TRANSWORLD

THE TRANSATLANTIC RELATIONSHIP AND THE FUTURE GLOBAL GOVERNANCE

ISSN 2281-5252 WORKING PAPER 19 | APRIL 2013

Transatlantic Tensions on Data Privacy

The paper analyses similarities and differences between US and European regulatory policy in the field of data privacy. It shows that US regulation in the field is not uniformly weaker than European regulation. It also argues that while European policy preferences in the field have been more globally influential than US preferences, the latter have also shaped the outcomes of the former, resulting in a transatlantic co-production of norms.

Lee A. Bygrave

Transworld is supported by the Seventh Framework Programme

SEVENTH FRAMEWORK PROGRAMME

Transatlantic Tensions on Data Privacy

Lee A. Bygrave*

United States European Union Data privacy Regulatory policy

Introduction

This paper focuses on US and European regulatory policies in the field of data privacy. These policies concern, at bottom, information processing and the infrastructure for such processing. Protection of human rights plays a key role in the field.

Rules on data privacy specifically govern the processing of data relating to persons (i.e., personal data) in order to protect, at least partly, the privacy and related interests of those persons. In Europe, such norms tend to be described as "data protection". Outside Europe, including the USA, they are often described in terms of protecting "privacy" or "information privacy" (Bygrave 2010:166). As elaborated further below, significant elements of these norms are formally grounded in human rights, particularly the right to privacy. Thus, human rights and accompanying doctrine provide a central normative basis for data privacy law, while much of the latter can be seen as both an expression and specialised branch of the former.

Focus on data privacy is justified on several grounds. First, while the transatlantic dialogue on data privacy has given rise to a considerable amount of policy convergence and consensus, it has also involved conflict, controversy and regulatory divergence. At the same time, the dialogue has often been intense, with each side exercising a marked degree of influence on the other across multiple planes, including the political, economic and academic. Additionally, the tensions in the US-European dialogue have had a significant impact on broader international policy initiatives – in other words, they have affected not just the USA and Europe but large parts of the rest of the world. Thus, depiction of the conflict as a "clash of data titans" (Charlesworth 2000) is apposite. This is not to say that similar tensions have been absent between other constellations of countries, but the tensions inherent in the US-Europe relationship have generated much noise and had the greatest impact in shaping policy at the international level. They are also long-standing tensions that are unlikely to disappear in the near future.

**** Lee A. Bygrave is Associate Professor at the Department of Private Law, University of Oslo. Within the Department of Private Law, he is attached to the Norwegian Research Center for Computers and Law.***

1. Transatlantic Commonality

Despite the focus of this paper on regulatory differences, it is important to stress at the outset that Europe and the USA share a great deal in their respective attitudes to protecting privacy and closely related interests, such as personal autonomy and integrity. In other words, the divergence under study here occurs on top of a basic transatlantic view that such protection is important. This commonality is evident in the shared commitment of Americans and Europeans (particularly West Europeans) to upholding civil liberties and liberal democratic ideals of government. Both sides of the Atlantic are firmly under the grip of what Bennett and Raab (2006:4) term the "privacy paradigm" – a set of assumptions which idealises civil society as made up of "relatively autonomous individuals who need a modicum of privacy in order to be able to fulfil the various roles of the citizen in a liberal democratic state". This paradigm has structured the basic reactions of both Americans and West Europeans to the vastly expanded (and expanding) possibilities for processing personal data brought on by developments in information and communication technology (ICT). Since the onset of the computer age in the 1950s, the public debates that have raged in Europe over the privacy-related threats posed by modern ICT have generally followed the lines of the equivalent, though often earlier, debates in the USA (compare, e.g., Westin 1967, Miller 1971, Sieghart 1974, Messadié 1974). As Hondius (1975:6) writes, "[a]lmost every issue that arose in Europe was also an issue in the United States, but at an earlier time and on a more dramatic scale".

We see too considerable common ground in regulatory responses, with legislators on both sides of the Atlantic recognizing a need for statutory regulation of the processing of personal data. While the US legislation on point has been generally less stringent and comprehensive than its European counterparts (more on that further below), it still makes up a hefty corpus of code. Moreover, the USA was far from being a legislative laggard in the field. It was one of the first countries in the world to enact data privacy legislation, initially in the form of the federal Credit Reporting Act 1970 and shortly thereafter the federal Privacy Act 1974. At that stage, only two other pieces of such legislation were in place – Sweden's Data Act 1973 and the Data Protection Act 1970 passed by the German *Land* of Hessen. Further, the US legal system already recognised a right to privacy more generally, both at common law (in tort) and under the US Constitution; and it boasted an extensive amount of case law dealing with both types of right (Schwartz and Reidenberg 1996).

The central US and European statutes on data privacy expound a core set of broadly similar principles for protection of personal data. These principles were first drawn up in the early 1970s on both sides of the Atlantic by expert committees working contemporaneously yet independently of each other. The first body appointed by the British Parliament to investigate the putative privacy problems with the operation of computerised personal data records drafted a set of regulatory principles (Younger Committee 1972) that are remarkably similar to the code of "fair information practices" recommended a short time later by the US Department of Health, Education and Welfare (1973). It is impossible to determine how, if at all, the one committee influenced the other (see too Bennett 1992:99). Subsequent policy development by experts in the field involved considerably greater – and better documented – cross-jurisdictional exchange of viewpoints. This is particularly evident with the work of the Council of Europe (CoE) and the Organisation for Economic Cooperation and Development (OECD) on their chief data privacy codes. The CoE expert committee that drafted the 1981 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data liaised closely with the expert committee that was charged with drafting the OECD's 1980 Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (Seip 1995). In light of this liaison it is not surprising that the core principles of the two instruments, while not identical, mirror each other considerably (Bygrave 2008:27).

This convergence is all the more notable given that the CoE is customarily more concerned than the OECD with human rights protection. And work on the 1980 Guidelines was motivated largely by economic concerns (Kirby 1991). These concerns arose because the nascent national data privacy laws of Europe imposed restrictions on flow of personal data to any countries not offering levels of data protection similar to the "exporting" jurisdiction (see, e.g., Nugter 1989). In recommending greater harmonisation of these restrictions and of national data privacy regimes more generally, the OECD sought to minimise their deleterious impact on international commerce and freedom of expression (Kirby 1991:5-6). To be sure, the work of the CoE on its 1981 Convention was informed by a similar desire, though its formal emphasis was less on commercial needs than safeguarding the rights to freedom of information and expression "regardless of frontiers" (see the preamble to the Convention; see further Bygrave 2008:21). As elaborated further below, a similar desire also informed the subsequent work of European Union (EU) institutions in the data privacy field, with economic factors playing a particularly major role in the initiatives of the European Commission.

