The regulation of transborder data traffic: Disputes across the Atlantic

Andreas Busch [1]

Introduction

Using the Internet, whether for professional or recreational purposes, has become an everyday activity in recent years.[2] But when we look for news or information on the Internet, do business or exchange chatter with friends and acquaintances through social networks, book our next journey or buy our favourite music, most of us are not aware that these activities cause data traffic across national borders. Very often this is the case, because IT services on the Internet are highly linked internationally. The computer centre reserving a flight between two European states may well be located in the United States of America; a financial transaction between two German banks may well be carried out by an IT service provider based in Ireland; and the carrying out of a business transaction by a multinational firm based in the United Kingdom could easily take place on a server owned by the firm but located in India. Such transactions — probably numbering in the millions every day and indispensable for modern economic life — thus cause streams of data which transcend national borders and therefore often also the borders of jurisdictions. But the data that are being transferred are often very valuable, which is why it is important to protect them. They may be of great commercial value, or they may be person related and thus fall under data protection rules. But the level of protection for such data can vary tremendously between jurisdictions, and that is why international data traffic requires rules that are supranational or international. How such rules come about is the topic of this article.

This article describes and analyses the conflicts, negotiations, and agreements in regulating transatlantic data traffic since the mid-1990s. It covers the negotiations between the USA and the European Union, and it focuses on the different interests, actor constellations, ability to exert pressure and the respective perspectives on the problem of data protection. The empirical core of the article rests on a number of case studies — the 'safe harbor' agreement, the negotiations about the exchange of flight passenger data, and the struggle over access to financial transactions data within the SWIFT network — that have constituted the empirical reality in this area over the last decade and a half.

In political science literature the issue of the transatlantic dispute over the regulation of exchanging personal data has only been treated cursorily so far. The

---

1 Andreas Busch is Professor of Comparative Politics and Political Economy at the Department of Political Science, Georg-August-Universität Göttingen.

2 This article draws on several prior publications by the author as well as research sponsored by the Economic and Social Research Council (grant RES 062–23–0536), the Social Science Research Centre (WZB) in Berlin, and the Hanse Institute for Advanced Study (HWK).

few authors in this field have so far mainly concentrated on describing approaches to regulation of personal data and the respective differences between the European Union and the United States of America.[3,4,5] As far as concrete negotiations in this area have been analysed, the 'safe harbor' agreement negotiated towards the end of the 1990s and focused on the then growth area of e-commerce has been the focus of scholarly interest.[6,7,8,9] But after the terrorist attacks of September 11, 2001 a shift has taken place in the area of cross-border data traffic from a focus on commercial interest towards one on security. Over the last decade, new transatlantic differences about how to regulate cross-border data streams have therefore sprung up. However, these have hardly been reflected in the academic literature, although they took place in a heavily changed context — and with substantially different results than would have been expected according to the analyses following the 'safe harbor' agreement.

The present article therefore contributes three new aspects to the so far existing political science literature on transatlantic data traffic:

- on the one hand, it undertakes an integrated analysis of the field by looking at all three conflict areas that have emerged so far, namely 'safe harbor', passenger name records, and access to financial transactions data;
- secondly, it proposes that the theoretical perspective that has so far dominated analyses in this field, namely constructivism – i.e. a theoretical perspective emphasizing the social construction of interests as well as the importance of ideas, norms, and culture –, should be complemented by other theoretical approaches in order to more fully understand the results of these conflicts;
- and thirdly the article tries to also take into consideration the intra-European dimension of the conflict (i.e. the struggles between the European Commission and the European Parliament) which it is argued

3 Shaffer, Gregory (1999). 'The power of EU collective action. The impact of EU data privacy regulation on US business practice', *European Law Journal,* 5:4, 419–37.

4 Zwick, Detlev, and Nikhilesh Dholakia (2001). 'Contrasting European and American approaches to privacy in electronic markets: Property right versus civil right', *Electronic markets,* 11:2, 116–20.

5 Whitman, James Q. (2004). 'The Two Western Cultures of Privacy: Dignity Versus Liberty', *Yale Law Journal,* 113:6, 1151–221.

6 Long, William J., and Marc P. Quek (2002). 'Personal data privacy protection in an age of globalization:. the US - EU safe harbor compromise', *Journal of European Public Policy,* 9:3, 325–44.

