Regulating privacy across the Atlantic: Of pyrrhic victories, arena switching, and policy U-turns

Andreas Busch
Dept. of Politics and International Relations
University of Oxford

Paper presented at the
ECPR Standing Group on Regulatory Governance conference
"(Re)Regulation in the Wake of Neoliberalism"
Utrecht, June 5–7, 2008

Abstract

In the late 1990s, the growing importance of electronic commerce forged a reconciliation of different stances towards the regulation of personal data between the United States and the European Union in the interest of trade. But the "Safe Harbor" agreement's compromise quickly came under pressure when in the wake of 9/11 the United States unilaterally tightened its position, forcing the EU to comply with US regulatory preferences.

What looked like a transatlantic conflict over the value of privacy in the making also developed an intra-European dimension when the European Parliament took the Commission to court over alleged negligence of European data protection legislation. The paper analyses the two conflicts and argues that the Parliament's court action and success resulted in substantial unintended consequences when competence for the subject matter was switched to another Directorate General, with different policy frames and preferences taking over, resulting in a substantive policy U-turn.

1 Introduction

This paper traces and analyses the regulation of privacy in transatlantic data traffic between the United States and the European Union over the last decade. Building on the analysis of a number of case studies – the "Safe Harbor" agreement, the dispute over passenger name records, and that over financial transaction data from the SWIFT network[1] – it makes three interrelated arguments: first, that an approach focusing on "framing" can well explain the different positions encountered in the empirical reality of transatlantic (and intra-European) disputes about privacy regulation; second, that the European position on data and privacy protection has changed considerably after ten years of championing a high level of protection against US demands for a lower level of protection; and third that this policy U-turn is largely the unintended consequence of the European Parliament's success before the European Court of Justice – an exemplary case of a pyrrhic victory.

The paper starts by outlining the differences in regulatory philosophies and approaches regarding privacy between the European and American sides. They came to a head in the 1990s with the spread of electronic commerce. A first successful agreement that reconciled the differences is contrasted with two more recent episodes which can only be interpreted as results of unilateral exercise of power, thus undermining an interpretation of the "Safe Harbor" agreement as the harbinger of regulatory things to come. The ensuing part of the paper therefore offers an analytical approach based on "framing" that can accommodate the different outcomes, before the final part of the paper analyses the recent shift in the European Union's position on privacy and data protection. The more or less complete U-turn conducted on the subject of passenger name records is seen as the consequence of arena switching within the European Commission's bureaucracy, thus emphasizing the importance of institutional factors in combination with the beliefs held by leading policy actors.

2 Regulating privacy in e-commerce: Different positions across the Atlantic

Electronic commerce, much of it conducted over the internet, has come to play an enormously important role in business today – and in international trade. Access to each other's e-commerce markets, as a consequence, has come to be of great importance to both the United States and the European Union. But regulatory philosophies and approaches have differed in the past, and the problem of divergent laws and regulations became ever more pressing as cross-border transactions made the mismatch between boundless economic space and territorially based jurisdictions very clear. Since much of e-commerce is concerned with the exchange of information, this was particularly acute in the area of privacy and data protection, where substantially different approaches to

[1] These case studies are here only presented in very compressed form. More information about them can be found in previous papers by the author (Busch (2006, 2007)) as well as (for the Safe Harbor case) in Farrell (2003) or Heisenberg (2005).

regulation had been employed on both sides of the Atlantic.

In the United States, privacy protection through statutory law is not very highly developed. Although there is a long-standing debate about the subject, starting in the late 19th century with the pathbreaking contribution by Warren and Brandeis (1890), the legal situation has been characterized by experts as a "patchwork quilt" (Holvast et al., 1999, USA-1), "at best a thin patchwork" (Froomkin, 2000, 1539) or as "fragmented, ad hoc and narrowly targeted to cover specific sectors and concerns" (Shaffer, 1999, 422).[2] With no comprehensive privacy legislation in place and unwilling to produce one, yet in recognition of the fact that privacy protection is imperative if e-commerce is to succeed, the United States approach focused on self-regulation by the industry. As the "Framework for Global Electronic Commerce", co-authored by President Clinton and Vice-President Gore and published by the White House in July 1997, put it:

