

From Safe Harbour to the Rough Sea? Privacy Disputes across the Atlantic

Andreas Busch

Dept. of Politics and International Relations

University of Oxford

andreas.busch@politics.ox.ac.uk

<http://users.ox.ac.uk/~busch>

Paper presented at the
Workshop “Privacy and Information: Modes of Regulation”

Directors:

Andreas Busch (University of Oxford) and Charles Raab (University of Edinburgh)

ECPR Joint Sessions of Workshops
Helsinki, May 2007

Draft – please only quote with author’s permission!

Abstract

Contrary to initial hopes of its founders, the increased economic, social-cultural and political importance of “cyberspace” has led to substantial state regulation of it. The issue of transborder data traffic therefore requires the cooperation of nation states which, however, encounters many difficulties.

The established literature on the regulation of disputes in transatlantic data transmissions focuses on the importance of values, norms, and discourse in a constructivist perspective. Building on an analysis of three illustrative case studies (the “Safe Harbor” agreement between the U.S. and the EU that was meant to provide a framework for firms in the face of different standards of private sector data protection between the two areas; the dispute between the U.S. and the EU about the transmission of airline passengers’ personal data; and the controversy between the U.S. and European institutions about the confiscation of financial transfer data), this paper argues that an approach that combines the analysis of “frames” with that of interests and institutions can better account for the diversity in outcomes. The cases also demonstrate that initial expectations for a “policy transfer” of EU privacy standards to the U.S. did not materialise.

The paper concludes by offering speculations about conditions conducive to the emergence of an international regime on privacy and data protection.

1 Introduction

This paper¹ analyses the politics of transborder data flows in a transatlantic perspective by looking at three case studies related to the issue of privacy and data protection: the agreement between the United States and the European Union to bridge the differences in privacy approaches in e-commerce (“Safe Harbour”), the dispute between the same two actors about the handing over of passenger name records (PNR) in transatlantic flights originating in the European Union, and their controversy regarding the secret confiscation of the data about international financial transfers within the SWIFT network through the U.S. administration.

The political science literature that has covered the topic of transborder data flows has so far focused on the case of the “Safe Harbour” agreement and has analysed it from a constructivist point of view, emphasizing the importance of values, norms, and discourse for the outcome reached in the negotiations. 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 than to power and a perspective on interests.

The present paper challenges this line of interpretation. It points to the differences in outcomes if one looks beyond the “Safe Harbour” case and the apparent absence of compromise and constructive discourse in the cases of the passenger name records and financial transfer data disputes. Here, signs of ad-hoc agreements, unilateral action and even imposition are far more in display than would be expected from a constructivist perspective, and the paper argues that an approach focusing on (actors’ divergent) interests and institutional factors is better suited to explain the dynamic of international interaction in the cases under consideration. This is all the more so since an evaluation of the “Safe Harbour” case through this perspective can also offer interesting insights. The approach taken in this paper thus seems better suited to offer a general explanation of the politics of transborder data flows.

After an introductory part that looks at aspects of the development of state regulation of transatlantic data flows, the paper proceeds to offer narratives of the three policy episodes in some detail, with a focus on initial positions and the outcome of the negotiations. In the analytical part, the paper attempts to offer an explanation for the differences in the outcomes of the case studies. Differences in the “framing” of issues between the actors as well as differences in interests play a role, but both are influenced

¹This paper contains first results from a larger project the author is undertaking on “The Politics and Governance of Privacy”. Previous versions of it have profited from discussions at the conference “Safety & Security in a Networked World: Balancing Cyber-Rights & Responsibilities”, Oxford Internet Institute, 8.–10. September 2005; at seminars at the Free University, Berlin, the University of Edinburgh, and the Department of Politics and International Relations, University of Oxford; at the ECPR Standing Group on Regulation’s conference on “Frontiers of Regulation. Assessing Scholarly Debates and Policy Challenges” at the University of Bath, 7.–8. September 2006, and at the meeting of the German Political Science Association’s standing group on International Political Economy on the occasion of the Association’s Conference at the University of Münster, 25.–29. September 2006.

by deeply rooted differences in the conceptualisation of privacy. The paper concludes with a section offering some speculative thoughts about the conditions under which the EU data protection regulations could spread and provide the seed for an international regime in this policy area.

2 Regulating the Internet

Today, the internet today is undoubtedly of major importance for transactions of a commercial nature (“e-commerce”). However, its origins are quite different. In the early 1970s, DARPA (a branch of the U.S. Department of Defense) initiated work on a decentralised communication network that would be resistant to a massive attack, and in the mid-1980s the U.S. National Science Foundation (NSF) initiated further development of a backbone communication infrastructure primarily for research purposes, linking major national research sites and their networks into what eventually became known as the “internet”.² Development and use were driven by a relatively small community of experts, and consequently little regulation was necessary. What rules there were emanated from egalitarian discussion processes, relations were largely based on trust, and what little hierarchies there were on recognized expertise.