7 Farrell, Henry (2003). 'Constructing the international foundations of E-commerce - the EU - US Safe Harbor arrangement', *International Organization,* 57:2, 277–306.

8 Regan, Priscilla M. (2003). 'Safe harbors or free frontiers? Privacy and transborder data flows', *Journal of Social Issues,* 59:2, 263–82.

9 Drezner, Daniel W. (2004). 'The Global Governance of the Internet. Bringing the State Back In', *Political Science Quarterly,* 119:3, 477–98.

have had considerable influence on the dynamics of conflict in recent years.

The article starts with chapters briefly summarizing questions of the regulation of the internet, and of differences in the approach to data protection across the Atlantic. The empirical core of the article consists of three case studies detailing transatlantic disputes in that field. It is followed by the presentation of an analytical approach that attempts to understand the differences in policy dynamics and results by focusing on actors' differences in framing, and of changes in actor constellations. In concluding the article argues that an analysis focusing on institutional and power variables is best suited to comprehensively explain all three cases of conflicts over the regulation of transatlantic data traffic.

Regulation of the internet

Today we have come to think of the Internet primarily as a medium for commercial transactions (e-commerce) and for social exchange; but the origins of this truly global medium of communication lie in a completely different area. At the beginning of the 1970s, the *Defence Advanced Research Projects Agency* or DARPA (the arm of the US Department of Defence specialised in research) initiated work on a decentralised system of communication that would be able to withstand a massive — possibly nuclear — attack without ceasing to function. Under conditions of the then Cold War, this was an essential requirement, demanding a decentralised structure of communication. In the mid-1980s, the National Science Foundation of the United States then funded the further development of this communication infrastructure for the purposes of research by linking national centres of research excellence and their local communications networks with each other. The result became known as the 'Internet'.[10]

Those developments were initiated and pursued by a small community of technically highly competent experts and thus required little regulation. The few rules that existed were derived from the discussion process with strongly egalitarian characteristics and a high degree of participation; relationships were largely based on trust; and the existing hierarchies in the administration of the network were based on recognised expertise.[11] Some twenty years ago, in the early 1990s, the founding generation of Internet engineers and users therefore dreamt of the development of a truly global communications network that would be devoid of state influence and regulation. Organisations like the Electronic Frontier Foundation (EFF), set up by technologists and proponents of the counterculture, consciously used founding myths of the United States when they referred to the challenges of the 'digital frontier' and spoke of defending the

10 A good historical overview of the development of the internet can be found in Hafner, Katie, and Matthew Lyon (1996). *Where wizards stay up late. The origins of the Internet.* New York: Simon & Schuster.

11 Here above all the 'requests for comments' (RFCs) have to be mentioned. See more at http://en.wikipedia.org/wiki/Request_for_Comments.

rights of the individual in the new 'cyberspace'. They had utopian ideas about how the new medium could be used to improve the world and extend individual liberty, and they refused any regulation enforced from outside. An illustrative summary of this attitude can be found in the 'Declaration of Independence of Cyberspace' written by John Perry Barlow, a founding member of the EFF and lyricist of the 1960s cult band *The Grateful Dead*, in 1996, when commercialisation and enforced regulation threatened to change the existing libertarian Internet:

> '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 us nor do you process any methods of enforcement we have true reason to fear'.[12]

But the eloquence of this and several other, comparable manifests could eventually not prevent an increasing regulation of the Internet by state forces. The main reason was that the Internet simply became too important for states to ignore it. For there was a lot of potential tension between the Internet and state rules, regulations and laws — the tension between a communication structure designed and implemented to be global, and the largely territorially-based rules of nation states and international organisations. While the Internet, according to the views of those who had set it up was to be perceived as one single entity, nation states each had different views about how matters should be conducted in this new space.