> "Americans treasure privacy, linking it to our concept of personal freedom and well-being. Unfortunately, the GII's great promise – that it facilitates the collection, re-use, and instantaneous transmission of information – can, if not managed carefully, diminish personal privacy. It is essential, therefore, to assure personal privacy in the networked environment if people are to feel comfortable doing business.
> [...]
> The Administration supports private sector efforts now underway to implement meaningful, consumer-friendly, self-regulatory privacy regimes. These include mechanisms for facilitating awareness and the exercise of choice online, evaluating private sector adoption of and adherence to fair information practices, and dispute resolution." (Clinton and Gore, 1997)

In Europe, the approach taken was quite different. Beginning in the early 1970s, countries such as Germany, Sweden, France, and Denmark had started to introduce legislation on "data protection", and this had spread across the continent. The legislation aimed to prevent threats to privacy emanating from the introduction of computer based technologies – such as vast databases – and was focused on the right to protect one's own data.[3] National data privacy protection regimes varied across the member states of the European Union, however, which could be a potential obstacle for trade between them and hamper the development of e-commerce.

As a consequence, the European Union "Directive 95/46/EU on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data" was passed in October 1995 after five years of negotiations and entered into force in October 1998. While the Directive makes it clear that henceforth "given the equivalent protection resulting from the approximation of national laws, the Member

[2] More comprehensive comparisons of international privacy regulations can be found in Michael (1994) and Electronic Privacy Information Center and Privacy International (2004).

[3] For overviews of the legal developments in Europe see the contribution by Viktor Mayer-Schönberger in the volume edited by Agre and Rotenberg (1997) and Bennett (1992), especially the tables on pp. 57 and 59.

States will no longer be able to inhibit the free movement between them of personal data on grounds relating to the protection of the rights and freedoms of individuals, and in particular the right to privacy" (preamble section 9), it also introduced regulations that made transfer of such data to third countries (i.e. outside the European Union) dependent on "an adequate level of protection" there (article 25). In other words, while facilitating trade within the EU, the Directive could potentially become a serious obstacle to electronic commerce with countries outside Europe (such as the United States), if their level of privacy protection was judged to be not adequate.

2.1 The "Safe Harbor" agreement

Given the amount of trade and economic interdependence between the EU and the United States, one would expect negotiations about the topic of transatlantic data flows to have been taken up immediately after the Data Protection Directive had been passed in 1995.[4] However, that was not the case. Rather, the initial U.S. reaction was quite nonchalant, assuming that the exemption clauses of article 26 of the Directive would leave data flows unimpeded. Real discussions only started in the first half of 1998 when the U.S. administration realised that this might not be the case.

Initially both sides took negotiation positions that can be described as insisting on their own approaches and demanding from the other side to adopt that. EU officials suggested they would only be satisfied if the United States introduced appropriate formal legislation and authorities to protect privacy. The United States further pursued its strategy, laid down in the "Framework", to rely on independent privacy auditing agencies that would award seals for websites, and White House e-commerce policy architect Ira Magaziner expressed hope that spreading this approach internationally would diffuse the disagreement with the European Union. Take-up of this approach, however, was very low even in the United States themselves: hardly any companies applied to agencies like TRUSTe or BBBOnline for their seal, which reinforced the EU Commission's skepticism about the unworkability of the American approach of self regulation.

Both sides' positions seemed incompatible at that time, and it was hard to see how a compromise could be reached. But the increasingly tense situation started to induce some movement. U.S. industry began to recognize that the EU was chiefly concerned with the lack of an enforcement mechanism in U.S. self regulation, and together with U.S. policymakers' threats that legislation would not be ruled out if take-up rates of the certification mechanisms remained low, this started to change the situation. In addition, the federal government started to step up the enforcement of regulations on unfair or deceptive company privacy principles.