In the early 1990s, when internet use became more widespread under such terms as “information superhighway” or “Global Information Infrastructure” (GII), the founding generation of the internet dreamt of a future without state influence and regulation on this communication tool that began to span the globe. Organisations like the “Electronic Frontier Foundation” (EFF), set up by technologists and exponents of the counter-culture in 1990, deliberately invoked myths of the founding fathers of the United States when they claimed to stand at a “digital frontier”, fighting to protect rights online. Their utopian idea was that of the new medium as a tool for world improvement and liberty, free from imposed regulation. As John Perry Barlow, a founding member of the EFF and sometime lyricist for the 1960s cult band *The Grateful Dead* put it in exemplary fashion in a “Declaration of the Independence of Cyberspace” in 1996, when commercialisation and imposed regulation threatened to alter the free-wheeling spirit that had prevailed until then:

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

We have no elected government, nor are we likely to have one, so I address you with no greater authority than that with which liberty itself always speaks. I declare the global social space we are building to be naturally independent of the tyrannies you seek to impose on us. You have no moral right to rule

²For a brief history of the technological development, see e.g. the webpages at <http://www.isoc.org/internet/history/> [19 July 2005].

us nor do you possess any methods of enforcement we have true reason to fear.”³

However eloquently stated, this and other comparable manifestos could do little to prevent the eventual imposition of state regulation upon “cyberspace”. The reason is that the internet simply became too important for states to ignore because it interfered with their rules and laws – in many ways. In 1996, for example, U.S. based *Playboy* magazine was granted an order from a court in New York against a company based in Italy that had created an internet site featuring the name *Playmen* on the grounds that – since the website was accessible to viewers in the United States – this constituted a violation of a judgement from 1981 that had banned the Italian company from distributing its *Playmen* magazine in the United States on trademark grounds. The Italian company was ordered to revise its internet site so that all subscription requests from potential United States customers would be denied. In 2000, a French court ruled that the U.S. based internet company Yahoo! had to prevent French citizens from accessing auction sites that were selling Nazi and Ku Klux Klan memorabilia, because a French law prohibits the selling or display of anything that incites racism. Similarly, Germany exerted pressure on the U.S. based auction site eBay not to sell Nazi memorabilia – even though in the United States it is legal to do so for freedom of speech considerations. Both companies eventually complied with the requests, although Yahoo! first sought a ruling from a U.S. court that the French judgement was not enforceable, only to then ban *all* its customers from buying or selling Nazi paraphernalia, and in addition claiming that this move had nothing to do with the legal threats from France (which included a fine of 100 000 French francs per day of non-compliance).⁴ Complying, both Yahoo! and eBay had probably calculated that they stood to lose more from adverse PR and legal costs than they profited from the respective sales, and that they could gain more from concentrating on the sale of non-controversial goods and the growth of their business in both the United States and Europe.

Indeed, e-commerce has been among the fastest growing business areas over the last decade: retail e-commerce in the United States grew at a rate of 28.1% in the first quarter of 2004, when total retail only grew by 8.8%; internet sales in the EU totalled \$86 bn. in 2001, and U.S. consumers are expected to spend \$120 bn. in 2004; total e-commerce, which also includes business-to-business transactions, amounted in the United States to \$1080 bn. in 2001, and to \$430 bn. in the European Union.⁵

Given this degree of economic volume, access to each other’s e-commerce markets was of great importance to both the United States and the European Union. But the problem of divergent laws and regulations became ever more pressing in the new context of commerce in cyberspace, as cross-border transactions made the mismatch between boundless economic space and territorially based jurisdictions very clear. And since

³ Available at <http://homes.eff.org/~barlow/Declaration-Final.html> [19 July 2005].

⁴ More details on this case can be found e.g. at <http://news.bbc.co.uk/1/hi/world/europe/1032605.stm> [19 July 2005] which also gives further links. See also, for a more general analysis of the role of states in regulating the internet, Drezner (2004).

⁵ All figures after UNCTAD (2004) and *The Economist*, 15 May 2004: 9.

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 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).⁶ 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 on-line, 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.⁷ 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

⁶More comprehensive comparisons of international privacy regulations can be found in Michael (1994) and Electronic Privacy Information Center and Privacy International (2004).

⁷For 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.

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 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.

3 Transatlantic privacy dispute I: e-commerce and the “Safe Harbour” 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 1995.⁸ 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.

⁸This section draws on the descriptions of the “Safe Harbour” negotiations in Long and Quek (2002), Farrell (2003), Regan (2003), and Kobrin (2004).

Notice: Organizations must notify individuals about the purposes for which they collect and use information about them. They must provide information about how individuals can contact the organization with any inquiries or complaints, the types of third parties to which it discloses the information and the choices and means the organization offers for limiting its use and disclosure.