Differences in approaching data protection

As the importance of the Internet for commercial profit and economic growth became more evident and more manifest, access to the emerging markets for electronic commerce became ever more important, particularly in the advanced market economies of North America and Western Europe that were spearheading this development. But this also had the consequence that the problem of differing legal and regulatory rules became both painfully clear and pressing in the context of commercial use of cyberspace: there was a clear contrast between the borderless economic space that was emerging on the one hand, and the

12 Barlow, John P. (1996). 'A Declaration of the Independence of Cyberspace'. http://homes.eff.org/~barlow/Declaration-Final.html

territorially bound legal spaces of prior existence. And since electronic commerce largely rested upon the exchange of information, this problem was particularly acute in the field of data protection and privacy where substantially different regulatory approaches had emerged on both sides of the Atlantic.[13]

In the United States of America, protection of privacy by statutory regulation is not very highly developed. In spite of a long debate about the issue which started in the late 19th century with the pathbreaking article by Warren and Brandeis (1890), the legal situation is described by experts as akin to 'a patchwork quilt'[14] and 'fragmented and ad hoc'[15] as well as narrowly confined to specific sectors and problems. Since there is no comprehensive data protection legislation and no political will to pass one, it was attempted to achieve the protection of privacy required for successful e-commerce through self-regulation by industry. The 'Framework for Global Electronic Commerce', authored by President Clinton and Vice President Gore in July 1997 and published by the White House, put it like this:

> '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 ensure personal privacy in the network 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'.[16]

---

13 For an analysis of the differences see Reidenberg, Joel R. (2000).'Resolving Conflicting International Data Privacy Rules in Cyberspace', *Stanford Law Review,* 52, 1315–7; Whitman, James Q. (2004). 'The Two Western Cultures of Privacy: Dignity Versus Liberty', *Yale Law Journal,* 113:6; Feick, Jürgen, and Raymund Werle (2010). 'Regulation of Cyberspace', in: Robert Baldwin, Martin Cave and Martin Lodge (eds.), *The Oxford handbook of regulation.* Oxford: Oxford Univ. Press. An overview of the regulation of privacy can be found in Busch, Andreas (2011). 'The Regulation of Privacy', in: David Levi-Faur (ed.), *Handbook on the Politics of Regulation.* Cheltenham UK Northampton MA: Edward Elgar.

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

15 Shaffer, Gregory (1999). 'The power of EU collective action. The impact of EU data privacy regulation on US business practice', *European Law Journal,* 5:4, 419–37.

16 Clinton, William J., and Albert Gore, JR. (1997). 'A Framework For Global Electronic Commerce'. http://clinton4.nara.gov/WH/New/Commerce/.

In Europe, on the other hand, a substantially different approach was chosen combining regulation both on the level of the nation state and on the supranational level. Beginning in the early 1970s, countries like the Federal Republic of Germany, Sweden, France and Denmark had begun to pass statutes about 'data protection', and this legislation had begun to spread across the whole continent. It aimed to pre-empt dangers to privacy that could emerge from the introduction of computer-based technologies (such as comprehensive databases), and they focused on the right of an individual to protect his or her own data. However, these protection regimes differed in detail from country to country in the European Union, which puts the danger of becoming an obstacle both to trade between them and to the development of e-commerce more widely.

This problem became more acute in the context of the completion of the European single market in the early 1990s. After five years of negotiations, in October 1995 the European directive 95/46/EU 'on the protection of individuals with regard to the processing of personal data and on the free movement of such data' was passed and entered into force in October 1998. The directive decreed that '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 protection of the rights and freedoms of individuals, and in particular the right to privacy' (Preamble, section 9). However, at the same time it introduced regulations that make the transfer of such data to countries outside the European Union dependent on the existence of 'an adequate level of protection' (article 25). In other words: while the directive clearly facilitated trade *within* the European Union, it could be a serious obstacle to electronic trade with states *outside* the European Union (such as the United States), should their regulations concerning data protection not be deemed appropriate.

Case studies on regulating data traffic

Transatlantic dispute I: The 'Safe Harbor' agreement

The background for the first transatlantic dispute about the regulation of cross-border data traffic was formed by three things: the differences in regulatory philosophies described in the previous section, the initiative to pass an EU directive on data protection, and the frantically growing field of electronic commerce. Given the close economic and trade relations between the European Union and the United States, one could have expected negotiations on the topic of transatlantic data traffic to start immediately after the EU directive had been passed in 1995. But this was not the case. Rather, the United States assumed that they would obviously be granted the exception clause of article 26 of the directive without problems and therefore there would be no disruption in data traffic. Serious discussions only started in the first half of 1998 when the US administration became aware that this might not be so.