The OECD Guidelines show that early convergence on basic principles for data privacy occurred not only between the USA and Europe but also between a considerable number of other advanced industrial nations, including Australia, New Zealand, Japan and Canada. It would be misconceived, though, to see this convergence as simply the result of transnational agreement between expert policy entrepreneurs; other factors were at work too. Bennett (1992:ch.4) canvasses five hypotheses for explaining the convergence: (1) similarity of perceived technological threats, which forced policy makers to adopt similar solutions; (2) desire by policy makers to draw lessons from, and emulate, policies adopted earlier in other countries; (3) agreement amongst a small, cross-national network of experts as to appropriate data privacy policy; (4) harmonisation efforts of international organisations, such as the OECD; and (5) "penetration" (a process in which countries are forced to adopt certain policies because of the actions of other countries). After extensive analysis, Bennett (1992:150) finds that none of these hypotheses on its own adequately explains the policy convergence but that they have considerable explanatory utility in combination with each other.

2. Transatlantic Difference

While the OECD Guidelines represent a highpoint in transatlantic agreement on basic data privacy principles, their broadbrush, abstract formulation papered over tensions that likely prevented a drafting of the principles with greater detail, precision and bite. The chair of the expert group charged with formulating the Guidelines describes these tensions as follows (Kirby 1999:25):

"Within the Expert Group there were brilliant antagonists. The chief US delegate, Mr William Fishman, expressed with great clarity the American commitment to the free flow of data and of ideas. The head of the French delegation, Mr Louis Joinet, led those in the Expert Group who were alarmed by the dangers to individual privacy of completely unrestrained collections of personal data, vastly expanded in quantity and kind by the new technology. Each protagonist spoke with sincere conviction and gathered supporters. The contemporary state of technology meant that US business interests stood to gain from the growth of informatics and the spread of transborder data flows. The French and European business interests, on the other hand, coincided generally with restrictions insistent upon privacy protection. Not for the first time, philosophy and law followed trade."

These transatlantic tensions over data privacy simmered throughout the 1970s and 1980s but did not really boil over until the ensuing decade when the EU (or, more accurately, the European Community (EC)) took centre stage in the field. The EU and its older related bodies were not as quick as the CoE and OECD to develop data

privacy codes. However, the instruments eventually adopted within the EU/EC framework ended up being the most ambitious, comprehensive, and complex in the field. The key instrument is the 1995 Data Protection Directive (EU 1995). The Directive has had the greatest practical impact in shaping other data privacy initiatives within the EU. As elaborated further below, it has proven highly influential outside Europe as well, at the same time as being highly contentious, especially for American business interests. The contention derives mainly from the Directive's qualified prohibition on transfer of personal data to non-European countries that fail to provide "adequate" levels of data protection (Art. 25).

The Directive had a long and troublesome gestation. The Commission issued its first proposal for the Directive in 1990, although the European Parliament had made repeated calls for such an instrument well before then (see, e.g., Bygrave 2008:31). Throughout the 1980s, the Commission and Council of Ministers resisted these calls, directing their energies to fostering the internal market and a European computer industry (see, e.g., Ellger 1991:59-61). Only when faced with clear signs that the uneven nature of EU member states' respective rules on data privacy threatened realisation of the internal market did the Commission put serious effort into drafting a framework Directive (see further Newman 2008:90ff). The unevenness between national regimes at the time—with some EU member states (e.g., Italy, Spain and Greece) lacking even rudimentary data privacy laws—partly reflected the weakness of the 1981 CoE Convention and OECD Guidelines in prompting nation states to adopt comprehensive and relatively uniform data privacy regimes. This weakness was exacerbated by the Convention and Guidelines also permitting derogation on numerous significant points (see, e.g., Art. 3, 6 and 9 of the Convention). As of 1990, the Convention had failed to establish more than a minimal, formal equivalence between the national data privacy laws of the Federal Republic of Germany, France, the UK and the Netherlands (Nugter 1990:ch.8). This meant that the free flow of personal data between a considerable number of EU states could not be guaranteed.

From the initial Commission proposal for a framework Directive in the field, another five years of frequently frenetic negotiations went by before Data Protection Directive was adopted (further on these negotiations, see Platten 1996 and Simitis 1995). The final text is dense yet often nebulous, showing clear signs of the extensive tugs-of-war between various member states, organisations and interest groups during its drafting. The Directive is also somewhat ambivalent in its general policy thrust. On the one hand, it is aimed at promoting realisation of the European internal market, in which goods, persons, services, capital and, concomitantly, personal data are able to flow freely throughout Europe, and it goes so far as to proscribe privacy-based restrictions on the flow of personal data between EU member states (Art. 1(2)) – a prohibition not present in the CoE Convention or OECD Guidelines. This aspect of the Directive's rationale reflects the Commission's long-term preoccupation with fostering development of the internal market.

On the other hand, the Directive is also aimed at promoting data privacy in the face of technological and economic developments (Recitals 2, 3, 10, 11 in its Preamble). Indeed, it was the first EU/EC Directive to expressly accord protection of human rights a prominent place. It strives to bring about a "high" level of data protection across the EU (Recital 10), and seeks not just to "give substance to" but "amplify" the 1981 CoE Convention (Recital 11).

The human rights aspect of the Directive's rationale – and, indeed, of EU policy on data privacy generally – has become stronger and more salient in recent years. Indeed, the EU's constitutional framework, as amended by the Treaty of Lisbon, now recognises protection of personal data as a fundamental right in itself (see Charter of Fundamental Rights, Art. 8; TFEU, Art. 16) – that is, a right separate to the more traditional right to respect for private and family life as provided for by Article 7 of the Charter (see too ECHR Art. 8). These developments have

been stimulated by case law of the European Court of Human Rights pursuant to ECHR Article 8 (see, e.g., ECtHR 2000 and 2007) and reinforced by the European Court of Justice (see particularly ECJ 2003).