Choice: Organizations must give individuals the opportunity to choose (opt out) whether their personal information will be disclosed to a third party or used for a purpose incompatible with the purpose for which it was originally collected or subsequently authorized by the individual. For sensitive information, affirmative or explicit (opt in) choice must be given if the information is to be disclosed to a third party or used for a purpose other than its original purpose or the purpose authorized subsequently by the individual.

Onward Transfer (Transfers to Third Parties): To disclose information to a third party, organizations must apply the notice and choice principles. Where an organization wishes to transfer information to a third party that is acting as an agent, it may do so if it makes sure that the third party subscribes to the safe harbor principles or is subject to the Directive or another adequacy finding. As an alternative, the organization can enter into a written agreement with such third party requiring that the third party provide at least the same level of privacy protection as is required by the relevant principles.

Access: Individuals must have access to personal information about them that an organization holds and be able to correct, amend, or delete that information where it is inaccurate, except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question, or where the rights of persons other than the individual would be violated.

Security: Organizations must take reasonable precautions to protect personal information from loss, misuse and unauthorized access, disclosure, alteration and destruction.

Data integrity: Personal information must be relevant for the purposes for which it is to be used. An organization should take reasonable steps to ensure that data is reliable for its intended use, accurate, complete, and current.

Enforcement: In order to ensure compliance with the safe harbor principles, there must be (a) readily available and affordable independent recourse mechanisms so that each individual's complaints and disputes can be investigated and resolved and damages awarded where the applicable law or private sector initiatives so provide; (b) procedures for verifying that the commitments companies make to adhere to the safe harbor principles have been implemented; and (c) obligations to remedy problems arising out of a failure to comply with the principles. Sanctions must be sufficiently rigorous to ensure compliance by the organization. Organizations that fail to provide annual self certification letters will no longer appear in the list of participants and safe harbor benefits will no longer be assured.

Table 1: Safe Harbour principles (source: see text)

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 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 (see Table 1)⁹ 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.

4 Transatlantic privacy dispute II: Terrorism and 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.¹⁰

⁹From http://www.export.gov/safeharbor/sh_overview.html [19.7.2005].

¹⁰There are four major CRSs, only one of whom – AMADEUS – is located in the European Union, while the others are in the United States. Information in this section draws on European Parliament Report A6-0226/2005 (4.7.2005), the chapter on travel privacy in Electronic Privacy Information Center

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 contain 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. The goal of the U.S. side was set out in a State Department document as negotiating “an agreement with the EU that gives CBP and TSA [Transportation Security Administration, A.B.] permanent access to PNR data” after which such access should be won on a global basis.¹¹ In other words, complete access to foreign PNR data should be granted, without any control. The EU found these demands unacceptable, as its Internal Market commissioner Frits Bolkestein made clear repeatedly. In a speech given before the European Parliament’s Civil Liberties committee on 9 September 2003 he declared that so far the Commission could not regard the requirements of “adequate protection” under the Data Protection Directive to have been met and pointed out four principal shortcomings in the negotiations up to then:¹²

- that the U.S. was not prepared to limit the use of PNRs to terrorism and terrorism-related crimes;
- that 39 PNR elements were required by the U.S. which was “not proportionate to the purpose”;
- that the U.S. still demanded a very long PNR data storage period of 6 to 7 years;¹³
- and that there was “insufficient legal bindingness of the U.S. undertakings” (i.e. that the rights agreed were not actionable before U.S. courts).

After further negotiations, however, Bolkestein announced on 16 December 2003 that a compromise had been reached. The European Commission issued an “adequacy ruling” on 14 May 2004, and two weeks later an agreement was signed between both sides in Washington. Testing it against the criteria Bolkestein had set out six months ago makes clear that the U.S. side largely prevailed with its demands:

and Privacy International (2004), and the “Opinion 6/2002 on transmission of Passenger Manifest Information and other data from Airlines to the United States” by the EU Article 29 Working Group (adopted 24 October 2002).

¹¹Cf. the “FY 2005 Performance Plan” at <http://www.state.gov/s/d/rm/rls/perfplan/2005/html/29302.htm> [1.8.2005].

¹²See also his op-ed commentary “Resisting U.S. demands: Passenger privacy and the war on terror” in the *International Herald Tribune* of 24 October 2003 which makes similar points.

¹³The initial U.S. demand had been 50 years.

