than the FTC acknowledges having received.[[51]](#footnote-51)

A series of public and private sector reviews of the agreement demonstrated a number of weaknesses in the agreement. A 2004 implementation study commissioned by the European Commission, for example, concluded that “Key concepts such as ‘US organization,’ ‘personal data’, and ‘deceptive practices’ lacked clarity. Moreover, the jurisdiction of the FTC with regard to certain types of data transfers was dubious.”[[52]](#footnote-52) The Safe Harbor Agreement faced increasing hostility within Europe, as scandals erupted over US-based IT firms. For example, Google’s monitoring of residential WiFi traffic, as its cars were imaging neighborhoods for its streetview service, caused considerable pushback in Europe.[[53]](#footnote-53)

Although privacy advocates in Europe became increasingly vocal as to their opposition towards Safe Harbor, they had difficulty in gaining traction vis-à-vis their governments. Through most of the 2000s, the European Commission continued to support the agreement leading to a generalized assumption that it would be maintained.[[54]](#footnote-54) Vivien Reding, EU Commission Vice-President and Justice Commissioner, made a forceful defense of the agreement in October 2012, concluding “Safe Harbor will stay.”

Despite the claim by U.S. observers that European privacy policy was a form of tacit protectionism, European policy-makers had much to lose from an end to Safe Harbor.[[55]](#footnote-55) Companies like Google, eBay, and Apple employ thousands of workers across Europe. Furthermore, important European firms conducting business with the US used Safe Harbor too, to handle e.g. transfers of employee data. Facing concerns about the rupture of Safe Harbor (described in more detail below), the European Commission (2013: 6-7) made the economic case for maintaining the agreement:

The Safe Harbour scheme is an important component of the EU-US commercial relationship, relied upon by companies on both sides of the Atlantic…

its revocation would adversely affect the interests of member companies in the EU and in the US. The Commission considers that Safe Harbour should rather be strengthened.

In conclusion, when privacy emerged as an important controversy in the EU-US relationship, it was firmly located in the commercial and economic issue space. The major international dispute turned on the question of whether government needed to regulate businesses in order to assure citizens’ privacy, or whether, alternatively, self-regulatory tools would suffice. The battle between the EU and the US over this question led to the creation of Safe Harbor, an arrangement that was intended specifically to defuse this controversy, by providing governments with a backstop role to mechanisms that primarily involved self-regulation and self-certification.

*The Changes after September 11*

The September 11, 2001 attack led to a swift and dramatic change in transatlantic debates over privacy. Specifically, it brought the relationship between state security and privacy to the center of debate, pushing earlier disputes about commercial access to private data to the side.[[56]](#footnote-56) By October 2001, President Bush had already written to the European Union, requesting that the EU “[c]onsider data protection issues in the context of law enforcement and counterterrorism imperatives” and engage in extensive information exchange on terrorist financing and law enforcement.[[57]](#footnote-57) These imperative requests went together with both declared and undeclared unilateral actions. The US swiftly passed legislation requiring that all airlines flying to the United States provide “Passenger Name Record” (PNR) data on the passengers on incoming flights, a demand which directly contravened European privacy law. The US also clandestinely started to require SWIFT, a Belgium-based private financial messaging consortium that plays a crucial role in international financial flows, to start providing it with information, again in breach of European privacy law.

These demands led to a complex reaction in Europe. Some – including privacy activists, many members of the European Parliament and specialized privacy officials – were indignant at what they saw as US unilateralism that trampled on the fundamental rights of European citizens.[[58]](#footnote-58) Others, including European security officials, were tacitly tolerant of US demands, and in some cases actively welcoming, seeing them as a means of weakening privacy protections that they themselves were impatient with.[[59]](#footnote-59)

Key officials in both the EU and US sought to insulate these controversies from the existing framework for commercial privacy. Initially, the officials charged with data protection in the European Commission’s Internal Market Directorate General moderated their response to US PNR demands, because they did not wish to be seen as hindering the fight against terrorism.[[60]](#footnote-60) These officials then found themselves gradually being sidelined from the negotiations.

We were under instructions in this particular DG to keep out of it as much as possible. We were not encouraged to be very forward. [[61]](#footnote-61)

In March 2005, data protection responsibilities were transferred away from DG Internal Market altogether, to the Directorate-General concerned with civil liberties and justice and home affairs. There, the key data protection dossiers were shifted to the units charged with policing and anti-terrorism cooperation.[[62]](#footnote-62) As a Commission data protection official described it, data protection was no longer an economic issue, but a security issue, which was downgraded as a priority and subordinated to the fight against terrorism.[[63]](#footnote-63)

Members of the European Parliament, and independent data protection commissioners remained committed to a more expansive vision of privacy. As the focus shifted to the relationship between privacy and security, their concerns gravitated away from worries of commercial abuses, and towards fears that fundamental civil rights were being breached. European concerns about privacy went hand-in-hand with fears about the excesses of US foreign policy and counter-terrorism policy.[[64]](#footnote-64) While they recognized the need for increased police cooperation, they wanted it to take place in the context of a traditional bilateral agreement, which would respect civil liberties.[[65]](#footnote-65) However, they soon found themselves shut out of negotiations.

Unfortunately, when the US started to put pressure on the European Union to deal with PNR questions, the Commission chose to approach it – I think under pressure from the member-states -- in a way that was not going to involve the European Parliament at all. They initially told us, in September of 2002, that they would give us...rights to sign off on the agreement. That was then withdrawn; then they decided on a different approach.[[66]](#footnote-66)

Parliamentary officials began to fear that they were being systematically cut out of European policy making, not only involving negotiations with the US, but also domestic security (which was handled under a different decision-making processes or ‘pillar’ of the European Union’s founding treaties, providing Parliament with only a minimal role).[[67]](#footnote-67)

Their fears were justified. In 2004, the European Parliament launched a court proceeding, with the support of the recently appointed European Data Protection Supervisor, to claw back influence over the PNR negotiations. This case was rebuffed by the European Court of Justice, which found that the agreement fell under the area of Justice and Home Affairs, rather than the area of market integration that the initial privacy directive had built upon.[[68]](#footnote-68) Under the EU’s complex legal regime, this meant that both the Parliament and European data protection officials were excluded from any real influence over these data sharing negotiations.[[69]](#footnote-69)

More broadly, as the EU and US began to engage on controversies such as PNR as well as less publicly visible issues such as border control and passports, they began to construct new networks of relations between security officials on both sides[[70]](#footnote-70), which played the crucial role in shaping a common agenda across both sides of the Atlantic. The so-called High Level Political Dialogue on Transportation and Border Security took over discussions on PNR and related problems. This network was specifically and deliberately constructed so as to exclude civil liberties advocates, allowing relatively like-minded officials to concentrate on pragmatic problem solving from a shared perspective that emphasized security.[[71]](#footnote-71) Not only diplomats, but also members of the European Parliament, European data protection officials and US privacy officials were cut out of the loop. The consequence was that “the security dimension dominated the discussion about the balance between security and civil liberties”,[[72]](#footnote-72) although network participants still had to pay some attention to outside actors such as the European Parliament and data protection authorities.