Initially the positions of both sides were characterised by the expectation that the other side would accept to change their regulatory approach. EU

representatives made it clear that according to their view only the introduction of formal statutory regulation — i.e. a comprehensive law on data protection — and a supervisory authority — i.e. the equivalent of the data protection commissioner — could win the United States the recognition of an appropriate level of protection for personal data. The United States on the other hand further pursued their strategy of relying on independent certification agencies in the private sector for the protection of privacy. These should grant a seal of certification to Internet websites, and it was expected, that this approach would spread across countries, gaining international recognition and thus ending the differences of opinion with the European Union.[17] But even in the United States the self certification approach did not really take off: a number of firms requesting certification of their websites by agencies such as TRUSTe or BBBOnline remained low, thus strengthening the doubts about the effectiveness of the US approach of self-regulation.

A blockade threatened. It was only avoided when the American lead negotiator David Aaron suggested the concept of a 'safe harbor' — a number of principles to which companies could subscribe and which in turn would be recognised as 'adequate protection' under the EU directive. This suggestion transformed the negotiations. For the first time, a solution seemed possible that would combine a solution to European worries about the protection of privacy and personal data with avoiding comprehensive institutionalisation and legislation in this field by the United States. Even though several EU member states remained critical, a compromise between the United States and the EU commission was struck more or less along these lines. US firms could commit annually to keeping seven principles drawn up by the US Department of Trade in cooperation with the EU according to their data protection principles. The Federal Trade Commission would publish a list of these firms on a website, and a breach of keeping the commitment would constitute a breach of the Federal Trade Commission Act, thus subjecting the firm to legal procedures. The European Commission would resolve to recognise this procedure as constituting 'adequate protection' under its data protection directive.

The 'safe harbor' agreement thus neither constituted a recognition by the EU of the system practised in the United States, nor did it extend the EU system of formal legislation and institutionalisation to the United States. Instead it differed in quality from both and thus created something new — a fact that was lauded by many commentators and described as particularly appropriate for the lack of congruence between economic and political spaces as well as the problem of regulatory spill-over between different jurisdictions. Both politicians and academics judged it to be a success and a model solution for future agreements in this area, when it entered into force in November 2000.

17 Farrell, Henry (2003). 'Constructing the international foundations of E-commerce – the EU-US Safe Harbor arrangement', *International Organization,* 57:2, page 288.

Transatlantic dispute II: Terrorism and flight passenger data

But less than a year later, conditions for agreements about the regulation of transatlantic data traffic change substantially after the terrorist attacks of September 11, 2001. This first became evident in the area of flight passenger data.

When booking, paying for or actually boarding a flight, person-related data are being created for each passenger which will then be electronically stored and processed. Such flight passenger data exist in the form of so-called passenger name records (PNR), and they are created by airlines for each journey a passenger books. PNRs are usually held in a computerised reservation system (CRS), and they contain the name of the traveller, details of flights, hotels, car rentals, and other travel services. Furthermore they contain residential and business postal and email addresses as well as phone numbers, credit card details, and names and personal information of emergency contacts. In addition — through billing, conference, and discount eligibility codes — PNRs can give information about memberships and organisational affiliations as well as religious meal preferences and details about physical and medical conditions. We can conclude that PNRs can be regarded as sensitive personal information.

After the attacks of September 11, 2001 the United States decided to use data from PNRs in their fight against international terrorism. On November 19, 2001, Congress passed the 'Aviation and Security Act' which required airlines operating passenger flights to, from or through the United States to provide the US Bureau of Customs and Border Protection (CBP) with electronic access to PNR data contained in their reservation and departure control systems before takeoff or at least 15 minutes after departure. As those data, being highly sensitive and personal in nature, fall under the EU data protection directive, this created a regulatory conflict between the United States and the EU requiring negotiations. To convey the importance of their position, the United States threatened to withdraw landing rights from all EU airlines unless the required data were handed over.[18]

A provisional agreement in March 2003 resolved a first pressing conflict by allowing European airlines to provide PNR data to the CBP without being penalised for this by European authorities. Negotiations then took place throughout 2003 between the European Commission's Directorate-General for the Internal Market (which is responsible for data protection) and the US Department of Homeland Security about these data transfers. Although the EU side initially found the US demands unacceptable,[19] in December 2003 it agreed to a solution that largely accepted those demands:

---

18 Busch, Andreas (2006). 'From Safe Harbour to the Rough Sea? Privacy Disputes across the Atlantic', *SCRIPT-ed. A Journal of Law and Technology,* 3:4, page 317. http://www.law.ed.ac.uk/ahrc/script%2Ded/vol3-4/busch.asp.