1. PNR record locator code
2. Date of reservation
3. Date(s) of intended travel
4. Name
5. Other names on PNR
6. Address
7. All forms of payment information
8. Billing address
9. Contact telephone numbers
10. All travel itinerary for specific PNR
11. Frequent flyer information (limited to miles flown and address(es))
12. Travel agency
13. Travel agent
14. Code share PNR information
15. Travel status of passenger
16. Split/divided PNR information
17. E-mail address
18. Ticketing field information
19. General remarks
20. Ticket number
21. Seat number
22. Date of ticket issuance
23. No show history
24. Bag tag numbers
25. Go show information
26. OSI information
27. SSI/SSR information
28. Received from information
29. All historical changes to the PNR
30. Number of travellers on PNR
31. Seat information
32. One-way tickets
33. Any collected APIS (Advanced Passenger Information System) information
34. ATFQ (Automatic Ticketing Fare Quote) fields

Table 2: PNR data elements required by CBP from air carriers (Source: EU website)

- PNR data could be used for “preventing and combating: 1. terrorism and related crimes; 2. other serious crimes, including organised crime, that are transnational in nature; and 3. flight from warrants or custody for the crimes described above”;
- 34 PNR elements would be transmitted (see Table 2);
- 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 Chief Privacy Officer of the Department of Homeland Security who “will review the situation and endeavour to resolve the complaint”.

Furthermore, the data given to the CBP can be shared within the Department of Homeland Security (DHS), which is a vast umbrella organisation encompassing 22 formerly independent federal agencies (including the CBP) with more than 170 000 employees (Kettl 2004). Assurances by the DHS against “bulk sharing” of data with other federal agencies are thus of questionable value.

Consequently, the agreement met criticism from the working party of EU national data protection officers¹⁴ and from the European Parliament, which had already been very critical of the provisional agreement for PNR transfer and had voted with 445 to 31 (with 21 abstentions) in October 2003 to bring the PNR transfer into line with EU data protection legislation. 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. Two years later, on 30 May 2006, the European Court annulled 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.

5 Transatlantic privacy dispute III: Terrorism and international payments data

On June 23, 2006, barely three weeks after the court decision about the PNR case, the *New York Times* published a story revealing another case that has been causing privacy related disagreement across the Atlantic since, namely the U.S. administration’s secret

¹⁴See 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.

gaining of access to 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 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 access to these transaction data for the purposes of their “Terrorist Finance Tracking Program” (TFTP).¹⁵ Initial plans to do so covertly were vetoed by the U.S. Treasury (UST), and the administration decided to seek access to the data through direct contact with SWIFT. It did so by serving 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.¹⁶ 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.

Although it is neither a payment nor a settlement system, SWIFT is (by agreement of the central banks of the G-10 countries) supervised by the National Bank of Belgium as the lead overseer in cooperation with the other G-10 central banks. According to press reports,¹⁷ SWIFT demanded guidance from the Belgian, British, United States and European Central banks on how to proceed with the subpoenas, but received none. SWIFT thus saw itself as having to choose between three options:¹⁸

1. comply with the subpoenas (without obtaining any privacy protections);
2. refuse to comply and risk that the UST would enforce the subpoenas via a court action (which would have most likely resulted in SWIFT losing any ability to obtain privacy protections); or

¹⁵The narrative of the events described here is based on Lichtblau and Risen (2006), the report of the Article 29 Group of European Data Protection Officers (Opinion 10/2006, adopted 22 November 2006), the German Data Protection Officer’s report 2005/06, the German government’s answer to a parliamentary question regarding the matter (BT Drs. 16/2741, 27 September 2006), the Canadian Privacy Commissioner’s Report of Findings (2 April 2007), the 2005 Annual Report of SWIFT, information from the SWIFT website (<http://www.swift.com>), and various press reports further detailed below.

¹⁶The other SWIFT data processing centre is located in an EU member state.

¹⁷See the website of German financial daily *Handelsblatt*, http://www.handelsblatt.com/news/printpage.aspx?_p=200051&_t=ftprint&_b=1100064 (accessed 11 July 2006).

¹⁸See the Canadian Privacy Commissioner’s report, paragraph 31.

3. choose to negotiate with the UST to obtain the best level of privacy protection.

SWIFT chose option 3 and negotiated privacy protections with the U.S. Treasury,¹⁹ but then handed over the data. The amount of data obtained by the U.S. Treasury is disputed: while the *New York Times* quotes two sources (among them then U.S. Treasury Secretary John Snow) as saying that SWIFT had agreed to hand over “all the data”, i.e. “the entire Swift database”, the Canadian Privacy Commissioner’s report (paragraph 34) quotes SWIFT as denying that and stating that “it has only ever transferred information pursuant to the subpoenas in accordance with the agreement between it and the UST.” While the amount of data passed on from SWIFT is thus unclear, SWIFT certainly did not notify its member institutions of the subpoenas (no less than 64 between September 2001 and November 2006²⁰ – 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;²¹ 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.²²

A number of data protection agencies in Europe undertook detailed analyses of the case. The German data protection officer, for example, determined that both the mirroring of data to the SWIFT data processing centre in the United States and the passing on of data to U.S. authorities are without legal foundation in German and European law;²³ the Belgian data protection commission similarly concluded that SWIFT had broken fundamental EU data protection rules; and the conference of EU data protection officers

¹⁹According to the Canadian Privacy Commissioner’s report (paragraph 32), they were:

1. The information is to be solely related to terrorism investigations and cannot be used for any other purpose.
2. Limited sets of messages are given (such messages may be relevant to a terrorism investigation; messages may be from anywhere, not simply a particular country).
3. The data remains under SWIFT’s indirect control.
4. The data is protected and kept confidential.
5. SWIFT has a right to monitor and audit the U.S. Treasury compliance with the negotiated arrangement.