These security negotiations largely sidelined commerce interests as well. Business interests found it very difficult to exercise influence or even provide their perspective to officials and negotiators, except at occasional, largely stage managed public events. As described by one European airline industry official:

somehow at the European level, we are not [consulting with industry about the negotiations]. It’s not only an airline thing. I know from my colleagues representing the airports here in Brussels that they have not been consulted either. I know that a lot of human rights organizations have not been consulted either. I don’t understand to be quite honest. [[73]](#footnote-73)

Importantly, these security negotiations did not directly impinge upon the Safe Harbor arrangement, which officials depicted as covering a quite separate set of issues. Assessing the impact of US security legislation passed in the wake of the September 11, 2001 attacks on the Safe Harbor Agreement, an EU Commission implementation study concluded, “Since the new US legislation only rarely contradicts the SH principles for data covered by SH, these conflicts do not appear to undermine the level of protection for any significant flows of personal data to the United States. The controversial provisions of the USA PATRIOT ACT are essentially irrelevant for SH data flows.”[[74]](#footnote-74) As the Safe Harbor agreement contained an exemption for national intelligence activities, officials argued there was a barrier between the economics-focused agreement and routine surveillance policy. When the two occasionally impinged on each other, as when the SWIFT organization entered into the Safe Harbor after it had restructured its data flows, EU and US policy clearly distinguished between the commercial flows enabled by Safe Harbor, and the purportedly distinct question of government use of information from those flows, which fell under the entirely separate and inviolable area of security and policing cooperation.

In negotiations, the officials on both sides of the table were not charged with representing business interests, nor especially concerned by them. A switch occurred from DG internal market and the US Commerce department to interior ministers and the Department of Homeland Security and the Department of Treasury. Notably, the Treasury officials concerned were those like Stuart Levey, whose mandate involved security questions such as sanctions enforcement, rather than general economic questions and management of financial flows. Treasury saw substantial internal changes during this period, retaining and over time expanding a set of capacities that were employed directly for intelligence and security enforcement purposes.[[75]](#footnote-75)

In time, the High Level Dialogue paved the way for a more expansive High Level Contact Group, initiated in November 2006, to allow senior EU and US security officials to confer, identify and resolve potential problems in the policy process before they broke out into overt conflict, and spur more general cooperation on security questions. Europeans hoped that this Group could pave the way to a broader agreement, while the US simply wanted to avoid roadblocks and deliver concrete and specific forms of cooperation. The US also used the Group as a way to influence internal EU deliberations among member states in the Council and elsewhere.

The Group issued its first report in May 2008[[76]](#footnote-76), which was followed up by an addendum in October 2009[[77]](#footnote-77). While it set out a series of principles aimed at alleviating conflict, it had difficulty in defining what these principles meant in concrete terms, failing to agree on whether “law enforcement” extended to national security as well as criminal investigations (the US pushed for the less restrictive definition), and not reaching any resolution on the question of how EU citizens might receive redress for violation of their rights by US authorities. While the US wanted redress to be purely administrative, the EU pushed for enforceable legal rights. Apart from these ambiguities, the principles encountered skepticism from outside officials, who had not been consulted.[[78]](#footnote-78) However, they provided some impetus to security officials to continue to negotiate in the hope that they could create a so-called ‘umbrella agreement’ on law enforcement and privacy, that would provide a general template for public sector data exchanges.[[79]](#footnote-79)

Thus, the period from 2001 to 2012 saw a dramatic change in how privacy was treated in EU-US dialogue. Specifically, it was transformed from a commercial issue of market completion, to a security issue. Forms of exchange that were previously commercial in nature, such as airline flight information and SWIFT financial messaging, were leveraged for security purposes. However, in terms of policy, security and intelligence use of this information was insulated from the previously existing arrangement governing commercial data exchange, Safe Harbor.

This redefinition of the policy question went hand in hand with a change in the issue space and associated forms of influence. Notably, in contrast to the emphasis of conventional issue linkage accounts, states sought to make a deal easier to reach by decoupling security from economics, rather than treating them as a package. Privacy ceased to be dealt with by the commerce-friendly Directorate-General on the Internal Market, and was taken over instead by security officials with a very different mandate. EU justice officials, together with their US counterparts in the Departments of Homeland Security and Treasury not only prioritized security, but took advantage of the sensitivity of negotiations specifically to exclude actors, whether governmental or business, that associated privacy with different issues. The High Level Contact Group was both largely insulated from other parts of the governmental frameworks involved, and highly secretive, resulting in complaints e.g. from some member states that it was not responsible to them. In short, two parallel but distinct systems developed for transatlantic data sharing – one covering commercial data and another for intelligence sharing.

**Snowden Affair Crosses the Commercial and Security Policy Streams**

In 2013, the data privacy debate took a new turn thanks to the revelations made by Edward Snowden. A former national security employee and contractor with access to top secret documents, Snowden released information to the world about a number of National Security Agency surveillance programs. These revelations documented how the US national intelligence community monitored electronic communication in the US and globally.

The most important consequence of these revelations for EU-US relations was that they potentially highlighted new linkages between flows of commercial information and national security.[[80]](#footnote-80) European civil liberty groups were especially troubled by the NSA’s PRISM program. Under this program, the NSA was able to monitor the Internet traffic of many of the largest IT companies and had access to a significant amount of data maintained by the companies. While the US administration argued that use of the data was limited to targeted searches, many feared that the program included bulk collection, leading to much controversy, especially given the non-intuitive ways in which terms like targeting were used by the US intelligence community. Equally troubling, IT companies claimed that they had no knowledge of the data collection, leading to allegations that the NSA had direct access to the physical networks underlying the Internet.

The evidence suggests that US intelligence was accessing data flows both within and outside the US. However, it was the former that caused particular political concern, even if it was possibly less invasive (the rules covering domestic information gathering are potentially more onerous). The reason was that US access implied that data which had traveled to the US could be used in ways that violated the privacy of EU citizens. Paradoxically, it was more difficult for EU actors who were dissatisfied with the post September 11 security arrangements to address surveillance activities within the European Union than outside it. Surveillance by European states fell outside the European Union’s Treaties,[[81]](#footnote-81) while US surveillance was conventional espionage and hence not protected by law. However, if surveillance used data that had left the EU and entered the US through commercial channels, there was a possible opening to be exploited. Two European Commission studies tasked with evaluating the Snowden documents found that US government agencies had wide spread access to the personal information of European citizens stored on the databases of US companies.[[82]](#footnote-82) Additionally, they found that European citizens have no clear mechanism to seek redress for any possible abuse of the use of such data.

This had implications for Safe Harbor. In sharp contrast to its previous findings about the irrelevance of US surveillance after September 11, the European Commission was obliged to conclude (2013: 6) that “Safe Harbour also acts as a conduit for the transfer of the personal data of EU citizens from the EU to the US by companies required to surrender data to US intelligence agencies under the US intelligence collection programmes.”

It also created a clear and dramatic change in publicly available knowledge. Previously, there had been no effective basis for challenging information exchange between the EU and US. Now, the Snowden revelations highlighted how this commerical exchange facilitated broad scale surveillance. Peter Schaar (2015), the former federal data protection commissioner of Germany, argued that the Snowden revelations injected security concerns directly into Safe Harbor in a way that was likely not considered during the initial negotiations or the later assessments.

At the first glance, law enforcement authorities, police and intelligence do not fall within the scope of the Safe Harbor agreement and therefore they do not have to be subject to the assessment. But this first impression is wrong. As Art. 25 of the GD [Privacy Directive] is pointing out, the assessment is to be done in the light of “all circumstances” surrounding a data transfer to the third country. Even activities of authorities in the third country have to be examined. It is unclear how far this happened during the Safe Harbor assessment in the late 1990s.