19 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.

- PNR data could be used for more than fighting 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[20] 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. Some two years later, on May 30, 2006, the ECJ annulled both the Council of Ministers' decision about the agreement with the USA and the Commission's 'adequacy of protection' decision (cases C-317/04 and C-318/04). However, this ruling was based solely on an assessment of formal competences: the Court found that the Council of Ministers acted ultra vires when it concluded the agreement, and that the Commission overstepped its competences when issuing the adequacy ruling. The Court thus did *not* pronounce on the substantive matter regarding the protection of privacy and the breach of fundamental rights. Further negotiations resulted in a new agreement between the EU and the United States in July 2007.[21] In sum it resulted in concessions to the American side, by extending the storage period from 3.5 to up to 15 years and granting access to more federal agencies. European preferences were taken into account by changing access from a *pull* to a *push* procedure, i.e. disabling direct American access to the booking systems. The reduction in the number of data types from 34 to 19, however, must be assessed as a face-saving exercise for the European side as it was almost completely accomplished by adding up positions in the enumeration.[22]

20 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 CPB)', adopted 29 January 2004.

21 Available at http://register.consilium.europa.eu/pdf/en/07/st11/st11595.en07.pdf (12.3.2013).

22 This is evident if one compares the positions in the 2007 agreement with those in the 2004 Commission Decision available at http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:235:0011:0022:EN:PDF (12.3.2013).

Transatlantic dispute III: Terrorism and financial transaction data

Barely three weeks after the court decision about the PNR case, on June 23, 2006, the New York Times published a story[23] revealing another case causing privacy related disagreement across the Atlantic, namely the US 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 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 US 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.[24] 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,[25] SWIFT certainly did not notify its member institutions of the subpoenas (no less than 64 between September 2001 and November 2006[26] — or on average one per month) and therefore of the transfer of data to US authorities.

After the existence of the TFTP program had been published and acknowledged by the US 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

23 Lichtblau, Eric, and James Risen (2006). 'Bank Data Sifted in Secret by US to Block Terror', *The New York Times,* 1.

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

25 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).

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

knowledge of the program; member state parliaments debated the issue and criticised the US administration's actions strongly;[27] 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.[28] However one may ultimately judge these allegation, it is safe to say that the secrecy with which the US 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 US administration to choose that route. It clearly was not concerned by regards about balancing differences in interests or considerations of partnership.

Theoretical perspectives

Political science analyses of transborder data flows between the US and the EU have so far focused on the 'safe harbor' case and have primarily analysed it from a 'constructivist' viewpoint.[29] This perspective emphasizes the importance of values, norms, and discourse over conventional, 'realist' analyses of power in international relations. With respect to the 'safe harbor' 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 US 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'.[30]

However much this may indeed have been the case in the 'safe harbor' 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 two cases, far from there being persuasion and argument, quite clearly the United States prevailed, achieving their goals of unhindered access to

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

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

29 Cf. Long, William J., and Marc P. Quek (2002). 'Personal data privacy protection in an age of globalization:. the US-EU safe harbor compromise', *Journal of European Public Policy,* 9:3, 325-44; Farrell, Henry (2003). 'Constructing the international foundations of E-commerce -- the US-EU Safe Harbor arrangement', *International Organization,* 57:2, 277-306; Regan, Priscilla M. (2003). 'Safe harbors or free frontiers? Privacy and transborder data flows', *Journal of Social Issues,* 59:2, 263-82. An exception is Heisenberg, Dorothee (2005). *Negotiating Privacy. The European Union, the United States, and Personal Data Protection.* Boulder (CO): Lynne Rienner Publishers.

30 Farrell, Henry (2003). 'Constructing the international foundations of E-commerce - The US-EU Safe Harbor arrangement', *International Organization,* 57:2, 277–306.

passenger name records and financial transfers data without effective control by the European side over their further use — which clearly goes against 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 next sections will argue that this is best achieved by taking into account differences in framing the problem, and considering institutional variables.