²⁰See Article 29 Working Party Opinion 10/2006, p. 8.

²¹See e.g. the German Bundestag debate on 29 March 2007.

²²See e.g. reports in the German daily *Handelsblatt* (11 July 2006) and the Austrian daily *Die Presse* (11 July 2006).

²³See the agency’s annual report for 2005/06: 183. A further detailed analysis of the case is provided by the *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein* (in German) at https://www.datenschutzzentrum.de/wirtschaft/swift/060710_swift.htm (18 July 2006).

(the so-called “Article 29 Working Party”) in its analysis of the case concluded that the European Data Protection Directive was applicable and had been violated. The main reason for this assessment was the fact that the United States did not have the level of data protection required by Article 25 of the European Data Protection Directive, that only the “Safe Harbour” scheme provided adequate protection, but that the latter did not cover financial services.²⁴ The fact that the Canadian Privacy Commissioner’s report states that SWIFT upheld the Canadian privacy law, in addition, puts into sharp relief the fact that the dispute is specifically one between the United States’ actions and European privacy law.

After the Article 29 Working Party’s decision that the current practice was illegal, the Commission declared in late November 2006 that this necessitated talks with the United States. Several months later, German banks who own shares in SWIFT demanded that the company alter its practices, for example by discontinuing the mirroring of purely European transactions to its data processing centre in the United States and restricting the mirroring to such transactions of which at least one party is in the United States.²⁵ Shortly before that, the European Data Protection Supervisor told the European Central Bank that it would have to take action by April 2007 to stop the transfer of personal information from SWIFT to the American authorities.²⁶ In April 2007, SWIFT’s CFO Francis Vanbever revealed in an interview that SWIFT intended to use the “Safe Harbour” concept for its operations in the future.²⁷

From a legal point of view, the case is complicated by the fact that it concerns the interaction of state authorities with a private sector actor, namely SWIFT, because of uncertainties over the obligations the firm was under with respect to European and American legislation. From a political point of view the secrecy with which the U.S. administration carried out the data confiscation is 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.

6 Analysis: Why do the outcomes differ?

Comparing the policy episodes described in the preceding sections of the paper, we find striking differences in outcomes. While the result of the “Safe Harbour” case can be described as a constructive compromise, it is difficult to see the outcome of the PNR episode as anything else than a thinly veiled victory for the American side – a view supported by the court action sought by the European Parliament. In a similar way, U.S. action in the SWIFT case did not even try to reach an understanding with the European side, but instead chose to keep the appropriation of the financial flows data secret. How can these differences be explained?

²⁴See Article 29 Working Party Opinion 10/2006, p. 21, 26.

²⁵See Handelsblatt 29 March 2007.

²⁶See New York Times, 2 February 2007.

²⁷See Handelsblatt, 2 April 2007.

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.²⁸ 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).

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.

The issue of transborder data flows can be approached from different viewpoints, and 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 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.

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. 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 Par-

²⁸Cf. Long and Quek (2002); Farrell (2003); Regan (2003).

liament’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.

Having established that the different cases of transborder data flows led to the actors using different frames – which in itself can account for some difference–, we can go on to look at variables beyond discourse that might shed more light on the reasons for the differences in outcomes. Here we find differences in interests, differences in values, and differences in institutions.

Looking at differences in interests between the actors, we find that there are substantial asymmetries in the first two cases which have likely influenced the outcomes of the respective negotiations – but which have been neglected by constructivist scholars.²⁹ In the “Safe Harbour” case, the United States were in a weaker position compared to the European Union, because they had a strong e-commerce industry that was conducting considerable business in Europe. With the EU being its largest trading partner³⁰ and the site of most U.S. foreign investment, with U.S. controlled affiliates depending on information flows across the Atlantic, and with an information-related industry ranging from credit card companies eager to expand into Europe to information brokers such as LexisNexis, the United States had a vast interest in resolving the dispute and not letting transatlantic data flows be interrupted. Furthermore, the U.S. could not have retaliated against any EU actions under WTO rules, thus having to shoulder most of the costs of a potential conflict. All these factors will likely have contributed to the United States’ willingness to find a constructive compromise that took the shape of the “Safe Harbour” agreement.

In the PNR case, strengths and weaknesses were distributed quite differently: here the European Union found itself in the weaker position, being confronted with the threat of a withdrawal of landing rights for European carriers in the United States.³¹ While the EU stresses that it had to keep the interests of 10–11 million transatlantic passengers in mind, this was also a commercial decision. A huge amount of business was at risk, which might have bankrupted national carriers who would have lost profitable business to their U.S. competitors. And again, no retaliation would have been possible under WTO rules. With the odds against them in this case, the European side will likely have found agreeing to U.S. demands more appealing than fighting for their concept of data protection on grounds of principle.