But even if such assessment once took place, the result may be invalid today, because things changed dramatically after 9/11 2001. As we have learnt from Edward Snowden and other whistleblowers, US government has obtained broad access to private companies’ databases, telecommunications and Internet services.

The Snowden documents, then, created new knowledge that potentially allowed actors to create links between two issue areas that EU and US authorities had previously been at pains to keep distinct – commercial data transfers, which had become more or less routinized via Safe Harbor and other means, and the highly political and volatile national security and privacy issues centered on the sharing of national intelligence information.

**The Schrems Case and the Unraveling of the Transnational Agreement**

This new knowledge then created an opportunity for entrepreneurial issue linkage. European privacy advocates, who had previously been stymied in their efforts to push back against national security encroachments and to disrupt or reform the Safe Harbor Agreement, found new ammunition in the Snowden documents. In particular, they turned to domestic institutions, including courts and regulators, to press their case that the Safe Harbor provided insufficient protection of the civil liberties of European citizens.

Issue linkage between economics and security was vital. It allowed them both to argue that existing remedies were grossly inadequate – how could the FTC monitor the NSA, when it has no jurisdiction over public sector actors? – and that the commitments made in Safe Harbor not to share data broadly were hollow. By linking the two domains, they could exploit opportunity structures that had been inaccessible in the past. Specifically, they were able to bring a plausible case to the European Court of Justice, which had no direct authority over intelligence surveillance and national security, but did have jurisdiction over economic markets and privacy rights.[[83]](#footnote-83) In short, the issue linkage coupled the high-politics domain of intelligence, where states and security officials in the Council had previously enjoyed considerable discretion, with the low-politics domain of economic issues, where the Court had far greater institutional power, to the detriment of member state discretion.

The key entrepreneurial move was made by Max Schrems, a young Austrian lawyer and privacy advocate who had previously served as a thorn in Facebook’s side. When Schrems heard about the Snowden revelations, he soon realized that there was a plausible case that Facebook, by transporting users’ information from the EU to the US, was in violation of European law. In his words:

I thought that’s actually something where Europe has jurisdiction, since this mass surveillance only works in public-private partnership, because the NSA’s not going to be in every phone … you actually have a point where you can actually hit them, where you have jurisdiction and at least a remote possibility that someone could possible care about it.[[84]](#footnote-84)

He initially sought relief from Ireland’s data protection agency, which supervised Facebook and other major US e-commerce firms, which based their European operations in Dublin in part to take advantage of Ireland’s relaxed approach to privacy regulation. When the Irish data protection agency denied him relief, claiming that it did not have authority to revisit the European Commission’s Safe Harbor’s adequacy decision, he appealed to Ireland’s High Court.

Schrems’ framing, which treated economic relations under their security aspect, worked. In the preliminary judgment offered by Ireland’s high court as it referred the matter to the European Court of Justice, the Irish court concluded “The Snowden revelations demonstrate a massive overreach of the security authorities, with an almost studied indifference to the interests of ordinary citizens. Their data protection rights have been seriously compromised by mass and largely unsupervised surveillance programmes.” Similarly, the European Court in its ruling directly tied the fate of the Safe Harbor program to the blurring of private sector data collection and public surveillance in the United States, concluding:

national security, public interest and law enforcement requirements of the United States prevail over the safe harbour scheme, so that United States undertakings are bound to disregard, without limitation, the protective rules laid down by that scheme where they to conflict with such requirements. The United States safe harbour scheme enables interference, by United States public authorities, with the fundamental rights of persons…

Importantly, the Court found that the oversight requirements agreed to in the Safe Harbor agreement could not be met because of the institutional mismatch – the FTC lacks jurisdiction over public sector actors conducting the surveillance. At the same time, the Court found that the extent of data collection by private sector actors went far beyond anything allowed in EU law. The advocate general to the Court (2015: 19), in his preliminary ruling stressed the role that Schrems’ leveraging of new knowledge played in activating the Court’s attention:

In view of the fact that an adequacy decision is a particular type of decision, the rule that its validity might be assessed only by reference to the factors that existed at the time of its adoption must be qualified in this instance. Otherwise, such a rule would have the consequence that, a number of years after an adequacy decision has been adopted, the assessment of validity that the Court must carry out cannot take into account events that have occurred subsequently, even though there is no limit on the period within which a reference for a preliminary ruling on validity may be made and it may be prompted specifically by subsequent facts that reveal the deficiencies of the act in question.

Hence, the Snowden documents created a window of opportunity for European privacy advocates to link commercial activity to surveillance, and hence to activate domestic institutions like the European Court of Justice so as to undermine the legitimacy of the transnational agreement. The linkage between the two issue areas was crucial. Without the economic basis of Safe Harbor, the European Court of Justice would not have had jurisdiction to rule on information sharing arrangements. Without the evidence of national security surveillance, the Court would not have had sufficient motivation to unravel Safe Harbor and hence challenge EU-US information exchange.

At the same time, the European Court of Justice created new and additional hurdles for intelligence sharing. The original Safe Harbor agreement contained standard language that exempted ‘necessary’ law enforcement and intelligence sharing activity. In the decision, however, the Court ruled that this exemption does not trump European law or fundamental rights. In particular, the Court stressed that third countries must guarantee that they have equivalent data protection policies in place through their domestic law. More specifically, exemptions for national security must still meet key privacy principles such as the proportionality of data collected and the clear ability to remedy abuse. As the Court (2015; 25) concludes,

…protection of the fundamental right to respect for private life at EU level requires derogations and limitations in relation to the protection of personal data to apply only in so far as is strictly necessary…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, as guaranteed by Article 7 of the Charter…Likewise, legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data, does not respect the essence of the fundamental right to effective judicial protection, as enshrined in Article 47 of the Charter.

In short, the Court decision narrowed the window of acceptable exemptions for national security purposes and at the same time increased the scope of its own purview over such issues.

The European Court of Justice decision has further empowered the Court and European data privacy authorities to scrutinize adequacy decisions pertaining to third countries. Prior to the Court decision, the Commission would evaluate the privacy protections of other countries, receive input from data privacy authorities, and make an adequacy decision. All actors had hitherto assumed that these decisions were binding and that other institutional actors could not challenge them. The Court ruled that even after the negotiation of such agreements, citizens can bring complaints to data privacy authorities regarding the legitimacy of international data transfers. In the Court (2015: press release)’s words “the existence of a Commission decision finding that a third country ensures an adequate level of protection of the personal data transferred cannot eliminate or even reduce the powers available to the national supervisory authorities under the Charter of Fundamental Rights of the European Union and the directive.” Moreover, it made clear that the Court and not the Commission is the ultimate arbiter of such decision, “It is thus ultimately the Court of Justice which has the task of deciding whether or not a Commission decision [concerning third country adequacy] is valid.”

**A New Negotiation Dynamic**

The ECJ decision sent a shock wave through the transatlantic market as it established a new reversion point, creating uncertainty as to the legitimacy of data transfers outside of the EU absent some compromise. U.S. Commerce Secretary Penny Pritzker warned that the dispute could “put at risk the thriving transatlantic digital economy”, costing U.S. firms billions. Without a diplomatic solution, there exists a real possibility that personal data would have to be quarantined within Europe. Microsoft president, Brad Smith, feared that such fragmentation of the Internet threatens a “digital dark ages”, which could undermine digital services ranging from payment systems to airline reservations. Alphabet (the new parent company of Google) Chairman, Eric Schmidt, went so far as to claim that the dispute put in jeopardy “one of the greatest achievements of humanity”. While these warnings were perhaps hyperbolic, they were to some extent borne out by the immediate response of the newly empowered data privacy authorizes, who gave EU-US negotiators a four-month reprieve before they pledged to start enforcing European privacy laws. Business pressed urgently for a solution, arguing for a revamped Safe Harbor. It also pushed the US to accelerate the necessary legislation, the so-called Judicial Redress Act, that was required for the Umbrella Agreement to come into force (see below).