Three 'frames' on the issue

The dispute about transborder data flows is one that can be approached from different viewpoints, and therefore different actors can take different positions with respect to these viewpoints. As a consequence, both the relevant facts in a contested area as well as the goals to be achieved in the respective disputes and negotiations are not fixed, but are themselves legitimately under discussion. In social science terminology this is known as framing.[31] The convictions, perceptions, and valuations that underlie the policy positions of actors are designated as frames, and policy controversies between actors are being interpreted as conflicts between their respective frames.[32] It is these frames that produce interpretations which turn a diffuse and complex reality into a concrete situation by selecting facts as important. Frames therefore on the one hand define the precise nature of the problem and also what counts as a fact and which arguments are relevant and convincing. If actors interpret a policy topic through different frames, the underlying controversy will be difficult to solve, in particular if these frames are not openly addressed or defined. In international negotiations it has often been the fact that the definition of a problem is a decisive step towards setting the agenda and towards progress in the policy process.[33]

For the issue of transborder data flows we can assume the existence of different frames that are determined by the different characteristics and the multitude of different uses for such data. They are

- on the one hand a perspective of *economic interests*, which focuses on aspects like cost efficiency, profitability, and an increase in market share;
- on the other hand a perspective of *security interests* which centres on the minimisation of risk and the prevention of misuse of data;

31 Schön, Donald A., and Martin Rein (1994). *Frame reflection. Toward the resolution of intractable policy controversies.* New York: Basic Books.

32 See Rein, Martin, and Donald A. Schön (1996). 'Reframing Policy Discourse', in: Frank Fischer and John Forester (eds.), *The Argumentative Turn in Policy Analysis and Planning.* London: Duke Univ. Press, 23-6.

33 See Mitchell, Ronald B. (2002). 'International Environment', in: Walter Carlsnaes, Thomas Risse and Beth A. Simmons (eds.), *Handbook of international relations.* London, Thousand Oaks, New Delhi: SAGE, 500–16.

- and lastly a perspective of *civil rights interests* which emphasises the protection of privacy and freedom of information.

We can hypothesise that the different frames will likely be used by different classes of actors who make their choice based on their respective interests and definitions of the situation:

- The 'economic interests' frame will likely be chosen by commercially oriented actors such as firms[34] and market-oriented actors in the bureaucracy such as regulatory agencies who supervise and regulate markets. 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 while wanting to realise 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, their interests and thus the collective perspectives on the issue of regulating transatlantic data traffic will enable us to achieve a more precise and more clearly distinguishing analysis of the case studies than using only the interpretation from a constructivist point of view that has been dominating the literature so far. As was mentioned above, this approach dominated the political science literature on the 'safe harbor' case[35,36,37] and the

34 Unless their business is in the security industry, which would likely make them adopt the 'safety interests' frame.

35 Long, William J., and Marc P. Quek (2002). 'Personal data privacy protection in an age of globalization:. the US - EU safe harbor compromise', *Journal of European Public Policy,* 9:3, 325–44.

authors subscribing to this approach had always emphasised the important role played by social norms in resolving this conflict. In addition it had been pointed out that the agreement was characterised by neither subscribing to US preferences for self-regulation through the EU nor by extending the European system of comprehensive data protection legislation to the United States; instead, it constituted something genuinely new. Through deliberation the two parties have succeeded in finding a common solution in spite of initial positions in the negotiations that seemed incompatible — and, what is more, one that might have repercussions upon the regulatory systems both in the EU and the US. Approaching a solution by iterative dialogue seems to show that cooperation between nation states was possible without one side dominating the solution or the outcome being a blockade or a trade conflict. Thus the 'safe harbor' solution was widely regarded as a model for future solutions in the area of regulating transatlantic data traffic both from an academic point of view, and by politicians: Pat Cox, the former president of the European Parliament considered the agreement 'a template for the future'.[38] From today's perspective these expectations sound excessively optimistic. For developments in the regulation of transatlantic data traffic over the last decade have deviated considerably from the expectations uttered after the conclusion of the 'safe harbor' agreement. In the light of more recent disputes between the transatlantic partners — over the transmission of flight passenger data and access to international financial transactions data — these expectations will have to be re-evaluated.