The Directive is broad in scope. With some qualifications (see Art. 3(2) and Art. 9), it applies to the processing of personal data in large swathes of both the private and public sectors. While it allows member states a "margin for manoeuvre" in transposing its requirements (Recital 9; see too Art. 5), it also specifies in relatively great detail a baseline of standards from which member states cannot depart. For example, it requires not just that member states establish independent authorities to monitor and enforce their data privacy laws, but stipulates additionally a large number of attributes that such authorities must have (Art. 28). These sorts of details are missing from both the CoE Convention (as originally adopted) and OECD Guidelines. To take another example, the Directive is the first and only international code in the field to tackle directly the vexed issue of which national law is applicable to a given case of data processing (see Art. 4). In doing so, it provides for the law of an EU state to apply outside the EU in certain circumstances – most notably where a data controller (i.e., the person or organisation who/which determines the purposes and means of processing personal data), based outside the EU, utilises "equipment" located in the state to process personal data for purposes other than merely transmitting the data through that state (Art. 4(1)(c)).

The latter provision gives the impression that the EU is, in effect, legislating for the world. It also nourishes accusations of "regulatory overreaching" (see, e.g., Bygrave 2000, Kuner 2007:ch. 3) and it has raised the ire of US businesses. Google, for instance, has protested that its operations are not governed by EU data privacy law even if it maintains servers in European countries (see, e.g., Article 29 Working Party 2008). However, most US ire has been directed at the Directive's restrictions on transborder data flow pursuant to Article 25. Before elaborating on that matter, though, it is important to elaborate basic differences in the US and EU approach to data privacy regulation.

These differences manifest themselves in myriad ways and some of them run deep. They are differences in views about the value of data privacy, the most appropriate means of safeguarding it, and, concomitantly, about who should foot the bill for its protection. As noted above, Europeans tend to view data privacy as a fundamental right deserving of rigorous, comprehensive legislative safeguards. Part of those safeguards is the establishment of independent regulatory authorities (typically termed "data protection authorities" or DPAs) with protection of data privacy as their specific and often sole remit. The Directive requires these authorities to operate in close cooperation with each other (Art. 28(6) and 29), thereby strengthening their practical impact. Furthermore, the status of data privacy as a fundamental right means that relatively comprehensive legislative limits are placed on the ability to contract around data privacy rules (Purtova 2010). Thus, a data subject (i.e., the person to whom the data relates) is largely prevented from disposing of their statutorily enumerated rights over use of the data, at their discretion or according to the dictates of the market. The statutory obligations placed on the data controller are also largely insulated from contract-based modification. While the Data Protection Directive provides room for data processing to occur based on the consent of the data subject (see Art. 7(a) and 8(2)(a); further on the role of consent in this context, see Bygrave and Schartum 2009), the consent mechanisms do not allow a data subject to enter into an agreement that permits a data controller from derogating fundamentally from their basic duties pursuant to, for example, Article 6 ("principles relating to data quality") and Article 12 (access rights).

The US regime, however, affords contract and market mechanisms relatively great latitude in setting data privacy standards. It permits a significant degree of contractual "override" of the privacy-related interests of data subjects. Concomitantly, US legislative safeguards for data privacy are generally less stringent than in Europe.

To be sure, a large number of data privacy statutes have been enacted in the USA, both at federal and state level. Yet these tend to be narrowly circumscribed, and the coverage they offer, particularly with respect to processing of personal data by private sector bodies, is haphazard and riddled with gaps (Solove and Schwartz 2011, Schwartz and Reidenberg 1996). This reflects a piecemeal legislative strategy. As Regan states (2008:51), "[g]enerally it takes an incident to focus attention on the issue of information privacy – and such incidents tend to focus on one type of record system at a time". Schwartz characterises this approach also in terms of "regulatory parsimony": "[i]n the absence of a need for the US legal system to act, the lawmaker will wait for strong evidence that demonstrates the need for a regulatory measure" (Schwartz 2013:7).

When legislative protection for data privacy interests does obtain, it is often not as far reaching as European rules. For example, US legislation refrains from imposing privacy-related restrictions on export of personal data to other countries. Monitoring and enforcement schemes for data privacy are also far less developed than in Europe. There is no federal regulatory authority with the mandate and powers of European DPAs. Generally, enforcement of data privacy rights is by way of court litigation.

Any proposed legislative measures in the field usually face strong opposition from affected business groups. The latter will typically have well-oiled lobbyist machinery at their disposal, along with a considerable number of "veto points" (Newman 2008:54) through which to exert pressure. Even if legislation gets enacted, it will often face challenge in the courts, the litigation typically centering on putative infringement of the First Amendment to the Bill of Rights in the US Constitution (Regan 2008:51). A recent case in point is *Sorrell v IMS Health, Inc.* in which the US Supreme Court (2011) overturned a Vermont statute restricting marketeers' use of pharmacy records, on the grounds that the law unduly violated free speech.

The latter case is one of many examples of the strong emphasis on freedom of expression by the US legal system. In line with this prioritisation, a basic point of departure under US law is that processing of personal data is permitted. The opposite pertains under EU law, which prohibits such processing unless it has a legal basis (see especially Art. 7 and 8 of the Data Protection Directive). Similarly, case law of the European Court of Human Rights holds that mere storage of personal data (albeit without consent or knowledge of the data subject) can constitute an interference with the right to respect for private life under ECHR Article 8(1), even if there is no evidence that the data was used to the practical detriment of the data subject or even at all (ECtHR 2000).

3. Explanations for Transatlantic Divergence

The aetiology of these transatlantic differences is complex. The relative laxity of US legislative safeguards, particularly regarding the private sector, reflects multiple factors. One set of factors are ideological. Americans tend to see privacy as important primarily in ensuring freedom from government intrusion (Eberle 2002, Whitman 2004). In Whitman's words, American concern for privacy centers upon "the right to freedom from intrusions by the state, especially in one's own home" (Whitman 2004:1161). This is part and parcel of Americans' general constitutional vision, which focuses on "the limits of government, reflecting the original American republican revolution, and securing a basis for the pursuit of liberty and happiness" (Eberle 2002:257). Americans tend also to view privacy as an interest that is mainly, if not exclusively, valuable for individual persons *qua* individuals, and therefore often in tension with the needs of wider society (see generally Regan 1995:chs.2 and 8).

In much of Europe, however, protection of privacy tends to be intimately tied to protection of dignity and honour (Eberle 2002, Whitman 2004). It is also often perceived as valuable not just for individual persons but society generally, particularly for maintaining civility, pluralism and democracy (Bygrave 2002:ch.7 and references cited therein).

Lindsay (2005:169) neatly sums up the contrasting ideologies as follows:

"On the one hand, the American approach takes autonomous individuals as given, and conceives the role of the law as one of setting limits on government in order to secure pre-existing individual autonomy. On the other hand, the European approach regards individual autonomy as being only fully realised in society, and conceives an important role for the law in creating the conditions for autonomous individuals as participating members of a community."