EU-US negotiators looked to rebuild the institutional status quo ante to the ECJ decision as best as they could. Facing the impending deadline of regulatory enforcement, they released the EU-US Privacy Shield on February 2, 2016.[[85]](#footnote-85) In some respects, the deal provided a more substantial institutional backstop to Safe Harbor. It provided a more transparent and robust monitoring and enforcement regime for transatlantic data transfers, gave European data privacy authorities the authority to follow up unresolved complaints with the FTC and the Department of Commerce, and put in place clear sanctions for non-compliance as well as a dispute settlement mechanism.

However, it failed to provide robust institutional changes that would meet the challenges raised by the Snowden documents and the Schrems decision, which centered on the access of public agencies to private sector data. The negotiating parties on the US side - the Department of Commerce and FTC - do not have direct authority to monitor or oversee the actions of national intelligence authorities. While intelligence officials, including Bob Litt, the General Counsel of the Director for National Intelligence, explained the operation of the US national intelligence system, and provided broad assurances, the concrete reforms to intelligence operations offered were relatively modest, consisting of some promised limitations on access of US agencies to transferred data, and an ombudsperson in the US Department of State who could review complaints about intelligence uses of data provided under Safe Harbor.

Despite these new safeguards, national security and economic policy have become linked in ways that empower the actors who were previously cut out of transatlantic information exchange, making it very difficult to cement these new arrangements. In April 2016, the Article 29 Working Party, which represents the Europe-wide network of data privacy authorities that oversee European privacy policy, released a statement regarding the deficiencies of the proposed Privacy Shield.[[86]](#footnote-86) On the one hand, they criticized the proposed redress and transparency mechanisms for the private sector as too vague, putting pressure on the Commission to further strengthen the monitoring and enforcement of the private sector over and above the original Safe Harbor. On the other, they cast doubt on the new safeguards against security abuses. Here they focused on the fact that the commitments offered by national security officials are voluntary rather than legally binding (e.g. the Director of National Intelligence’s pledge to limit mass surveillance) and that the independence of the proposed ombudsperson is questionable. These sentiments have been echoed by privacy advocates, who have pledged to file additional suits against the legitimacy of the Shield. Max Schrems, who brought the original Safe Harbor case, warned, “with all due respect, but a couple of letters by the outgoing Obama administration is by no means a legal basis to guarantee the fundamental rights of 500 million European users in the long run”. Jan Philipp Albrecht, a German member of the European Parliament and strong privacy advocate, concluded “The new Privacy Shield framework appears to amount to little more than a re-marketed version of the pre-existing safe harbor decision, offering little more than cosmetic changes.” Peter Swire, who assisted in the negotiation of the original Safe Harbor Agreement for the US, has concluded, “I’m convinced the new agreement will face legal challenges.” On May 30, 2016, the European Data Protection Supervisor, Giovanni Buttarelli, concluded “the Privacy Shield as it stands is not robust enough to withstand future legal scrutiny before the Court. Significant improvements are needed should the European Commission wish to adopt an adequacy decision, to respect the essence of key data protection principles with particular regard to necessity, proportionality and redress mechanisms. Moreover, it’s time to develop a longer term solution in the transatlantic dialogue.”[[87]](#footnote-87) In short, the institutional footing of the transnational agreement has shifted as the linking of security and economic policy has opened up new channels for non-state actors like privacy advocates to shape the negotiations.

Perhaps equally important, the issue linkage between economic and security issues has motivated reform of domestic US law. A key issue raised by the Court in the Schrems’ decision is the lack of judicial redress for European citizens, who suffer because of data sharing with public sector bodies. The US Privacy Act, which was enacted in 1974 as the primary privacy legislation in the US covering the data collection and usage policies of the federal government, explicitly exempts non-US citizens from its protections. The legislative history actually identifies national security and intelligence sharing as the justification to "exempt [from] the coverage of the bill intelligence files and data banks devoted solely to foreign nationals or maintained by the State Department, the Central Intelligence Agency and other organizations for the purpose of dealing with nonresident aliens and people in other countries.”[[88]](#footnote-88) This distinction, however, is out of step with much European legislation, which applies to both citizens and non-citizens, and more important makes it hard for the US to maintain that its privacy protections provide adequate cover for Europeans. Despite the fact that Europeans have been calling for the extension of the Privacy Act since the 1980s, the US government has long resisted such efforts, which would ultimately require legislative action.[[89]](#footnote-89)

The Schrems decision, by linking economic interests and security interests, altered the political dynamic. In particular, it meant that the US tech industry’s ability to obtain a successful commercial data sharing agreement relied in part on US government policy and its reform of the Privacy Act.

This spurred momentum for the long stalled Judicial Redress Act, which was supposed to activate the Umbrella Agreement and extend some of the protections of the Privacy Act to non-citizens. A group of nearly two dozen US tech firms including Apple, Facebook, Google, and Microsoft lobbied collectively in support of the reform.

The last two years have seen a significant erosion of global public trust in both the U.S. government and the U.S. technology sector. The judgment of the Court of Justice of the European Union last week to invalidate the European Commission’s adequacy decision regarding the U.S.-EU Safe Harbor agreement confirms a trust deficit persists between the U.S. and the European Union (EU). Prior to the decision, this degradation of trust had already translated into significant negative commercial consequences for U.S. firms. After the decision, the commercial consequences could become even more significant by further undermining the ability of U.S. companies to engage in business with EU companies and consumers. Without the adequacy finding, many of the 4,400 companies that relied solely upon the Safe Harbor agreement to transfer data from the EU to the United States face tremendous uncertainty regarding what bases exist to justify transatlantic flows of data.

The enactment of the Judicial Redress Act is a critical step in rebuilding the trust of citizens worldwide in both the U.S. government and our industry and in addressing the misperceptions underlying the decision.[[90]](#footnote-90)

Fourteen days after the Schrems’ decision, on October 20th 2015, the US House of Representatives passed the Judicial Redress Act on a voice vote. In a clear signal of the linking of domestic reform to the transatlantic dispute, the Senate adopted its version on February 9th, 2016, seven days after the announcement of the EU-US Privacy Shield and President Obama signed the legislation later that month.[[91]](#footnote-91) However, the final version of the Act made US granting of Privacy Act protection to foreign citizens conditional on their states maintaining flows of commercial data, linking the provision of rights against national security and policing agencies to continued economic cooperation.