The logjam in the negotiations was only overcome, however, when the American lead negotiator David Aaron suggested the concept of a "Safe Harbour", i.e. a set of principles to which companies would be able to subscribe and which would be considered "adequate" under the EU Directive. This proposal transformed the negotiations, because it pointed out a way how EU substantive concerns about privacy protection could be achieved

[4] This section draws on the descriptions of the "Safe Harbour" negotiations in Long and Quek (2002), Farrell (2003), Regan (2003), and Kobrin (2004).

without the United States having to pass comprehensive privacy legislation and setting up respective institutions. While some EU member states remained skeptical, an agreement was eventually reached between the United States and the European Commission along the lines suggested by Aaron. Companies would be able to self-certify annually that they met the agreed set of seven privacy principles[5] on data protection issued by the U.S. Department of Commerce. The Federal Trade Commission would maintain a list of complying organisations on its website, and failure to comply would be actionable under the Federal Trade Commission Act. In return, the European Commission issued a finding of adequacy of this procedure under the Data Protection Directive.

The "Safe Harbour" agreement was thus neither a recognition of the previous U.S. system by the European Union, nor was it an extension of the EU system of formal legislation combined with state privacy commissioners. Rather it is qualitatively different from both and a new system that was hailed by many observers as particularly adequate for the conditions of incongruity between economic and political space and the problem of regulatory spill-over across jurisdictions. This perspective has been taken up and amplified in the political science literature analysing the agreement as a shining example of future agreements in this area (see below).

2.2 The fight over Passenger Name Records

But if hopes had been expressed that the "Safe Harbour" solution would be a model of future solutions for problems of this kind (see, for instance, Farrell (2003, 297)), then such assessments will likely have to be reevaluated in the light of another, more recent, dispute between the two parties, namely that about airline passenger name records or PNRs.

A PNR is a file created by an airline for each journey a passenger books, is usually held in a Computerized Reservation System (CRS) and contains the name of the traveler, details of flights, hotels, car rentals, and other travel services. But it can also contain residential and business postal and e-mail addresses as well as phone numbers, credit card details, and names and personal information of emergency contacts. Furthermore, through billing, meeting, and discount eligibility codes, PNRs also contain information about memberships and organizational affiliations, they can contain religious meal preferences and details on physical and medical conditions. PNRs must therefore be regarded as sensitive personal information.

After the attacks of September 11, 2001, the United States decided to use PNR data in their fight against terrorism. On 19 November 2001, Congress passed the "Aviation and Security Act" which required airlines operating passenger flights to, from or through the United States, to provide the U.S. Bureau of Customs and Border Protection (CBP) before take-off or at least 15 minutes after departure with electronic access to PNR data contained in their reservation and departure control systems. Since PNRs con-

[5] They require companies to give individuals *notice,* give them *choice*, inform them about *onward transfer*, grant them *access* to information about them, undertake reasonable precautions regarding *security* and *data integrity,* and have in place a mechanism for *enforcement.* See details at `http://www.export.gov/safeharbor/doc_safeharbor_index.asp` [19.5.2008].

tain personal data, this fell under the EU Data Protection Directive and thus required negotiations between both sides.

After a provisional agreement in March 2003 – allowing European carriers to provide PNRs without being penalised in the EU for this – negotiations took place throughout 2003 between the European Commission's Directorate-General for the Internal Market (which is responsible for data protection) and the U.S. Department of Homeland Security about these data transfers. Although the EU side initially found the US demands unacceptable,[6] in December 2003 it agreed to a solution that largely accepted those demands:

- PNR data could be used for more than preventing and combating terrorism and related crimes;
- 34 PNR elements would be transmitted (including addresses, religious meal preferences, and all information about previous travels);
- PNR data storage would be for 3.5 years, after which data which had not been accessed during that period would be destroyed, but other data kept for an additional 8 years;
- complaints about the handling of PNRs could be made "in writing" to the Chef Privacy Officer of the Department of Homeland Security who "will review the situation and endeavour to resolve the complaint".

The European Commission issued an "adequacy ruling" (regarding compliance with the Data Protection Directive) on 14 May 2004, but the agreement met criticism from the working party of EU national data protection officers[7] and from the European Parliament. In June 2004 the European Parliament then decided to ask the Court of Justice of the European Communities to annul both the agreement and the adequacy finding.