A closer inspection of the two policy episodes analysed here thus reveals considerable asymmetries. The assumptions made by constructivist scholars about “comparable”

²⁹Since there have been no negotiations between the U.S. and the European sides in the SWIFT case so far, it will be excluded from consideration in the further analysis of this section.

³⁰See Shaffer (2000: 39) for estimates.

³¹Cf. the statement by EU External Affairs Commissioner Patten before the European Parliament on 12 March 2003. See also Opinion 6/2002 by the Article 29 Working Group, adopted 24 October 2002.

bargaining powers between both actors in the “Safe Harbour” case (cf. Long and Quek (2002: 326, 340)) thus have to be refuted, which also casts doubt on their emphasis of argument and persuasion as the central explanatory variables of the result. And if asymmetry in this case has contributed to the outcome, a reverse asymmetry has likely contributed to the result in the PNR case.

But these differences in interests are not the only explanation for the divergences in outcome between the “Safe Harbour” and the PNR and SWIFT cases. There are also deeply rooted value differences concerning privacy, and ongoing differences in institutions between the European and American sides. Both factors can help us further to understand the developments in this policy area.

As briefly pointed out above, conceptions about privacy differ considerably on both sides of the Atlantic, and these differences are deeply rooted. If the U.S. legal approach is akin to a “patchwork”, as quoted above, and almost exclusively directed towards the public sector, the European approach must be characterized as being comprehensive: its privacy regulations apply to public *and* private sectors, they apply to a wide range of activities, impose affirmative obligations, and they have few, if any, sectoral limitations (Swire and Litan 1998: 23).

These different approaches reflect fundamentally divergent regulatory philosophies in the sphere of privacy.³² The European approach sees privacy as a fundamental or human right, which is a precondition for the individual’s autonomy and thus cannot be traded away. The burden of protection rests not with the individual, but with society. Explicit statutes and regulatory agencies to oversee enforcement are the chosen mechanisms for this, and protection can be seen as being proactive, not reactive. Historical experiences with dictatorships such as the Nazis (who used census data for the holocaust) and repressive regimes in East Europe have sensitized Europeans to the importance of data protection. The absence of such experiences, combined with a long tradition of distrust against government, led to a preference for markets and self-regulation in the area of commerce generally and also privacy in the United States. Privacy is seen as a property right rather than a human right, a commodity that is tradeable, and the legal system treats it like private property. Therefore the private sector and free market are seen as the most effective mechanisms for protecting privacy, with the focus being more on the consumer than the citizen. Consequently protection is often more reactive than proactive.

Many scholars expected the existence of the European Data Protection Directive to lead to a “ratcheting up” of U.S. personal privacy standards through a variety of mechanisms such as EU collective action and market clout, firms’ desire to expand their markets and the constraints of supranational trade rules (see, for example, Regan (1993); Shaffer (1999, 2000)). So far, this has not materialized – there has been no comprehensive privacy legislation, and no institutionalisation in terms of a federal agency or a commissioner for privacy in the United States, and there are currently no plans for such a change. This suggests that the fundamental philosophical differences outlined above – on which it is not really possible to compromise – exert a powerful influence in favour of

³²See for example Zwick and Dholakia (2001), Long and Quek (2002: 331f.) or Kobrin (2004: 115f.).

the status quo that is not easily overcome.

Furthermore, the continuing differences in the institutionalisation of privacy matters on both sides of the Atlantic serve as a further reinforcement mechanism for continuing difference. It can probably best be illustrated by the advantages institutional isomorphism might generate: If institutions existed on both sides that had similar remits, they would likely be charged with conducting negotiations about transborder data flow issues, which would facilitate similarity in perspectives and a build-up of trust over repeated interactions in different issue areas. The absence of such an institutional match makes negotiations more difficult because learning is unlikely to take place if each issue is negotiated by a different institution on the American side.

7 Conclusion

This paper has compared three cases of transborder data flows that fall into two different issues areas – business and safety. It has found that transatlantic negotiations over issues of privacy have led to quite different results in the three cases, one resulting in a compromise, while the other two have seen the U.S. position prevail: a substantial acceptance of American demands and a giving in on the part of the European Commission in the PNR case,³³ and completely unilateral U.S. action in the SWIFT case.

This comes as some surprise – not only because scholars had expected U.S. privacy regulations to be “ratcheted up” as a result of the EU Data Protection Directive (as seen in the previous section), but also because initially political scientists had analysed this policy area as leading to “policy convergence” and learning from each other’s experiences, and had projected these trends to continue into the future (see, e.g. Bennett (1991a, b, 1992)). Similarly, scholars taking a “constructivist” approach to the analysis of international negotiations on transborder data transmissions (e.g. Long and Quek (2002); Farrell (2003); Regan (2003)) had pointed out the importance of argument and persuasion in the solution of the case about e-commerce and the “Safe Harbour” agreement, as seen above.