Lindsay further portrays the division between the US and European approaches in this area as reflecting a tension between "consequentialist", harms-focused ideology that is closely aligned with utilitarian thinking (the US approach), and a "deontological" ideology that is grounded in the thought of Kant and emphasises respect for persons as morally autonomous beings (the European approach) (see too, *inter alia*, Schwartz 1989).

Going beyond ideology, a strong case can be made out that the relative laxity of US data privacy rules is partly symptomatic of the paucity of first-hand domestic experience of totalitarian oppression in the USA (at least for the bulk of "white society"), particularly given the strength of consequentialist ideology there. On the other side, the traumas from first-hand experience of such oppression in large parts of Europe have imparted to European regulatory policy an anxiety and gravity that is considerably more subdued in US policy. Lindsay too emphasises the importance of first-hand experience of totalitarianism in explaining the European approach to data privacy:

"The European experience of mid-20th century totalitarianism resulted in a deep suspicion of any attempts by centralised authorities to increase their capacity for surveillance of individuals. Moreover, the activities of the secret police in the totalitarian regimes of Eastern Europe and the Soviet Union, which focused on monitoring individuals and collecting personal information in extensive (and often inaccurate) filing systems, provided a continuing example of the repressive use of information management techniques. European data protection law is part of the broader European project of building institutions and practices, including the EU itself, which are intended to ensure that the horrors of European totalitarianism are not revisited" (Lindsay 2005:157-158).

Newman, however, downplays the purchase of the "fascist legacy" argument in explaining the rise of comprehensive data privacy laws in Europe and the absence of such laws in the USA. He highlights a lack of empirical correlation between the fascist legacy of a nation state and the form of its subsequent data privacy regime. For example, he correctly points to the fact that Italy and Spain were slow to adopt comprehensive rules on point. Nonetheless, he recognizes that "the Nazi experience sensitized the advanced industrial societies on both sides of the Atlantic to the potential of government abuse" (Newman 2008:54). I would go further and claim that this sensitization was generally greater on the European than the US side.

4. Splintering Cleavage Lines

Care must be taken not to cast transatlantic divergence in this area along bright, clear-cut lines in which US legal protections for data privacy are uniformly weaker than those of Europe. Similarly, care must be taken not

to portray the lines of cleavage as running simply along the Europe-US divide, nor to treat Europe and the USA as homogeneous entities.

For instance, while the USA has federal legislation requiring providers of public electronic communications networks to preserve, in particular cases, electronic traffic data that they have already recorded (see Stored Communications Act, enacted as part of the Electronic Communications Privacy Act (US 1986) and codified at 18 USC section 2701-11; see especially section 2703(f)), it has not (yet) passed legislation that generally requires network providers to record and store traffic data for a particular period of time independent of a specific court order or warrant. The EU, however, has passed the latter type of legislation in the form of the Data Retention Directive (EU 2006) – a hugely controversial enactment from a privacy perspective. To take another example, data on personal income is publicly available as a matter of course in some Nordic countries (e.g., Norway). Such a disclosure practice is unthinkable in the USA and, indeed, in many other parts of Europe.

The latter fact underlines that data privacy regimes are far from uniform across Europe (European Commission 2012). Moreover, there has been considerable variation between European countries in their readiness to adopt comprehensive data privacy rules. Compare, for instance, the early and fairly fast adoption of such rules in Scandinavian countries with the much slower adoption process in Spain, Greece and Italy. Further, the adoption of such rules in Europe has often been close-run and contentious. As noted above, this was the case with the Data Protection Directive. It was also the case, for example, with the Federal Republic of Germany, which only just managed to pass comprehensive data privacy legislation in the late 1970s after a protracted, intensely debated process with massive industry opposition to the enactment (see further, e.g., Newman 2008:65-67).

The data privacy regimes of the various states making up the USA differ considerably too. Take, for instance, statutory rules requiring notification of security breaches involving personal information. In 2002, California was the first jurisdiction in the USA and, indeed, the world to enact such legislation (codified in Californian Civil Code sections 1798.82 and 1798.29). Most US states have since enacted similar rules, though their notification criteria vary. A handful of states (e.g., Alabama and New Mexico) have not enacted any such rules at all (National Conference of State Legislatures 2012). Under EU legislation, mandatory notification requirements – inspired by Californian law – have only been imposed on providers of public electronic communications networks (see EU 2002, Art. 4(3), added pursuant to EU 2009, Art. 2). A recent proposal for a general Regulation on data protection (European Commission 2012, elaborated below) provides for more general application of such requirements (see Art. 31-32 of the proposed Regulation).

5. Open Power Struggles

As indicated above, tensions between EU and US regulatory approaches in this area initially came to a head with the adoption of the Data Protection Directive. The restrictions placed by Article 25 of the Directive on flow of personal data to non-European states were especially problematic for the USA, which feared that these restrictions would be to the serious detriment of legitimate business interests. US federal government officials estimated that the restrictions threatened up to 120 billion dollars in trade – an amount far higher than had supposedly been at stake in previous trans-Atlantic trade conflicts (Heisenberg 2005:2, 84). At the same time, the Directive as a whole was viewed as a dirigistic form of regulation anathema to US preferences. The Clinton-Gore administration made this clear when formulating its general regulatory approach to Internet-based commerce in the late 1990s. In *A Framework for Global Electronic Commerce*, the administration stated that "governments should establish a predictable and simple legal environment based on a decentralized, contractual model of law rather than one based on top-down regulation" (US White House 1997). It further stated:

"To ensure that differing privacy policies around the world do not impede the flow of data on the Internet, the United States will engage its key trading partners in discussions to build support for industry-developed solutions to privacy problems and for market driven mechanisms to assure customer satisfaction about how private data is handled. The United States will continue policy discussions with the EU nations and the European Commission to increase understanding about the U.S. approach to privacy and to assure that the criteria they use for evaluating adequacy are sufficiently flexible to accommodate our approach."

These discussions were lengthy, tense and marked by brinkmanship. Each side claimed that the other was trying to impose unacceptable terms. Some of the US discussion even considered bringing the EU before the World Trade Organisation for alleged breach of the 1994 General Agreement on Trade in Services (Shaffer 2000:46-55). The clash of values was perhaps best summed up in a remark by Spiros Simitis, one of the pioneers of European data privacy policy, in an interview with the *New York Times* in May 1999: "This is not bananas we are talking about" (Andrews 1999).