2.3 Privacy and Financial Data: The SWIFT raid

Barely three weeks after the court decision about the PNR case, on June 23, 2006, the *New York Times* published a story (Lichtblau and Risen, 2006) revealing another case causing privacy related disagreement across the Atlantic since, namely the U.S. administration's secret raid on worldwide financial transaction data of the *Society for Worldwide Interbank Financial Telecommunication* (SWIFT). SWIFT is an industry-owned cooperative incorporated under Belgian law that has been providing services to the international financial industry through a transfer message service since its foundation in 1973. It has upwards of 8000 financial institutions as customers in more than 200 countries, and is routing up to 12 mio. transactions per day which have a volume of

[6] Cf. Commissioner Bolkestein's op-ed commentary "Resisting U.S. demands: Passenger privacy and the war on terror" in the *International Herald Tribune* of 24 October 2003.

[7] See their "Opinion 2/2004 on the Adequate Protection of Personal Data Contained in the PNR of Air Passengers to Be Transferred to the United States' Bureau of Customs and Border Protection (US CBP)", adopted 29 January 2004.

up to 6 trillion US-Dollars. In short, SWIFT is the backbone through which all formal international financial transactions are being carried out, not least because it is the only such service that exists. Since the messages relayed contain personal data as well as potentially strategic business data, they are highly relevant in terms of privacy.

After the terrorist attacks on the United States on September 11, 2001, the U.S. administration decided to seek and gained access to these transaction data for the purposes of their "Terrorist Finance Tracking Program" (TFTP). It served subpoenas which mandated SWIFT to hand over data for the purposes of terrorist investigations. These subpoenas were directed to the SWIFT data processing centre in the United States, one of two data processing centres the company operates.[8] Data are mirrored between both for backup purposes and kept for 124 days. As a result, the data content in both centres is the same, and data accessible in the United States include data emanating from business in the European Union and elsewhere around the globe.

SWIFT had no choice but to hand over the data. While the amount of data passed on is unclear,[9] SWIFT certainly did not notify its member institutions of the subpoenas (no less than 64 between September 2001 and November 2006[10] – or on average one per month) and therefore of the transfer of data to U.S. authorities.

After the existence of the TFTP program had been published and acknowledged by the U.S. administration in June 2006, European reactions were very critical of it. The European Parliament passed a resolution on 6 July 2006 demanding full information from EU institutions about their awareness of the program and expressing strong disapproval and deep concern about the operation affecting European citizens' privacy in secret; European governments denied previous knowledge of the program; member state parliaments debated the issue and criticised the U.S. administration's actions strongly;[11] and business associations as well as the financial press expressed worries that the data handed over could also be used for the purposes of industrial espionage.[12] However one may ultimately judge these allegation, it is safe to say that the secrecy with which the U.S. administration carried out the data confiscation was clearly very one-sided, and not designed to accommodate in any way EU sensitivities regarding the issue of privacy. In fact, the knowledge that EU institutions and European governments would try to block the data transfer probably was a main reason for the U.S. administration to choose that route.

[8] The other SWIFT data processing centre is located in an EU member state.

[9] The respective claims vary from "the entire Swift database" (New York Times) to "it has only ever transferred information pursuant to the subpoenas in accordance with the agreement between it and the US Treasury." (Canadian Privacy Commissioner's Report of Findings (2 April 2007), paragraph 34).

[10] See Article 29 Working Party Opinion 10/2006, p. 8.

[11] See e.g. the German Bundestag debate on 29 March 2007.

[12] See e.g. reports in the German daily *Handelsblatt* (11 July 2006) and the Austrian daily *Die Presse* (11 July 2006).

3 Analysing the disputes: Three frames of viewing privacy

Political science analyses of transborder data flows between the U.S. and the EU have so far focused on the "Safe Harbour" case and have primarily analysed it from a "constructivist" viewpoint.[13] This perspective emphasizes the importance of values, norms, and discourse over conventional, "realist" analyses of power. With respect to the "Safe Harbour" case, it has been claimed that, especially under conditions of comparable power, dialogue can break logjam, prevent both domination by one side or the decline into (trade) conflict, and that persuasion and argument can achieve results that cannot be explained by conventional bargaining theory. Faced with a difficult negotiating situation, the analysis goes, "[t]hrough a process of argument, [the U.S. and the EU] succeeded in discovering new possibilities of action, reaching a provisional understanding about a new institutional approach to resolving the vexing dispute over privacy regulation, which may be applied to other areas of e-commerce." (Farrell, 2003, 302). The agreement between the United States and the European Union, whose main aim was to provide a framework for firms that would enable them to engage in electronic commerce across the Atlantic in the face of different standards of private sector data protection rules between the two areas was generally hailed as a constructive compromise that owed more to attempts at mutual understanding then to power and a perspective on interests.