In the light of the case studies presented in this paper, these claims seem questionable now and will need to be reevaluated. This paper has argued that an approach that combines the analysis of “frames” with interests, values and institutions can better account for the differences, explaining both the successful compromise in the “Safe Harbour” case and the rather one-sided results in the PNR and SWIFT cases.

³³The latter assessment is also supported by the stance adopted by the Commission after the ECJ ruling on the PNR case mentioned above. For the Commission did not use the ruling to try to renegotiate the agreement (which might, of course, not have been very successful anyway). Rather, on 19 June 2006, the Commission adopted two initiatives that pledged to renew the agreement, but under the intergovernmental pillar of the Union and using a procedure that would exclude the European Parliament from the decision making process (namely Art. 38 of Title VI of the Treaty on European Union). Thus the European Parliament’s victory before the Court may have spectacularly backfired by depriving it of any influence on the agreement. While the Parliament could try to bring the agreement again before the Court on substantive grounds, there are indications – from the Advocate General’s opinion in this case, dating from November 2005 – that these may not have much merit.

In a more general view, one can speculate that in the post-9/11 world a “policy window” (Kingdon 1995) has opened for political forces aiming to reduce privacy protection. If that were the case, this would surely run counter to all attempts at establishing an international regime in the area of privacy and data protection. While such a wide-ranging hypothesis can ultimately only be supported or refuted by future research, this paper will conclude by offering some analytical considerations about potential scenarios regarding conditions that may help or hinder such an endeavour.

According to Stephen Krasner’s (1983: 186) well-known definition a regime rests (apart from explicit and implicit rules) above all on the expectations of the participating actors. An international data and privacy protection regime would require an considerable number of additional participants beyond the European Union – what expectations concerning their utility would these potential participants have?

Whether regulatory competition will lead to a “race to the top”, i.e. a general rise in the level of protection (often referred to after David Vogel’s (1986) terminology in his study on the proliferation of environmental standards as the “California effect”), or to a competitive lowering of regulatory standards, the dreaded “race to the bottom”, depends on a number of preconditions. Cooperation is more easily achieved

- the more quickly utility gains materialise for all participants,
- the lower the incentives for “free riding” are, and
- the less sensitive the coalition of cooperating actors is against defection.

The fact that “free riders” profit can be an incentive for non-cooperation – for example in the area of tax harmonisation, where non-cooperation can be highly lucrative for single countries if they position themselves as tax havens. On the other hand regulatory standards often create public goods by establishing common points of reference which may contribute to market growth. The international agreements concerning minimum capital standards in international banking are a good example for this – they spread quickly and successfully and can be regarded as indicative for a “California effect”.³⁴

What will the utility gain for cooperating participants in an international privacy and data protection regime likely look like? We can discuss that with reference to a Schelling diagram. It depicts the change in an actor’s utility depending on his or her own choice of strategy and that of the other actors (see figure 1 on the following page). If we limit the choices to “cooperation” and “defection”, then an actor’s utility in the case of cooperation with the regulatory regime is determined by the C-curve; in the case of non-cooperation, by the D-curve. A self-sustaining cooperation will occur if k or more actors cooperate – for then their utility is at least as big as without any cooperation.³⁵ But also in this situation, incentives for defection remain – they will only disappear at point h , when cooperation brings greater utility than defection.

³⁴See e.g. Genschel and Plümper (1997).

³⁵The negative point at which the C-curve intersects with the y-axis is due to the costs incurred by regulation.

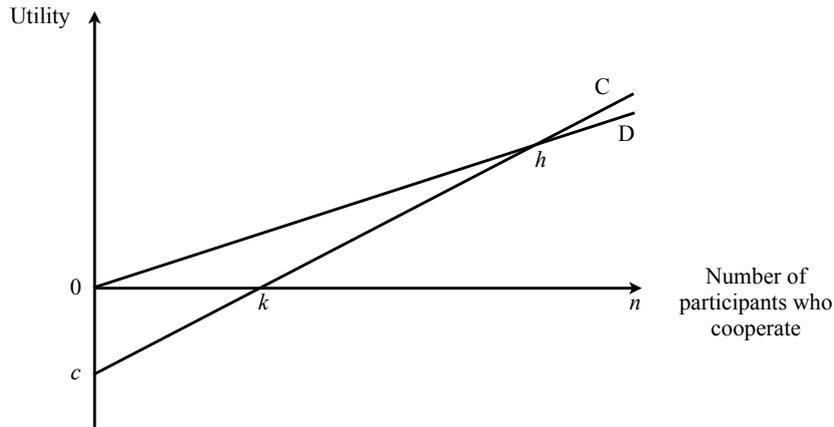


Figure 1: The dynamics of cooperation for an international data protection regime

Obviously, this is only a highly schematic illustration, that is not geared towards the specific case under consideration. But nevertheless we can deduce some general statements from it: since the EU countries already cooperate, we can assume that an international privacy and data protection regime would already be beyond the point k – it might therefore be the case that the EU standard could spread further rather quickly, which obviously depends on the positions of the curves and the degree of their convergence. As mentioned above, figure 1 merely serves as a heuristic device here.