In the end, the dispute ended up being patched over, at least temporarily, in the form of a "Safe Harbor" scheme brokered by the European Commission and US Department of Commerce (see European Commission 2000). The scheme allows for the flow of personal data from the EU to US organisations that voluntarily agree to abide by a set of data privacy principles based loosely on the Directive. The principles are considerably watered down in their compass and stringency relative to what the Directive ordinarily requires. As such, they signal that the scheme's brokers were ultimately concerned not so much with protection of privacy but protection of transborder data flow. Heisenberg (2005:160) writes:

"[B]oth the EU Commission and the US Department of Commerce wanted to give the appearance of protecting Europeans' privacy, but whether or not it was actually protected was relatively unimportant to both. The chief goal of the Safe Harbor Agreement was to keep data flowing between the two economic regions, and that purpose was achieved".

While the European Parliament and European DPAs were fairly critical of the scheme (see, e.g., European Parliament 2000), they lacked the power then to block it.

The Directive's impact on flow of personal data from Europe to the USA has been further softened by a set of derogations (laid down in Art. 26) from the adequacy test in Article 25. Most importantly, derogation is allowed if the proposed transfer is accompanied by "adequate safeguards" instigated by the controller for protecting the privacy and other fundamental rights of the data subject (Art. 26(2)). The Directive states that "such safeguards may […] result from appropriate contractual clauses". The Commission was fairly quick to issue relevant Model Contractual Clauses (MCCs) (European Commission decisions 2001, 2002 and 2004). Use of MCCs has since been augmented by the acceptance of Binding Corporate Rules (BCRs) as a mechanism for facilitating transborder data flow within a single company or group of affiliated companies. Whereas the Commission played a central role in negotiating the Safe Harbor scheme and drafting MCCs, data protection authorities have been pivotal in stimulating BCR usage by streamlining the BCR approval process (see, e.g., Article 29 Working Party 2007a).

Transatlantic tensions have nonetheless flared in the aftermath of the "9/11" terrorist attacks when US border control agencies demanded advance disclosure of air passenger name records (PNR data) of persons flying from Europe to the USA. Again, these tensions were ultimately quelled through a series of negotiations between the European Commission and US government. However, the negotiations were reportedly tough (Phillips and Bilefsky 2006, Meller 2007). They were also complicated by more active intervention from the European Parliament and data protection authorities. Indeed, the Parliament instigated judicial review of the first decision

of the Commission regarding transfer of PNR data to the USA, together with the Council decision approving that decision. The European Court of Justice held both decisions to be unlawful, not for privacy-related reasons, but because they applied to matters that then fell outside the scope of EU law (ECJ 2006). A new agreement with new legal legs was quickly adopted in October 2006 (Council 2006). That agreement expired in July 2007 and was replaced by yet another (Council 2007). The end-result was strongly criticized by European data protection authorities for weakening protection of PNR data (Article 29 Working Party 2007b), but it remains in place.

We have also seen an ongoing transatlantic power struggle between, on the one hand, European data protection authorities and their umbrella body (the Article 29 Working Party on data protection) and, on the other hand, US corporations, such as Facebook and Google. The struggle concerns the level and calibration of data privacy standards for Internet-based services. The outcome is still difficult to predict. Facebook and Google have conceded some ground, though slowly and reluctantly (see, e.g., Article 29 Working Party 2008).

Intergovernmental dispute risks flaring up again as the EU currently revises its legal framework on data privacy. In January 2012, the European Commission issued a proposal for a Data Protection Regulation to replace Directive 95/46 (European Commission 2012). The proposed Regulation is more detailed and stringent than the current Directive in many respects. For example, it aims at a much higher degree of harmonisation of national regulatory regimes. It strengthens the right of data subjects to demand deletion of data on them – often called, somewhat misleadingly, the "right to be forgotten" (see Art. 17 of the proposal; cf. Art. 12b of the current Directive). It introduces new rights, such as a right to data portability – i.e., a right of data subjects to transfer data about them from one information system to another (see Article 18 of the proposal). Moves are afoot in the European Parliament to ratchet up the stringency of the proposed legislation (European Parliament 2012), although the result of these efforts remains far from clear. It will take quite a while before the dust has settled around the legislative process. Burton, Kuner and Pateraki (2013:7) remark: "The reform is a marathon, not a sprint. The process will likely take at least two more years to complete, if not longer, and there will be further important steps along the way".

Particularly important for transatlantic relations is that while the proposed legislation seeks to introduce greater flexibility to the current regime for regulating flow of personal data from European countries to the USA and other "third countries" (see Chapter V), restrictions on such flow are still to be imposed using the adequacy test as point of departure (Art. 41). Not surprisingly, US government officials as well as US businesses are paying close attention to the progress of the proposed Regulation and making extensive efforts to blunt its bite – as happened during the drafting of the Data Protection Directive (Regan 1999). A US diplomat is recently cited as warning of a new trade war in the event that certain rights in the proposed Regulation, such as the right to be forgotten, are not watered down (Pinsent Masons 2013).

Yet efforts are also being made to dampen open conflict. At a conference arranged in Brussels shortly after the Commission issued its legislative proposal, Vivian Reding (European Commission Vice-President) and John Bryson (US Secretary of Commerce) issued a joint statement stressing collaboration and conciliation at the intergovernmental level:

"Both parties are committed to working together and with other international partners to create mutual recognition frameworks that protect privacy. Both parties consider that standards in the area of personal data protection should facilitate the free flow of information, goods and services across borders. Both parties recognize that while regulatory regimes may differ between the US and Europe, the common principles at the heart of both systems, now re-affirmed by the developments in the US, provide a basis for advancing their dialog to resolve shared privacy challenges. This mutual

interest shows there is added value for the enhanced EU-U.S.-dialogue launched with today's data protection conference. We hope to also work with international stakeholders towards a global consensus on how to tackle emerging privacy issues." (EU 2012)

The reference in the joint statement to current developments in the US as re-affirming common principles at the heart of both the US and EU systems partly reflects the Obama administration's White Paper of February 2012 setting out a Consumer Privacy Bill of Rights (US White House 2012). At the heart of the latter is a set of "fair information practice principles" (FIPPs) to govern private-sector handling of personal data in commercial contexts. The FIPPs go in some respects further than previous US elaborations of such principles. For example, they include a new principle entitled "respect for context": "[c]onsumers have a right to expect that companies will collect, use, and disclose personal data in ways that are consistent with the context in which consumers provide the data" (US White House 2012:15). According to the White Paper, the Obama administration will push for the FIPPs' legislative adoption along with their implementation in industry codes of practice, with the Federal Trade Commission playing a central enforcement role (US White House 2012:27-29, 35-37). It also urges increased "global interoperability" between the US consumer privacy framework and other countries' regimes, through "mutual recognition" schemes (US White House 2012:31-33).