However much this may indeed have been the case in the "Safe Harbour" case, it is difficult to see how the same claims can be made in the PNR or SWIFT cases – and therefore be generalizable for disputes about transborder data flows. In the latter, far from there being persuasion and argument, quite clearly the United States prevailed, achieving their goals of unhindered access to passenger name records and financial transfers data without effective control by the European side over their further use, which goes against the fundamental principles of EU data protection legislation. To enhance our understanding of the differences between the three cases, further distinctions therefore need to be found, and additional variables need to be investigated for their explanatory potential.

We argue here that the issue of transborder data flows can be approached from different viewpoints, and that different actors can take different positions with respect to these viewpoints. In social science terminology we can say that they "frame" issues in different ways. Frames are the underlying structures of beliefs, perceptions and appreciations on which policy positions rest, and these frames determine what counts as a fact and what arguments are taken to be relevant and compelling (Rein and Schön, 1993; Schön and Rein, 1994). For the issue of privacy and transborder data flows, three different frames can be hypothesized to exist: one can be labelled "economic interests" and focuses on questions of cost effectiveness, profit and market extension; another one can be labelled "safety interests" and is concerned with such things as reduction of risk and prevention of misuse; and a third one can probably be best described as "civil liberty interests" and centres on such issues as privacy and freedom of information. These different frames are likely to be adopted by different classes of actors, and their choices will be driven by

[13] Cf. Long and Quek (2002); Farrell (2003); Regan (2003).

their respective interests and world views.

- The "economic interests" frame will likely be chosen by commercially oriented actors such as firms[14] and market-oriented actors in the bureaucracy such as regulating agencies supervising markets etc. They will above all look at minimizing transaction costs, be aware of (and publicly emphasize) the benefits of exchange and trade, and thus likely opt for a light regulatory touch which however realises a high level of privacy protection – given that trust in that protection is essential for the conduct of e-commerce.

- The "safety interests" frame will likely be chosen by the law enforcement community, by military interests, and commercial interests in the security industry. These actors will above all look at the minimization of risk and have little regard for keeping transaction costs low – the emphasis is on safety, after all, and on protecting lives. Compared to these, the protection of privacy is decidedly of second-rate interest; rather, from this point of view it will seem more important to collect as much information on individuals as possible in order to make effective protection possible.

- The "civil rights" frame will likely be chosen by actors whose interest in the subject is neither of the two aforementined ones, such as civil rights groups and political and bureaucratic actors who are mandated with the protection of civil rights and privacy or data protection. This group will likely include data protection commissioners on both firm, national and supranational levels, NGOs, and those political forces who see their constituencies more interested in the protection of these rights than in the pursuit of economic or safety interests – most likely libertarians of either the right or the left.

Differentiating the actors and their interests in this way, we argue, enables us to move beyond the unsatisfactory analysis that sees disputes about transborder data flows as most likely to be resolved in a constructive manner like the "Safe Harbor" case – but which cannot account for the PNR and SWIFT cases. We can now distinguish the three cases as being characterised by different issue areas, with accompanying differences in the configurations of actors and frames. The three cases described above, we argue here, fell into two different issue areas, namely business and safety, and the participating actors approached them with distinctive and different frames:

- In the e-commerce case, the American side used an economic interest frame, while the European Commission used a mix of economic and civil liberty frames. The compromise of "Safe Harbour" was closer to the European position as it took considerations from each frame into account.

[14] Unless their business is in the security industry, which would likely make them adopt the "safety interests" frame.

– In the PNR case, the American side used a pure "safety interests" frame, without regard to other considerations, while the European actors used safety and civil liberties frames, but in different measures: the European Parliament's "dose" of civil liberties was clearly greater than the European Commission's, and since the solution found so far reflects the American preferences more clearly, the difference between the European Commission's and the Parliament's perspective became quite substantial, leading to the European Parliament's court action.

– In the SWIFT case, the American position was like in the PNR case a pure "safety interests" frame, while European actors again used mixed frames, with in particular the data protection agencies focusing on the "civil liberties" (i.e. data protection) perspective.