Assumptions in favour of a positive dynamic towards a regime include the fact that acceptance of the existing standard will win outsiders access to the EU data processing market; that there is no alternative regulatory model competing on the international level; and that the early setting of a standard can lead to a “lock-in” with rising costs of exist for all participants – a process particularly likely in technological areas (Pierson 2000). From a regime theory point of view it would be especially interesting that rule-making would then not only occur without the participation of, but even against the interests of the hegemon USA. Indeed, the European Union has in the past been more successful in setting product regulation standards than the United States in a considerable number of areas, as Walter Mattli and Tim Büthe (2003) have demonstrated. Their work also shows that the decisive influence here emanates from the structure of European national and supranational institutions – who manage the task of coordination and information sharing between public and private actors better than is the case in the United States. The same could apply to the area of data traffic.

However, much of the above is speculative, and predictions are, as is generally known, difficult – especially if they concern the future. The influence of the 9/11 attacks has driven home that point quite forcefully, as became evident in several of the sections of this paper. In a similar way, future events could unfold to have a disruptive effect. It would thus seem plausible to sketch two potential scenarios:

- on the one hand, there could be the development towards a relatively stable regime of privacy and data protection that will likely take the EU rules as the common starting point;
- on the other hand, there could be a development that would eschew a coherent international framework of rules in favour of either ad-hoc agreements (as in the case of the passenger name records transmission) or completely unilateral action (as in the case of the SWIFT financial data confiscation).

It would seem likely that the choice between these two scenarios will be determined by the frame dominating this policy area in the next years. If it is that of economic interests, then the regime scenario would appear to be the more likely development; if it is that of security interests, then the ad-hoc and unilateral action scenario would seem the more plausible one.

References

- Agre, Philip and Rotenberg, Marc* (eds.), 1997: *Technology and privacy : the new landscape*, Cambridge (MA); London: MIT Press.
- Bennett, Colin J.*, 1991a: How States Utilize Foreign Evidence, in: *Journal of Public Policy* 11 (1), pp. 31–54.
- Bennett, Colin J.*, 1991b: Review article: What is Policy Convergence and What Causes it?, in: *British Journal of Political Science* 21, pp. 215–233.
- Bennett, Colin J.*, 1992: *Regulating privacy. Data protection and public policy in Europe and the United States*, Ithaca: Cornell University Press.
- Clinton, William J. and Gore, Albert, Jr.*, 1997: *A Framework For Global Electronic Commerce*.
- Drezner, Daniel W.*, 2004: The Global Governance of the Internet: Bringing the State Back In, in: *Political Science Quarterly* 119 (3), pp. 477–498.
- 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.
- Genschel, Philipp and Plümper, Thomas*, 1997: Regulatory competition and international co-operation, in: *Journal of European Public Policy* 4 (4), pp. 626–642.
- Holvast, Jan; Madsen, Wayne and Roth, Paul*, 1999: *The global encyclopaedia of data protection regulation*, The Hague ; London: Kluwer Law International.
- Kettl, Donald F.*, 2004: *System under stress : homeland security and American politics, Public affairs and policy administration series*, Washington, D.C.: CQ Press.
- Kingdon, John W.*, 1995: *Agendas, Alternatives, and Public Policies*, New York: HarperCollins, 2 ed.
- 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.
- Krasner, Stephen D.*, 1983: *International regimes, Cornell studies in political economy*, Ithaca ; London: Cornell University Press.

- 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.
- Mattli, Walter* and *Büthe, Tim*, 2003: Setting International Standards: Technological Rationality or Primacy of Power?, in: *World Politics* 56 (1), pp. 1–42.
- 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.
- Pierson, Paul*, 2000: Increasing Returns, Path Dependence, and the Study of Politics, in: *American Political Science Review* 94 (2), pp. 251–267.
- 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.
- Swire, Peter P.* and *Litan, Robert E.*, 1998: *None of your business : world data flows, electronic commerce, and the European privacy directive*, Washington, D.C.: Brookings Institution Press.
- UNCTAD*, 2004: *E-Commerce and Development Report 2004*, New York, Geneva: United Nations.
- Vogel, David*, 1986: *National styles of regulation: environmental policy in Great Britain and the United States*, Ithaca (NY): Cornell University Press.
- Warren, Samuel D.* and *Brandeis, Louis D.*, 1890: The Right to Privacy, in: *Harvard Law Review* IV (5), pp. 193–220.

Zwick, D. and Dholakia, N., 2001: Contrasting European and American approaches to privacy in electronic markets: property right versus civil right, in: Electronic Markets 11 (2), pp. 116–120.