Changing actor constellations

In the course of the last decade, substantial change has been evident in the field of regulating transatlantic data traffic. When negotiations first started in 1998, the perspective of economic interests and common profit through increased international trade was clearly dominant; however, as the two case studies of transferring flight passenger and financial transactions data made clear, circumstances changed considerably after the terrorist attacks of September 11, 2001. The frame of security interests became the dominant one, especially for the United States of America. According to the expectations outlined above, risk minimisation and the maximisation of security now dominated concentrations, and the costs in terms of privacy and Civil Rights incurred in striving for the most comprehensive collection of data possible was largely ignored.[39] But

36 Regan, Priscilla M. (2002). 'Privacy as a Common Good in the Digital World', *Information, Communication & Society,* 5, 264.

37 Farrell, Henry (2003). 'Constructing the international foundations of E-commerce -- the US - EU Safe Harbor arrangement', *International Organization,* 57:2, 297–302.

38 Cited after Farrell, Henry (2003). 'Constructing the international foundations of E-commerce – the US - EU Safe Harbor arrangement', *International Organization,* 57:2, 298.

39 An extreme case for the extent of data collection that was initially being considered is the *Total Information Awareness* project started by DARPA after the terrorist attacks which aimed at literally linking all available data (see O'Harrow, Robert (2006). *No Place to Hide. Behind the Scenes of of our Emerging Surveillance Society*. New York, NY: Free Press, and appendix

respective American demands were met by a European position striving to keep up the established standards of data protection and to defend them. Here the European Commission played an important role, acting (at least in the case of flight passenger data) as the United States' negotiation partner and processing the new conflict internally through the same mechanisms as in the 'safe harbor' case, mainly through the Directorate General for internal market affairs. Thus on the European side a frame emphasising economic interests continued to dominate, while on the American side actors had changed – to CBP and the new Department of Homeland Security, who were focusing almost exclusively on security interests. Faced with an American threat to withdraw landing rights for European carriers, the EU initially largely accepted demands for data transfer.

Within Europe, however, this perceived softness of the European Commission had considerable consequences. For it led to the European Parliament accusing the Commission of ignoring European data protection legislation and taking it to the European Court of Justice. Thus the transatlantic conflict was complemented by an intra-European Union one which highlighted the fact that considerable divergences of interests and positions existed within the European Union in this area. An important consequence of this conflict was the forced change of the actors in charge of negotiations on the European side as a consequence of the Court's ruling in 2006. For the Court ruled that under the existing EU treaties neither the Council of ministers nor the Commission had acted within the competences when reaching the agreement with the United States and testifying an 'appropriate level of protection' in the United States with regard to the EU data protection directive. As a consequence the whole matter was shifted (using Maastricht Treaty terminology) from the supranational 'first pillar' of European cooperation to the intergovernmental 'third pillar' of cooperation in justice and domestic affairs. This forum shift resulted in a change of actors on the European side: rather than the DG Internal market, it was now the national ministers of justice and domestic affairs together with the then EU Commissioner in charge of the justice portfolio, Franco Frattini, who called the shots for further negotiations. Their preferences were much more clearly aligned with the frame dominated by security concentrations than had been the case with DG internal market.

The European Parliament's legal action had thus resulted in an initial success, because the existing agreement with the United States on flight passenger data had to be annulled. But this success had unintended consequences insofar as the ensuing negotiations were now conducted on the European side, too, by actors who viewed the problem of data transmission very much through a frame of security interests. This was not aligned with the preferences of the European Parliament; but having once chosen the route through the Court this could no longer be changed. Furthermore, shifting the matter from the first to the third pillar also resulted in considerable weakening of the Parliament's

J in National Research Council (2008). It was renamed to *Terrorist Information Awareness* before its funding was discontinued.

participatory rights and thus little influence on the results of the new negotiations.

One could have assumed that the aforementioned changes would plausibly lead to a substantial convergence of transatlantic policy positions which would facilitate the conclusion of a new agreement. But this was only the case in a very limited way. Negotiations dragged on until the end of 2009, when yet another change in the constellation of actors further complicated an agreement. The reason was the entry into force of the Treaty of Lisbon on December 1, 2009 which substantially broadened the competences of the European Parliament in matters falling under the third pillar. Since prior to that date a substantial polarisation had taken place between the Parliament on the one side and the Commission and the Council on the other side (with the former suspecting that the latter were trying to push through a solution rejected by the Parliament while the old rules were still valid), already in February 2010 Parliament demonstrated its new veto power by rejecting the new interim agreement on SWIFT with a substantial majority.