4 The sudden U-turn: The EU changes course on privacy

Throughout the time since the mid-1990s and through all conflicts with the United States, the European Union had maintained a position of champion of data and privacy protection rights. Its Data Protection Directive had been seen as an instrument that would unfold influence on a global scale, leading to a "ratcheting up" of US personal privacy standards (cf. Regan (1993); Shaffer (1999, 2000)), and its principles, it was argued, might even provide the nascent origins of a global privacy regime (Busch, 2007, 20).

However, in the summer of 2007, the European Commission suddenly seemed to change course in two areas where it had previously strongly defended its position of privacy rights: on the issue of passenger name records (PNR), it suddenly advocated the use of these data within Europe for the purposes of anti-terrorism; and on the issue of financial data, it agreed to no longer try to block their transfer from SWIFT to the United States.

To explain this sudden shift in preferences, we have to go back to the dispute between the European Commission and the European Parliament over the PNR agreement with the United States. That dispute made clear that there was no unified European position on the subject, but rather a difference between the relative values ascribed to safety and civil liberties considerations between the Commission and the Parliament. Since the Parliament argued that the Commission's acceptance of the US demands constituted a breach of the Data Protection Directive and thus of European law, it decided to take the issue before the European Court of Justice and demanded that the Court annul both the agreement and the Commission's adequacy ruling of May 2004.

Two years later, on 30 May 2006, the European Court did indeed annul both the Council decision concerning the conclusion of the agreement with the United States and the Commission decision on adequacy (cases C-317/04 and C-318/04). However, the Court ruled solely based on the issue of competence, finding that the Council acted without competence in approving the agreement, and that the Commission acted outside its competences in declaring the agreement adequate in terms of the data protection directive. Consequently, the Court did *not* decide about the Parliament's claims regarding the substantive issues of breach of the right to privacy and breach of fundamental

rights.

While first considered by many a success of Parliament over the Commission, we can now argue that this success spawned substantial unintended consequences which ultimately changed the course of decisions in this area against the Parliament's preferences.

The underlying reason is that the Court decision led to a switch in the arena in which the issue of PNR was dealt with within the European Union, with concomitant changes in the bureaucratic procedures and decision making competences. The Court ruled that the Directorate-General *Internal Market and Services* (DG Markt) had no competences under the Treaty of European Union to deal with the PNR case, and thus the further negotiations with the United States (which led to a new agreement in June 2007) were conducted by the Directorate-General *Justice, Freedom and Security* (DG JLS). However, this is far more than an organisational detail: in terms of our above analysis of frames it means a shift from a dominant frame of "economic interests" to one of "safety interests". It had wide-ranging consequences for the outcome.

PNR data, so far regarded by the European Commission mainly as the property of passengers and to be protected under European data protection rules, suddenly became seen as a potentially valuable source of information in the fight against terrorism and for law enforcement. Rather than having to defend them against American demands, the main perspective now became one of learning from and copying the American use of them to spot and pin down potential terrorists and law breakers among the travelling crowds in Europe. Consequently, Justice Commissioner Frattini put forward a proposal for European legislation in November 2007 that would mandate EU member states to collect and keep PNR data for 13 years – far longer than had been considered acceptable when demanded by the American side in the first round of negotiations.

5 Conclusion

For the European Parliament, its success before the European Court of Justice in 2006 thus constituted a clear pyrrhic victory. Rather than being able to shift the policy outcome into the direction of its own preferences (i.e. towards more data protection, fewer data being collected, and shorter periods of storage), the exact opposite happened: there was no substantive change in the new agreement found between the EU and the United States; and the new commissioner in charge of the subject initiated European level legislation that *extended* the collection and use of PNR data to the area of the European Union. What is more, since the new procedures take place under the intergovernmental "pillar" of the European Union, the European Parliament has a vastly reduced influence in the decision making process – it is no longer as involved a player as it was in the first round of the agreement. And what is probably worst: the Parliament has noone but itself to blame for this shift in policy and procedures!