While implementation of the White Paper FIPPs, particularly in legislation, would greatly decrease the distance between the EU and US data privacy regimes, it cannot be assumed that the Article 25 hurdle would then be cleared and the Safe Harbor scheme made redundant. The FIPPs are still not as comprehensive or stringently formulated as the rules in the Data Protection Directive and the proposed Regulation.

Calls are occasionally made for the drafting of a truly international convention on data privacy, within the framework of the UN. The Council of Europe is also pushing for more non-European states to accede to its 1981 Convention on point – a possibility allowed for under Article 23 of the Convention (Greenleaf 2012). The White Paper contains little if any suggestion of the USA intending seriously to pursue either initiative, despite its emphasis on achieving greater "global interoperability" in the field. Thus, scant chance remains – at least in the short term – of the EU and USA brokering and ratifying a multilateral treaty containing fairly detailed data privacy provisions with real bite (see too Bygrave 2008 and 2010).

6. Winners, Losers – and Co-Producers

Is it possible to identify a clear victor in the ongoing transatlantic struggle over data privacy? In one sense it is. If the criterion for victory is set in terms of which party to the struggle has been most successful in setting global standards in the field, Europe is the winner. As many commentators have noted, the overwhelming bulk of countries that have enacted data privacy laws have followed, to a considerable degree, the EU model as manifest in the Data Protection Directive. The most extensive and up-to-date analysis on point states: "something reasonably described as 'European standard' data protection laws are becoming the norm in most parts of the world with data privacy laws" (Greenleaf 2012:77, see too Newman 2008). The USA, in contrast, is an increasingly solitary outlier in the field. This marginalisation is all the more remarkable given the extensive international purchase of US regulatory preferences in other areas of information policy, such as telecommunications regulation, protection of intellectual property, and governance of the Internet naming and numbering system. As Newman (2008) ably shows, the predominance of European policy preferences in setting data privacy standards across large parts of the globe is fundamentally a reflection of the EU possessing greater regulatory

capacity in the field than the USA. By "regulatory capacity" is meant the formal resources (e.g., statutory authority) and informal resources (e.g., expertise) to draft, monitor and enforce market rules. Enhanced internal capacity in this sense tends to enhance the ability to shape international markets (Newman 2008:121). In this process, the considerable size of the EU market is a necessary but not sufficient condition for influencing other markets (Newman 2008:100). Of particular importance have been the network of European data protection authorities which have been able, collectively, to punch well beyond their individual weight. Their advocacy of data privacy interests has been crucial at particular junctures in the development of EU policy. The USA has lacked an equivalent set of authorities despite providing an early model for them (Newman 2008:53).

Talk of winners and losers should not blind us, though, to the considerable degree of transatlantic co-production of regulatory outcomes in the field. It is far from the case that the EU has been able to unilaterally impose its regulatory vision on the USA and other countries. Many facets of the transatlantic data privacy equation are the product of a cross-fertilisation of regulatory traditions (Schwartz 2013). The Safe Harbor scheme is an obvious case in point; the PNR agreements another. In some cases, US law has inspired EU legislative developments. Security breach notification rules are an example in this respect, while interest in BCRs has undoubtedly been nourished by the US Sarbanes-Oxley Act (US 2002) with its pronounced emphasis on corporate accountability.

Finally, focus on the EU-US relationship should not blind us to the actions of other countries. My hunch is that the transatlantic dialogue on data privacy is unlikely to persist as the internationally most important driver of standards in the field. Other major players are likely to muscle their way on to the data privacy stage. In this respect, the role of the Peoples' Republic of China will be intriguing to follow. China will increasingly have a voice on data privacy issues, though the import of its message remains to be deciphered, let alone clearly heard. If its message runs deeply counter to the Western "privacy paradigm", we might well find even greater coordination and convergence of EU and US regulatory policy in the field.

References

1. Select Bibliography

Andrews, Edmund L. (1999), "Europe and US Are Still at Odds Over Privacy", *The New York Times*, 27 May, http://www.nytimes.com/library/tech/99/05/biztech/articles/27europe-us-privacy.html.

Bennett, Colin J. (1992), *Regulating Privacy. Data Protection and Public Policy in Europe and the United States*, Ithaca, Cornell University Press.

Bennett, Colin J., and Raab, Charles D. (2006), *The Governance of Privacy. Policy Instruments in Global Perspective*, 2nd edn, Cambridge, MIT Press.

Bing, Jon (2009), "Building Cyberspace: A Brief History of Internet", in Lee A. Bygrave and Jon Bing, eds., *Internet Governance. Infrastructure and Institutions*, Oxford, Oxford University Press, p. 8-47.

Burton, Cédric, Kuner, Chris, and Pateraki, Anna (2013), "The Proposed EU Data Protection Regulation One Year Later: The Albrecht Report", *Bloomberg BNA Privacy and Security Law Report*, 21 January, p. 1-7, http://www.wsgr.com/PDFSearch/proposed-EU-0113.pdf.

Bygrave, Lee A. (1998), "Data Protection Pursuant to the Right to Privacy in Human Rights Treaties", *International Journal of Law and Information Technology*, Vol. 6, No. 3 (Autumn), p. 247-284.

Bygrave, Lee A. (2002), *Data Protection Law. Approaching Its Rationale, Logic and Limits*, The Hague, Kluwer Law International.

Bygrave, Lee A. (2008), "International Agreements to Protect Personal Data", in James B. Rule and Graham Greenleaf, eds., *Global Privacy Protection. The First Generation*, Cheltenham, E. Elgar, p. 25-84.

Bygrave, Lee A. (2010), "Privacy and Data Protection in an International Perspective", *Scandinavian Studies in Law*, Vol. 56 (October), p. 163-200.

Bygrave, Lee A., and Schartum, Dag Wiese (2009), "Consent, Proportionality and Collective Power", in Serge Gutwirth et al., eds., *Reinventing Data Protection?*, Heidelberg, Springer, p. 157-173.

Charlesworth, Andrew (2000), "Clash of the Data Titans? US and EU Data Privacy Regulation", *European Public Law*, Vol. 6, No. 2 (June), p. 253-274.

Eberle, Edward J. (2002), *Dignity and Liberty. Constitutional Visions in Germany and the United States*, Westport, Praeger.