At the same time, US and European privacy NGOs have leveraged the issue linkage to push for domestic privacy reform in the US for the commercial sector as well. Since the passage of the Privacy Act, the private sector in the US has largely been governed through industry self-regulation (aside from a few sensitive sectors like health care and finance). In 2015, the Obama administration proposed creating national rules for the private sector, under the Consumer Privacy Bill of Rights Act. Based on similar principles to those used in European privacy law, the legislation would make significant step towards creating more equivalent rules between the two jurisdiction. In November 2015, a transnational alliance of over thirty civil liberties organizations wrote an open letter to the US Secretary of Commerce calling for the adoption of a strong version of the Consumer Privacy Bill of Rights, justifying its argument by directly citing the Schrems decision:

…the Court’s opinion is key to understanding why the United States must update domestic privacy law for transborder data flows to continue. The Court says directly “It is clear from the express wording of Article 25(6) of Directive 95/46 that it is the legal order of the third country covered by the Commission decision that must ensure an adequate level of protection.” Acknowledging that systems of law may vary, the Court concludes, “those means must nevertheless prove, in practice, effective in order to ensure protection essentially equivalent to the guaranteed within the European Union.”…

The intent is clear: the evaluation of adequacy of data transfers to the United States going forward will be based on the domestic law and international commitment of the United States…

A Revised Safe Harbor framework similar to the earlier Safe Harbor framework will almost certainly be found invalid by the national data protection agencies and ultimately by the CJEU. In a recent communication the Commission also acknowledges that it must ensure that “a new arrangement for transatlantic transfers of personal data fully complies with the standard set by the Court.” It is impossible to ignore that the Schrems decision requires necessary changes in the “domestic law” and ‘international commitments.”

While the Consumer Privacy Bill of Rights is still at the initial stage of its legislative history, non-state actors are clearly looking to take advantage of the issue linkage between economic and security issues to press not only for changes in the negotiating dynamic at the international level but for policy change at the domestic level as well.

Thus, in conclusion, the combination of new knowledge (released via the Snowden revelations) and entrepreneurial issue linkage has had transformative consequences for privacy protection. European privacy advocates, by undermining Safe Harbor, have fused together commercial and security issue areas that were previously quite discrete. This has in turn reshaped the politics of transatlantic data sharing, by allowing both European judges and data protection authorities to leverage their authority over economic transfers to exert powerful influence over national security arrangements that were previously inaccessible to them. Furthermore, it has led the US Congress to condition cooperation on arrangements intended to bridge security and privacy on continued flows of purely commercial data. These new politics make it effectively impossible for national security actors to continue the isolation between security and economic affairs that they had previously maintained, with potential consequences not only for the transatlantic relationship, but for domestic politics within the EU and US.

**Conclusion**

Cross-border flows of goods, people, and information increasingly erode the barriers between traditional economic and security issues. Despite the recognition that this processes of ‘complex interdependence’ might affect and be affected by linkage politics, most existing work has taken a strikingly statist view of how issues become politically embroiled with each other.[[92]](#footnote-92)

In this paper, we look to rectify this narrow view of linkage politics by offering a novel argument regarding how non-state actors may transform international negotiations. In particular, we focus on the conditions under which such non-state actors may matter by focusing on the heterogeneity in political discretion accorded to relevant actors across issue areas. Our argument shows how non-state actors may disrupt the political status quo by coupling issue areas in ways that activate new political constraints on more traditional diplomatic actors. Our detailed case study of transatlantic data transfers offers important initial evidence as to the plausibility of our argument. In order to push this research agenda further, more evidence will be needed from other issue areas to adjudicate the broader generalizability of the finding, and to test how well variation in initial conditions (e.g. extent of heterogeneity; different incentives of state and non state actors) match with the expected variations in outcome. That said, we expect the argument to travel to a wide-range of topics from money laundering to counter-terrorism to corruption.

Equally, our argument has broader critical implications for research on international relations. For one, building on suggestions articulated in Farrell and Newman (2014), it illustrates the limits of approaches that emphasize snapshot aspects of negotiations. Much work on negotiations – arguably the vast majority of it – seeks to elucidate the factors leading to an equilibrium outcome i.e. an ‘agreement’. Yet this fundamentally underplays the dynamics of negotiations, which tend typically not to produce equilibria, but instead new situations of continued contention. Agreements such as Safe Harbor do not eliminate politics so much as create new political struggles with associated frictions among states and other actors, which are often both unforeseen and unintended, as well as new tools that actors try to employ to resolve those frictions to their advantage. Our analytic narrative demonstrates the importance of taking this over-time view of negotiations that demonstrates the ways in which agreements do not simply resolve political conflict but rebalance them.

Second, we translate and incorporate a key concept from comparative politics to international relations – how forms of decision-making vary across issue areas in ways that have demonstrable political consequences. While IR has focused on the role of domestic politics, it has tended to pay most of its attention to differences in regime type. Our work – together with that of others – suggests that accounts of variation in domestic politics need to be more finegrained still. Work in comparative politics, for example, demonstrates how federalism, administrative delegation, or judicial jurisdiction may shape policy differently across issue areas. Our findings should help spur IR scholars to take up this insight across a range of debates.

Third, we push forward work on the role of non-state actors in diplomacy. There has been a growing literature that acknowledges the role of such actors in global politics. That said, this work is often largely descriptive in nature without setting out boundary conditions, and thus opening itself up to attack by skeptics. In this article, we hope to better specify the conditions under which transnational actors may shape global negotiations, creating initial foundations for future research to explore other possible scope conditions for such influence.

Finally, we hope to call attention to the critical empirical domain of information sharing. Whether by firms or governments, organizations increasingly move data across borders. That said, relatively little work in international relations focuses on these relationships. Given the prominence of and fallout associated with scandals such as Wikileaks, the Snowden Affair, or the Panama papers, it is time for international relations to engage with the deep interlinkages between security and economy in an age of complex governance.

**Bibliography**

Abbott, Kenneth W., Jessica F. Green, and Robert O. Keohane. 2016. “Organizational Ecology and Institutional Change in Global Governance.” *International Organization* 70 (2): 247–277. doi:10.1017/S0020818315000338.

Aldrich, R. 2004. “Transatlantic Intelligence and Security Cooperation.” *International Affairs* 80 (4): 731–53.

Avant, Deborah, Martha Finnemore, and Susan Sell. 2010. “Who Governs the Globe?” *Cambridge University Press*. http://www.cambridge.org/us/academic/subjects/politics-international-relations/international-relations-and-international-organisations/who-governs-globe.

Avant, Deborah, and Oliver Westerwinter, eds. 2016. *The New Power Politics: Networks and Transnational Security Governance*. 1 edition. New York, NY: Oxford University Press.

Axelrod, Robert, and Robert O. Keohane. 1985. “Achieving Cooperation under Anarchy: Strategies and Institutions.” *World Politics* 38 (1): 226–254. doi:10.2307/2010357.

Bach, D., and A. Newman. 2007. “The European Regulatory State and Global Public Policy: Micro-Institutions and Macro-Influence.” *Journal of European Public Policy* 16 (4): 827–46.

Baker, Stewart A. 2013. *Skating on Stilts: Why We Aren’t Stopping Tomorrow’s Terrorism*. Hoover Press.

Bennett, C. 2008. *Privacy Advocates*. Boston: MIT University Press.

Bensahel, N. 2003. *The Counterterror Coalitions: Cooperation with Europe, NATO, and the European Union*. Santa Monica: RAND.

Bicchi, Federica. 2014. “Information Exchanges, Diplomatic Networks and the Construction of European Knowledge in European Union Foreign Policy.” *Cooperation and Conflict* 49 (2): 239–59. doi:10.1177/0010836713482871.

Bob, Clifford. 2005. *The Marketing of Rebellion: Insurgents, Media, and International Activism*. Cambridge University Press.

Boyle, David C. 1989. “Proposal to Amend the United States Privacy Act to Extend Its Protections to Foreign Nationals and Non-Resident Aliens.” *Cornell International Law Journal* 22: 285.