The shift of responsibility for the PNR case from the Internal Market DG to the Justice DG was accompanied by a clear shift in policy preferences. Empirically, this illustrates the fact the European Union's position (and even more clearly of course the European position) is not a unitary one, but subject to different preferences, views,

and evaluations. This will come as no surprise to those whose scholarly arguments are informed by empirical facts, but may be a good reminder for students of politics intent on deriving detailed policy positions from a small set of "interests". Analytically, it confirms the usefulness of using a "framing" approach to make sense of policy disputes and policy puzzles – such as the ones of different outcomes in international negotiations between the same actors in the field of transborder data flows, and even in explaining sudden shifts in long-held policy preferences by the same actor!

References

Agre, Philip and *Rotenberg, Marc* (eds.), 1997: Technology and privacy : the new landscape, Cambridge (MA); London: MIT Press.

Bennett, Colin J., 1992: Regulating privacy. Data protection and public policy in Europe and the United States, Ithaca: Cornell University Press.

Busch, Andreas, 2006: From Safe Harbour to the Rough Sea? Privacy Disputes across the Atlantic, in: SCRIPT-ed. A Journal of Law and Technology 3 (4), pp. 304–321.

Busch, Andreas, 2007: From Safe Harbour to the Rough Sea? Privacy Disputes across the Atlantic [Paper presented at the Workshop "Privacy and Information: Modes of Regulation", ECPR Joint Sessions of Workshops, Helsinki, May 2007].

Clinton, William J. and *Gore, Albert, Jr.*, 1997: A Framework For Global Electronic Commerce.

Electronic Privacy Information Center and *Privacy International*, 2004: Privacy & Human Rights. An International Survey of Privacy Laws and Developments, Washington, D.C.; London: Electronic Privacy Information Center ; Privacy International.

Farrell, Henry, 2003: Constructing the international foundations of E-commerce – the EU–U.S. Safe Harbor arrangement, in: International Organization 57 (2), pp. 277–306.

Froomkin, A. Michael, 2000: The Death of Privacy?, in: Stanford Law Review 52, pp. 1461–1543.

Heisenberg, Dorothee, 2005: Negotiating Privacy: The European Union, the United States, and Personal Data Protection, Boulder (CO): Lynne Rienner.

Holvast, Jan; *Madsen, Wayne* and *Roth, Paul*, 1999: The global encyclopaedia of data protection regulation, The Hague ; London: Kluwer Law International.

Kobrin, Stephen J., 2004: Safe harbours are hard to find: the trans-Atlantic data privacy dispute, territorial jurisdiction and global governance, in: Review of International Studies 30 (1), pp. 111–131.

Lichtblau, Eric and *Risen, James*, 2006: Bank Data Sifted in Secret by U.S. to Block Terror, in: The New York Times, 23 June 2006 , p. 1.

Long, William J. and *Quek, Marc Pang*, 2002: Personal data privacy protection in an age of globalization: the US – EU safe harbor compromise, in: Journal of European Public Policy 9 (3), pp. 325–344.

Michael, James R., 1994: Privacy and human rights : an international and comparative study, with special reference to developments in information technology, Aldershot, Paris: Dartmouth ; Unesco.

Regan, Priscilla M., 1993: Globalization of privacy: implications of recent changes in Europe, in: American Journal of Economics and Sociology 52, pp. 257–274.

Regan, Priscilla M., 2003: Safe harbors or free frontiers? Privacy and transborder data flows, in: Journal of Social Issues 59 (2), pp. 263–282.

Rein, Martin and *Schön, Donald A.*, 1993: Reframing Policy Discourse, in: *Frank Fischer* and *John Forester* (eds.), The Argumentative Turn in Policy Analysis and Planning, Durham, London: Duke University Press, pp. 145–166.

Schön, Donald A. and *Rein, Martin*, 1994: Frame Reflection: Resolving Intractable Policy Issues, New York: Basic Books.

Shaffer, Gregory, 1999: The power of EU collective action: the impact of EU data privacy regulation on US business practice, in: European Law Journal 5 (4), pp. 419–437.

Shaffer, Gregory, 2000: Globalization and social protection : the impact of EU and international rules in the ratcheting up of U.S. privacy standards, in: Yale Journal of International Law 25 (1), pp. 1–88.

Warren, Samuel D. and *Brandeis, Louis D.*, 1890: The Right to Privacy, in: Harvard Law Review IV (5), pp. 193–220.