Ellger, Reinhard (1991), "Datenschutzgesetz und europäischer Binnenmarkt (Teil 1)", *Recht der Datenverarbeitung,* Vol. 7, p. 57-65.

Flaherty, David H. (1989), *Protecting Privacy in Surveillance Societies. The Federal Republic of Germany, Sweden, France, Canada, and the United States*, Chapel Hill, University of North Carolina Press.

Greenleaf, Graham (2012), "The influence of European data privacy standards outside Europe: Implications for globalization of Convention 108", *International Data Privacy Law*, Vol. 2, No. 2 (May), p. 68-92.

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

Hondius, Frits W. (1975), *Emerging Data Protection in Europe*, Amsterdam, North Holland.

Kirby, Michael (1991), "Legal Aspects of Transborder Data Flows", *International Computer Law Adviser*, Vol. 5, No. 5 (February), p. 4-10.

Kirby, Michael (1999), "Privacy Protection, a New Beginning: OECD Principles 20 Years On", *Privacy Law & Policy Reporter*, Vol. 6, No. 3 (September), p. 25-29, 44, http://www.austlii.edu.au/au/journals/PLPR/1999/41.html.

Kuner, Christopher (2007), *European Data Protection Law. Corporate Compliance and Regulation*, 2nd edn, Oxford, Oxford University Press.

Lindsay, David (2005), "An Exploration of the Conceptual Basis of Privacy and the Implications for the Future of Australian Privacy Law", *Melbourne University Law Review*, Vol. 29, No. 1 (April), p. 131-178.

Meller, Paul (2007), "EU, US sign passenger data sharing deal", *IDG News Service*, 2 July, http://www.networkworld.com/news/2007/070207-eu-us-sign-passenger-data.html.

Messadié, Gérald (1974), *La fin de la vie privée*, Paris, Calmann-Lévy.

Miller, Arthur R. (1971), *The Assault on Privacy. Computers, Data Banks, and Dossiers*, Ann Arbor, University of Michigan Press.

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

Nugter, Adriana C.M. (1989), *Transborder Flow of Personal Data within the EC. A Comparative Analysis of the Privacy Statutes of the Federal Republic of Germany, France, the United Kingdom, and The Netherlands and their Impact on the Private Sector*, Deventer and Boston, Kluwer Law & Taxation.

Phillips, Don, and Bilefsky, Dan (2006), "EU and U.S. shape a deal on passenger data", *International Herald Tribune*, 28 September, http://www.nytimes.com/2006/09/28/world/europe/28iht-euair.2966489.html.

Pinsent Masons (2013), "US diplomat warns of 'trade war' if 'right to be forgotten' proposals are followed through", *Out-Law*, 4 February; http://www.out-law.com/en/articles/february/us-diplomat-warns-of-trade-war-if-right-to-be-forgotten-proposals-are-followed-through.

Platten, Nick (1996), "Background to and History of the Directive", in David Bainbridge, ed., *EC Data Protection Directive*, London, Butterworths, p. 13-32.

Purtova, Nadezhda (2010), "Private Law Solutions in European Data Protection: Relationship to Privacy, and Waiver of Data Protection Rights", *Netherlands Quarterly of Human Rights*, Vol. 28, No. 2 (June), p. 179-198, http://ssrn.com/abstract=1555875.

Regan, Priscilla M. (1995), *Legislating Privacy. Technology, Social Values, and Public Policy*, Chapel Hill, University of North Carolina Press.

Regan, Priscilla M. (1999), "American Business and the European Data Protection Directive: Lobbying Strategies and Tactics", in Colin J. Bennett and Rebecca Grant, eds., *Visions of Privacy. Policy Choices for the Digital Age*, Toronto, University of Toronto Press, p. 199-216.

Regan, Priscilla M. (2008), "The United States", in James B. Rule and Graham Greenleaf, eds., *Global Privacy Protection. The First Generation*, Cheltenham, E. Elgar, p. 50-80.

Schwartz, Paul M. (1989), "The Computer in German and American Constitutional Law: Towards an American Right of Informational Self-Determination", *The American Journal of Comparative Law*, Vol. 37, No. 4 (Autumn), p. 675-701.

Schwartz, Paul M. (2013), "The E.U.-U.S. Privacy Collision: A Turn to Institutions and Procedures", *Harvard Law Review*, Vol. 126 (forthcoming), http://www.harvardlawreview.org/symposium/papers2012/schwartz.pdf.

Schwartz, Paul M., and Reidenberg, Joel R. (1996), *Data Privacy Law. A Study of United States Data Protection*, Charlottesville, Michie Law.

Seip, Helge (1995), "Data Protection, Privacy and National Borders", in Jon Bing and Olav Torvund, eds., *25 Years Anniversary Anthology in Computers and Law*, Oslo, TANO, p. 67-82.

Shaffer, Gregory (2000), "Globalization and Social Protection: The Impact of E.U. and International Rules in Ratcheting Up of U.S. Privacy Standards", *Yale Journal of International Law*, Vol. 25, No. 1 (Winter), p. 1-88, http://works.bepress.com/gregory_shaffer/3.

Sieghart, Paul (1974), *Privacy and Computers*, London, Latimer.

Simitis, Spiros (1995), "From the Market To the Polis: The EU Directive on the Protection of Personal Data", *Iowa Law Review*, Vol. 80, No. 3 (March), p. 445-469.

Solove, Daniel J., and Schwartz, Paul M. (2011), *Information Privacy Law*, 4th edn, New York, Wolters Kluwer Law & Business.

Warren, Samuel, and Brandeis, Louis (1890), "The Right to Privacy", *Harvard Law Review*, Vol. 4, No. 5 (15 December), p. 193-220.

Westin, Alan F. (1967), *Privacy and Freedom*, New York, Atheneum.

Whitman, James Q. (2004), "The Two Western Cultures of Privacy: Dignity versus Liberty", *Yale Law Journal*, Vol. 113, No. 6 (April), p. 1151-1221, http://www.yalelawjournal.org/images/pdfs/246.pdf.

2. Documents and Judicial Decisions

Article 29 Working Party (2007a), *Recommendation 1/2007 on the Standard Application for Approval of Binding Corporate Rules for the Transfer of Personal Data* (WP133), 10 January, http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2007_en.htm.

Article 29 Working Party (2007b), *Joint opinion on the proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes, presented by the Commission on 6 November 2007* (WP145), 5 December, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp145_en.pdf.