Carpenter, R. Charli. 2011. “Vetting the Advocacy Agenda: Network Centrality and the Paradox of Weapons Norms.” *International Organization* 65 (1): 69–102. doi:10.1017/S0020818310000329.

Cerny, Philip G. 2000. “The New Security Dilemma: Divisibility, Defection and Disorder in the Global Era.” *Review of International Studies* 26 (4): 623–646. doi:null.

———. 2010. *Rethinking World Politics: A Theory of Transnational Neopluralism*. Oxford University Press.

Colgan, Jeff D. 2010. “Oil and Revolutionary Governments: Fuel for International Conflict.” *International Organization* 64 (4): 661–694. doi:10.1017/S002081831000024X.

Davis, Christina L. 2004. “International Institutions and Issue Linkage: Building Support for Agricultural Trade Liberalization.” *The American Political Science Review* 98 (1): 153–69.

———. 2009. “Linkage Diplomacy: Economic and Security Bargaining in the Anglo-Japanese Alliance, 1902–23.” *International Security* 33 (3): 143–79. doi:10.1162/isec.2009.33.3.143.

Dewey, John, and Melvin L. Rogers. 2012. *The Public and Its Problems: An Essay in Political Inquiry*. Penn State Press.

Farrell, H. 2003. “Constructing the International Foundations of E-Commerce: The EU-US Safe Harbor Arrangement.” *International Organization* 2: 277–306.

Farrell, Henry, and Abraham Newman. 2015. “The New Politics of Interdependence Cross-National Layering in Trans-Atlantic Regulatory Disputes.” *Comparative Political Studies* 48 (4): 497–526. doi:10.1177/0010414014542330.

Farrell, Henry, and Abraham L. Newman. 2014. “Domestic Institutions beyond the Nation-State: Charting the New Interdependence Approach.” *World Politics* 66 (2): 331–63. doi:10.1017/S0043887114000057.

George, A., and A. Bennett. 2005. *Case Studies and Theory Development in the Social Sciences*. Cambridge: MIT Press.

Green, Jessica F. 2013. *Rethinking Private Authority: Agents and Entrepreneurs in Global Environmental Governance*. Princeton University Press.

Haas, Ernst B. 1980. “Why Collaborate? Issue-Linkage and International Regimes.” *World Politics* 32 (3): 357–405. doi:10.2307/2010109.

———. 1991. *When Knowledge Is Power: Three Models of Change in International Organizations*. University of California Press.

Haas, P. 1992. “Introduction: Epistemic Communities and International Policy Coordination.” *International Organization* 46 (1): 1–35.

Hafner, Katie, and Matthew Lyon. 1998. *Where Wizards Stay Up Late: The Origins Of The Internet*. Simon and Schuster.

Hale, Thomas, and David Held. 2011. *Handbook of Transnational Governance*. Polity.

Hameiri, Shahar, and Lee Jones. 2013. “The Politics and Governance of Non-Traditional Security1.” *International Studies Quarterly* 57 (3): 462–73. doi:10.1111/isqu.12014.

Hofheinz, Paul, and Michael Mandel. 2015. “Uncovering the Hidden Value of Digital Trade.” Lisbon Council.

Johnson, Tana, and Johannes Urpelainen. 2012. “A Strategic Theory of Regime Integration and Separation.” *International Organization* 66 (4): 645–677. doi:10.1017/S0020818312000264.

Jupille, J. 1999. “The European Union and International Outcomes.” *International Organization* 53 (2): 409–21.

Jupille, Joseph. 2012. “Procedural Politics: Issues, Influence, and Institutional Choice in the European Union.” *Cambridge University Press*. http://www.cambridge.org/us/academic/subjects/politics-international-relations/comparative-politics/procedural-politics-issues-influence-and-institutional-choice-european-union.

Kahler, M. 2009. *Networked Politics: Agency, Power, and Governance*. Ithaca: Cornell University Press.

Kahler, M., and D. Lake. 2003. *Governance in a Global Economy: A Political Authority in Transition*. Princeton: Princeton University Press.

Kaldor, Mary. 2013. *Global Civil Society: An Answer to War*. John Wiley & Sons.

Kaunert, Christian. 2010. “The External Dimension of EU - Counter-Terrorism Relations: Competences, Interests, and Institutions.” *Terrorism and Political Violence* 22 (1): 41. doi:10.1080/09546550903409551.

Keck, Margaret E., and Kathryn Sikkink. 1999. “Transnational Advocacy Networks in International and Regional Politics.” *International Social Science Journal* 51 (159): 89–101. doi:10.1111/1468-2451.00179.

Keck, M., and K. Sikkink. 1998. *Activists Beyond Borders: Advocacy Networks in International Politics*. Ithaca: Cornell University Press.

Keohane, R., and J. Nye. 1998. “Power and Interdependence in the Information Age.” *Foreign Affairs*, no. September/October: online.

Keohane, Robert O., and Joseph S. Nye. 1987. “Power and Interdependence Revisited.” *International Organization* 41 (4): 725–753. doi:10.1017/S0020818300027661.

Kerry, Cameron. 2014. “Missed Connections: Talking With Europe About Data, Privacy, And Surveillance.” Brookings Institution.

Khagram, Sanjeev, James V. Riker, and Kathryn Sikkink. 2002. *Restructuring World Politics: Transnational Social Movements, Networks, and Norms*. U of Minnesota Press.

Kobrin, S. 2004. “Safe Harbours Are Hard to Find: The Trans-Atlantic Data Privacy Dispute, Territorial Jurisdiction and Global Governance.” *Review of International Studies* 30: 111–31.

Long, J.W., and M.P. Quek. 2002. “Personal Data Privacy Protection in and Age of Globalization: The US-EU Safe Harbor Compromise.” *Journal of European Public Policy* 9 (3): 325–44.

Mahoney, J. 2003. “Strategies of Causal Assessment in Comparative Historical Analysis.” In *Comparative Historical Analysis in the Social Sciences*, edited by J. Mahoney and D. Rueschemeyer. Cambridge: Cambridge University Press.

McKibben, Heather Elko. 2010. “Issue Characteristics, Issue Linkage, and States’ Choice of Bargaining Strategies in the European Union.” *Journal of European Public Policy* 17 (5): 694–707. doi:10.1080/13501761003748682.

———. 2013. “The Effects of Structures and Power on State Bargaining Strategies.” *American Journal of Political Science* 57 (2): 411–27. doi:10.1111/j.1540-5907.2012.00628.x.

Meunier, S. 2005. *Trading Voices: The European Union in International Commercial Negotiations*. Princeton: Princeton University Press.

Mitchell, Sara McLaughlin, and Emilia Justyna Powell. 2011. *Domestic Law Goes Global: Legal Traditions and International Courts*. Cambridge University Press.

Monar, Jorg. n.d. “The EU as an International Actor in the Domain of Justice and Home Affairs.” *European Foreign Affairs Review* 9: 395–415.

Morrow, James D. 1992. “Signaling Difficulties with Linkage in Crisis Bargaining.” *International Studies Quarterly* 36 (2): 153–72. doi:10.2307/2600879.

Newman, A. 2008a. “Building Transnational Civil Liberties: Transgovernmental Entrepreneurs and the European Data Privacy Directive.” *International Organization* 62 (1): 103–30.

———. 2008b. *Protectors of Privacy: Regulating Personal Data in the Global Economy*. Ithaca: Cornell University Press.

ORREN, KAREN, and STEPHEN SKOWRONEK. 1996. “INSTITUTIONS AND INTERCURRENCE: THEORY BUILDING IN THE FULLNESS OF TIME.” *Nomos* 38 (January): 111–46.