The actor constellation had thus considerably changed twice between 2006 and 2010, once through the forum shift from the first of the third pillar of the European Union, and the second time through the entry into force of the Treaty of Lisbon with its increase in European Parliament decision powers. While the first resulted in a change in the European negotiation partners dominant perspective on the issue of transatlantic data traffic, this was not so in the second case. Still both changes illustrate that not only framing, but also institutional variables (such as the composition of the negotiation group and the decision rules and veto powers of particular actors) are of essential importance for the analysis of the regulation of transatlantic data traffic.

Conclusion

The technological and economic developments of the last two decades have resulted in an enormous increase of the extent and density of international data traffic and have thus led to the question of how to regulate that cross-border exchange of offering very sensitive data gaining great importance. As this article describes, a multitude of everyday activities in today's economic and private life is linked to the initiation of streams of data which often cross national boundaries; yet still the level of protection that such exchange of data enjoys varies greatly in international comparison. While there have been substantial regional attempts at harmonisation as well as successes in this area (e.g. within the European Union, but also within APEC), we are still far from achieving a unitary level of protection[40].

[40] See Busch, Andreas (2011). 'The Regulation of Privacy', in: David Levi-Faur (ed.), *Handbook on the Politics of Regulation.* Cheltenham UK Northampton MA: Edward Elgar, 227–40", for an overview.

This article has focused on the question how differences in the regulation of cross-border data traffic are being dealt with in the face of an increasing political and economic importance of this area, by looking at the disputes between the United States of America and the European Union. Given the close economic linkage between these two highly developed markets and the fact that the topic was initially seen as a primarily commercial one, a compromise over the regulation of cross-border data traffic between both jurisdictions was in the interest of all involved parties. In the shape of the 'safe harbor' agreement it also came about in November 2002 and was seen as an innovative and exemplary solution for future regulations in this field both in the scholarly literature and by political actors.

But the terrorist attacks of September 11, 2001 only a short time later led to a shifting of the dominant interpretive frame in the area of the regulation of cross-border data traffic from commerce to security. As this article has described in some detail, this shift in framing also meant the end of the good understanding between the USA and the European Union in this field. Rather than agreeing on compromises and attempting to take into account the other side's interests, increasingly one-sided action prevailed, as the USA (perceiving a substantial security threat) tried to dictate the conditions for access to transatlantic data, even taking refuge to threats such as the withdrawal of landing rights for European air carriers.

In political science literature the analysis of the regulation of cross-border data traffic has so far been dominated by a constructivist approach which focuses on values and norms and emphasises the importance of discourse and dialogue. But the increasing securitisation in this field and the changing reactions over time of the actors involved cannot really be explained by this approach. It needs to be augmented — not replaced! — by other analytical perspectives, and at this article argues, two of them seem to be particularly promising:

- on the one hand a distinction between the different frames by which actors view and interpret the topic in question and based on which they pursue their interests; and
- the consideration of institutional facts, especially with regard to the competences of actors and the convergences and divergences of interests between them. During the course of the last decade considerable changes in actor constellations have taken place, in particular on the European side. The increased power of the European Parliament resulting from the Treaty of Lisbon has led to considerable potential for blockade which has more than equalised the prior loss of influence resulting from the European Court of Justice's ruling and the ensuing forum switch. Strangely, the American side has so far not taken that fundamental shift into account in its negotiation tactics.

Taking these two additions into account, the present article manages to explain why we find such different dynamics and results in the three case studies of the

regulation of transatlantic data traffic. It can also show that today's positions of actors are to a considerable extent influenced by historically deeply rooted differences in the perception of state roles in general and the regulation of access to personal data in particular. A European approach of seeing such regulations as a task for the state to be achieved through legislation with the primary goal of the protection of the individual contrasts with US preferences which regard freedom of contract for the individual as of primary importance also in this field and therefore see voluntary agreements as the appropriate instrument.

For the area of transatlantic negotiations we can conclude from the latter a preference for concrete, single issue solutions, while the former would lead to a preference for general and comprehensive agreements. It is difficult to see how these two different standpoints can be reconciled. The challenge for the negotiation partners will be to break free from the previous cycle of attempted diktat at a solution, followed by blockade of a permanent agreement and refuge to a temporary solution. Whether this will succeed or not, it seems certain that this field will in the months and years to come provide further material for interesting political science case studies in the field of regulating privacy.