Pawlak, Patryk. 2009. “Network Politics in Transatlantic Homeland Security Cooperation.” *Perspectives on European Politics and Society* 10 (4): 560–81. doi:10.1080/15705850903314833.

———. 2010. “Transatlantic Homeland Security Cooperation: The Promise of New Modes of Governance in Global Affairs.” *Journal of Transatlantic Studies* 8 (2): 139–57. doi:10.1080/14794011003760277.

Pearce, G.a.P. 1998. “Achieving Personal Data Protection in the European Union.” *Journal of Common Market Studies* 36 (4): 529–47.

Pierson, P. 2006. “Public Policies as Institutions.” In *Rethinking Political Institutions*, edited by I. Shapiro, S. Skowronek, and D. Galvin. New York: NYU Press.

Poast, Paul. 2012. “Does Issue Linkage Work? Evidence from European Alliance Negotiations, 1860 to 1945.” *International Organization* 66 (2): 277–310.

———. 2013. “Can Issue Linkage Improve Treaty Credibility? Buffer State Alliances as a ‘Hard Case.’” *Journal of Conflict Resolution* 57 (5): 739–64. doi:10.1177/0022002712449323.

Porta, Donatella della, and Sidney Tarrow. 2004. *Transnational Protest and Global Activism*. Rowman & Littlefield Publishers.

Posner, E. 2009. “Making Rules for Global Finance: Transatlantic Regulatory Cooperation at the Turn of the Millennium.” *International Organization* 63 (4): 665–99.

Quaglia, Lucia. 2013. “The European Union, the USA and International Standard Setting by Regulatory Fora in Finance.” *New Political Economy* 19 (3): 427–44. doi:10.1080/13563467.2013.796449.

Rees, W. 2006. *Transatlantic Counter-Terrorism Cooperation: The New Imperative*. New York: Routledge.

Risse-Kappen, T. 1995. *Bringing Transnational Actors Back In.* Cambridge: Cambridge University Press.

Sandholtz, W., and J. Zysman. 1989. “1992: Recasting the European Bargain.” *World Politics* 42 (1): 95–128.

Sikkink, Kathryn. 2005. “Patterns of Dynamic Multilevel Governance and the Insider-Outsider Coalition.” In *Transnational Protest and Global Activism*. Rowman & Littlefield.

Slaughter, A.-M. 2004. *A New World Order*. Princeton: Princeton University Press.

Stone Sweet, A., W. Sandholtz, and N. Fligstein. 2001. *The Institutionalization of Europe*. Oxford: Oxford University Press.

Swire, P., and R. Litan. 1998. *None of Your Business: World Data Flows, Electronic Communication, and the European Privacy Directive*. Washington, DC: Brookings.

Swire, Peter P., and Lauren B. Steinfeld. 2001. “Security and Privacy after September 11: The Health Care Example.” *Minnesota Law Review* 86: 1515.

Tarrow, Sidney. 2001. “TRANSNATIONAL POLITICS: Contention and Institutions in International Politics.” *Annual Review of Political Science* 4 (1): 1–20. doi:10.1146/annurev.polisci.4.1.1.

Tollison, Robert D., and Thomas D. Willett. 1979. “An Economic Theory of Mutually Advantageous Issue Linkages in International Negotiations.” *International Organization* 33 (4): 425–449. doi:10.1017/S0020818300032252.

Weeks, Jessica L. 2012. “Strongmen and Straw Men: Authoritarian Regimes and the Initiation of International Conflict.” *American Political Science Review* 106 (2): 326–347. doi:10.1017/S0003055412000111.

Zarate, Juan. 2015. *Treasury’s War: The Unleashing of a New Era of Financial Warfare*. First Trade Paper Edition edition. PublicAffairs.

Zito, A. 2001. “Epistemic Communities, Collective Entrepreneurship and European Integration.” *Journal of European Public Policy* 8 (4): 585–603.

1. (Avant and Westerwinter 2016; R. Keohane and Nye 1998; Hameiri and Jones 2013; Cerny 2000; Kahler and Lake 2003; Kahler 2009) [↑](#footnote-ref-1)
2. (McKibben 2010; Davis 2009) [↑](#footnote-ref-2)
3. (Tollison and Willett 1979; Davis 2004; Poast 2013; McKibben 2013; Johnson and Urpelainen 2012) [↑](#footnote-ref-3)
4. (Risse-Kappen 1995; Kahler 2009; Cerny 2010; Farrell and Newman 2014; Khagram, Riker, and Sikkink 2002; Kaldor 2013; Hale and Held 2011; Kahler forthcoming) [↑](#footnote-ref-4)
5. (M. Keck and Sikkink 1998; Carpenter 2011; Sikkink 2005) [↑](#footnote-ref-5)
6. (Jupille 1999; Meunier 2005; Joseph Jupille 2012). [↑](#footnote-ref-6)
7. (ORREN and SKOWRONEK 1996; Pierson 2006) [↑](#footnote-ref-7)
8. For the sake of simplicity, we use the term ‘state’ to refer to the head of the government, acknowledging that sub-state actors may have distinct preferences from the chief executive. [↑](#footnote-ref-8)
9. (E. B. Haas 1980; E. B. Haas 1991; Bicchi 2014) [↑](#footnote-ref-9)
10. (M. E. Keck and Sikkink 1999) [↑](#footnote-ref-10)
11. (E. B. Haas 1980; McKibben 2013; Davis 2009; Poast 2013) [↑](#footnote-ref-11)
12. (Hale and Held 2011; Green 2013; Kaldor 2013) [↑](#footnote-ref-12)
13. (Mitchell and Powell 2011; Colgan 2010; Weeks 2012) [↑](#footnote-ref-13)
14. (E. B. Haas 1991; P. Haas 1992) [↑](#footnote-ref-14)
15. (Tollison and Willett 1979; Davis 2009; Poast 2012) [↑](#footnote-ref-15)
16. (Davis 2004). [↑](#footnote-ref-16)
17. (Davis 2004; McKibben 2010) [↑](#footnote-ref-17)
18. (Poast 2012; Axelrod and Keohane 1985; Morrow 1992) [↑](#footnote-ref-18)
19. (Johnson and Urpelainen 2012) [↑](#footnote-ref-19)
20. (Dewey and Rogers 2012) [↑](#footnote-ref-20)
21. (P. Haas 1992) [↑](#footnote-ref-21)
22. (Cerny 2010; Slaughter 2004; Avant, Finnemore, and Sell 2010; Kahler 2009; Kahler forthcoming) [↑](#footnote-ref-22)
23. (Avant and Westerwinter 2016; Hameiri and Jones 2013; Henry Farrell and Newman 2015; Kaldor 2013; Carpenter 2011) [↑](#footnote-ref-23)
24. (Cerny 2010; Slaughter 2004; Henry Farrell and Newman 2014; Sikkink 2005) [↑](#footnote-ref-24)
25. (P. Haas 1992; Zito 2001) [↑](#footnote-ref-25)
26. (Carpenter 2011; Kahler 2009; Bob 2005; Abbott, Green, and Keohane 2016) [↑](#footnote-ref-26)
27. (Tarrow 2001; M. E. Keck and Sikkink 1999; Risse-Kappen 1995; Khagram, Riker, and Sikkink 2002; Porta and Tarrow 2004) [↑](#footnote-ref-27)
28. (Stone Sweet, Sandholtz, and Fligstein 2001; Sandholtz and Zysman 1989) [↑](#footnote-ref-28)
29. (R. O. Keohane and Nye 1987):736. [↑](#footnote-ref-29)
30. (Pierson 2006; ORREN and SKOWRONEK 1996) [↑](#footnote-ref-30)
31. (J. Jupille 1999; Meunier 2005) [↑](#footnote-ref-31)
32. (Bach and Newman 2007; Posner 2009; Quaglia 2013) [↑](#footnote-ref-32)
33. This simple account helps to specify the relationship between issue linkage and entrepreneurialism, by predicting that it will be crucially affected by heterogeneity of influence structures associated with the relevant issues. However, it does not provide a strong predictive framework for determining whether those seeking to keep issue areas separate will win, or whether they will lose out to those who look to use new knowledge to join hitherto-separate issues together. [↑](#footnote-ref-33)
34. (Mahoney 2003; George and Bennett 2005) [↑](#footnote-ref-34)
35. (H. Farrell 2003; Newman 2008b; Kobrin 2004) [↑](#footnote-ref-35)
36. (Hafner and Lyon 1998) [↑](#footnote-ref-36)
37. Interview with Ira Magaziner, 2000. [↑](#footnote-ref-37)
38. (P. Swire and Litan 1998; Newman 2008b) [↑](#footnote-ref-38)
39. (Pearce 1998; Newman 2008a) [↑](#footnote-ref-39)
40. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML [↑](#footnote-ref-40)
41. Interview with Ira Magaziner, 2000. [↑](#footnote-ref-41)
42. http://clinton4.nara.gov/WH/New/Commerce/ [↑](#footnote-ref-42)
43. Quoted in Courtney Macavinta, “BBB privacy project faces critics,” <http://www.cnet.com/news/bbb-privacy-project-faces-critics/> (checked April 12 2016). [↑](#footnote-ref-43)
44. Interview with US negotiator, 2000. [↑](#footnote-ref-44)
45. Interviews with EU, US negotiators, 2000. [↑](#footnote-ref-45)
46. (H. Farrell 2003; Kobrin 2004; Long and Quek 2002) [↑](#footnote-ref-46)
47. http://www.export.gov/safeharbor/ [↑](#footnote-ref-47)
48. https://safeharbor.export.gov/list.aspx [↑](#footnote-ref-48)
49. (Hofheinz and Mandel 2015) [↑](#footnote-ref-49)
50. (Bennett 2008). Interview Max Schrems, 2016. [↑](#footnote-ref-50)
51. Dhont, Asinari, and Poullet 2004 [↑](#footnote-ref-51)
52. Dhont, Asinari, and Poullet 2004: 18 [↑](#footnote-ref-52)
53. https://epic.org/privacy/streetview/ [↑](#footnote-ref-53)
54. (Kerry 2014) [↑](#footnote-ref-54)
55. Senator Ron Wyden [argues](http://thehill.com/policy/cybersecurity/256150-eu-no-safe-harbor-for-us-firms) that the court’s “misguided decision amounts to nothing less than protectionism against America’s global data processing services and digital goods.” Before the Safe Harbor decision, President Obama [similarly claimed](http://recode.net/2015/02/15/white-house-red-chair-obama-meets-swisher/) that European privacy protections were more motivated by commercial selfishness than high-minded principle. [↑](#footnote-ref-55)
56. (Baker 2013; Rees 2006; Bensahel 2003) [↑](#footnote-ref-56)
57. http://www.statewatch.org/news/2002/feb/useu.pdf. [↑](#footnote-ref-57)
58. Interview European Parliamentarian, 2004. [↑](#footnote-ref-58)
59. (Henry Farrell and Newman 2015) [↑](#footnote-ref-59)
60. Interview with European Commission official, 2004. [↑](#footnote-ref-60)
61. Ibid. [↑](#footnote-ref-61)
62. Interview with European Commission official, 2009. [↑](#footnote-ref-62)
63. Ibid. [↑](#footnote-ref-63)
64. (Bennett 2008; P. P. Swire and Steinfeld 2001; Aldrich 2004) [↑](#footnote-ref-64)
65. Interview with Graham Watson, then leader of the ALDE (Liberal) party in the European Parliament, 2004. [↑](#footnote-ref-65)
66. Ibid. [↑](#footnote-ref-66)
67. Interviews with European Parliament officials, 2004. [↑](#footnote-ref-67)
68. <http://curia.europa.eu/juris/document/document.jsf?docid=57549&doclang=en>. [↑](#footnote-ref-68)
69. (Kaunert 2010) [↑](#footnote-ref-69)
70. (Pawlak 2009; Aldrich 2004) [↑](#footnote-ref-70)
71. (Pawlak 2009; Pawlak 2010) [↑](#footnote-ref-71)
72. (Pawlak 2009, p.567) [↑](#footnote-ref-72)
73. Interview with airline industry official, 2009. [↑](#footnote-ref-73)
74. Dhont, Asinari, and Poullet 2004: 101 [↑](#footnote-ref-74)
75. (Zarate 2015) [↑](#footnote-ref-75)
76. https://www.dhs.gov/xlibrary/assets/privacy/privacy\_intl\_hlcg\_report\_02\_07\_08\_en.pdf. [↑](#footnote-ref-76)
77. <http://www.statewatch.org/news/2009/dec/eu-usa-hlg-dp-14574-09.pdf>. [↑](#footnote-ref-77)
78. Interview with Commission official, 2009. [↑](#footnote-ref-78)
79. https://www.dhs.gov/news/2011/02/09/statement-information-sharing-and-privacy-and-personal-data-protection-between. [↑](#footnote-ref-79)
80. http://www.statewatch.org/news/2014/feb/ep-nsa-surveillance-report-consolidated-21-2-14.pdf. [↑](#footnote-ref-80)
81. Interview with Max Schrems, privacy activist, March 2016. [↑](#footnote-ref-81)
82. EU Commission (2013: 3) “Large-scale US intelligence collection programmes, such as PRISM affect the fundamental rights of Europeans and, specifically, their right to privacy and to the protection of personal data. These programmes also point to a connection between Government surveillance and the processing of data by private companies, notably by US internet companies” [↑](#footnote-ref-82)
83. (Kaunert 2010; Monar, n.d.) [↑](#footnote-ref-83)
84. Interview with Max Schrems, March 2016. [↑](#footnote-ref-84)
85. http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet\_eu-us\_privacy\_shield\_en.pdf [↑](#footnote-ref-85)
86. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp238\_en.pdf [↑](#footnote-ref-86)
87. https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNews/Press/2016/EDPS-2016-11-PrivacyShield\_EN.pdf [↑](#footnote-ref-87)
88. SENATE COMM. ON GOVERNMENT OPERATIONS PROTECTING INDIVIDUAL PRIVACY IN FEDERAL GATHERING AND DISCLOSURE OF INFORMATION, S. REP. No. 1183, 93d Cong., 2d Sess. 79 (1974), reprinted in SOURCEBOOK, supra note 6, at 232. [↑](#footnote-ref-88)
89. (Boyle 1989) [↑](#footnote-ref-89)
90. http://www.itic.org/dotAsset/5/8/58eb178a-e926-4783-959b-60d9464248e6.pdf [↑](#footnote-ref-90)
91. https://www.govtrack.us/congress/bills/114/hr1428 [↑](#footnote-ref-91)
92. (R. O. Keohane and Nye 1987) [↑](#footnote-ref-92)