Article 29 Working Party (2008), *Google: The Beginnings of a Dialog*, 16 September, http://ec.europa.eu/justice/policies/privacy/news/docs/pr_16_09_08_en.pdf

Council of the European Union (2006), Decision 2006/729/CFSP/JHA on the signing, on behalf of the European Union, of an Agreement between the European Union and the United States of America on the processing and transfer of passenger name record (PNR) data by air carriers to the United States Department of Homeland Security, 16 October, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006D0729:EN:NOT.

Council of the European Union (2007), *Decision 2007/551/CFSP/JHA on the signing, on behalf of the European Union, of an Agreement between the European Union and the United States of America on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the United States Department of Homeland Security (DHS) (2007 PNR Agreement)*, 23 July, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32007D0551:EN:NOT.

ECJ (2003), *Österreichischer Rundfunk and Others*, joined cases C-465/00, C-138/01, and C-139/01, ECR I-4989, 20 May, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62000CJ0465:EN:NOT.

ECJ (2006), *European Parliament v. Council of the European Union*, joined cases C-317/04 and C-318/04, 30 May, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:C2006/178/02:EN:NOT.

ECtHR (2000), Judgement on case of *Amann v. Switzerland*, Application No. 27798/95, 16 February, http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-58497.

ECtHR (2007), Judgement on case of *Copland v. United Kingdom*, Application No. 62617/00, 3 April, http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-79996.

EU (1995), *Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data* (Data Protection Directive), 24 October, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:NOT.

EU (2002), *Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)*, 12 July, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:NOT.

EU (2006), *Directive 2006/24/EC on the retention of data generated or processed in connection with the provision*

of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (Data Retention Directive), 15 March, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0024:EN:NOT.

EU (2009), *Directive 2009/136/EC amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws …*, 25 November, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32009L0136:EN:NOT.

EU (2012), *EU-U.S. joint statement on data protection by European Commission Vice-President Viviane Reding and U.S. Secretary of Commerce John Bryson*, Brussels, 19 March, http://europa.eu/rapid/press-release_MEMO-12-192_en.htm.

European Commission (2000), *Decision 2000/520/EC pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce …*, 26 July, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000D0520:EN:NOT.

European Commission (2001), *Decision 2001/497/EC on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC …*, 15 June, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32001D0497:EN:NOT.

European Commission (2002), *Decision 2002/16/EC on standard contractual clauses for the transfer of personal data to processors established in third countries*, under Directive 95/46/EC …, 27 December [2001], http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002D0016:EN:NOT.

European Commission (2004), *Decision 2004/915/EC amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries …*, 27 December, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004D0915:EN:NOT.

European Commission (2012), *Proposal for a Regulation on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)* (COM(2012) 11 final), Brussels, 25 January, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52012PC0011:EN:NOT.

European Parliament (2000), *Resolution on the Draft Commission Decision on the adequacy of the protection provided by the Safe Harbour Privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce (C5-0280/2000 - 2000/2144(COS)) (A5-0177/2000)*, Strasbourg, 5 July, http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P5-TA-2000-0306+0+DOC+XML+V0//EN.

European Parliament (2012), *Draft report on the proposal for a Regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data* (General Data Protection Regulation) (COM(2012)0011 - C7-0025/2012 - 2012/0011(COD)), Brussels, 20 December, http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/pr/922/922387/922387en.pdf.

European Parliament (2013), *Draft report on the proposal for a Regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data* (General Data Protection Regulation) (COM(2012)0011 - C7-0025/2012 - 2012/0011(COD)), Brussels, 16 January, http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/pr/924/924343/924343en.pdf.

National Conference of State Legislatures (2012), *State Security Breach Notification Laws*, 20 August, http://www.ncsl.org/issues-research/telecom/security-breach-notification-laws.aspx.

OECD (1980), *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, 23 September, http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

US (1986), *Electronic Communications Privacy Act,* Public Law 99-508, 21 October, http://www.justice.gov/jmd/ls/legislative_histories/pl99-508/act-pl99-508.pdf.

US (2002), *Public Company Accounting Reform and Investor Protection Act* (Sarbanes-Oxley Act), Public Law 107-204, 30 July, http://www.gpo.gov/fdsys/pkg/PLAW-107publ204/html/PLAW-107publ204.htm.

US (2011), *United States Code, Title 18: Crimes and Criminal Procedure*, Section 2701-2711, http://www.law.cornell.edu/uscode/text/18/part-I/chapter-121.

US Department of Health, Education and Welfare (1973), *Records, Computers and the Rights of Citizens*, Report of the Secretary's Advisory Committee on Automated Personal Data Systems, Washington, Government Printing Office, available at http://epic.org/privacy/hew1973report.

US Supreme Court (2011), Judgement on case of *Sorrell v IMS Health, Inc.*, case No. 10-779, 23 June, http://www.supremecourt.gov/opinions/10pdf/10-779.pdf.

US White House (1997), *A Framework for Global Electronic Commerce*, Washington, Government Printing Office, available at http://clinton4.nara.gov/WH/New/Commerce.

US White House (2012), *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*, Washington, The White House, February, http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

Younger Committee (1972), *Report of the Committee on Privacy*, Cmnd 5012, London, HMSO.

3. Treaties

1981, *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, Strasbourg, 28 January, http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm.

2007, *Charter of Fundamental Rights of the European Union*, Strasbourg, 12 December, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:12012P/TXT:EN:NOT.

2012, *Treaty on the Functioning of the European Union* (TFEU), 26 October, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:12012E/TXT:EN:NOT.

The Project

In an era of global flux, emerging powers and growing interconnectedness, transatlantic relations appear to have lost their bearings. As the international system fragments into different constellations of state and non-state powers across different policy domains, the US and the EU can no longer claim exclusive leadership in global governance. Traditional paradigms to understand the transatlantic relationship are thus wanting. A new approach is needed to pinpoint the direction transatlantic relations are taking. TRANSWORLD provides such an approach by a) ascertaining, differentiating among four policy domains (economic, security, environment, and human rights/democracy), whether transatlantic relations are drifting apart, adapting along an ad hoc cooperation-based pattern, or evolving into a different but resilient special partnership; b) assessing the role of a re-defined transatlantic relationship in the global governance architecture; c) providing tested policy recommendations on how the US and the EU could best cooperate to enhance the viability, effectiveness, and accountability of governance structures.

Consortium

Mainly funded under the European Commission's 7th Framework Programme, TRANSWORLD is carried out by a consortium of 13 academic and research centres from the EU, the US and Turkey:
Istituto Affari Internazionali, *Coordinator*
German Marshall Fund of the United States
University of Edinburgh
Free University of Berlin
Fondation Nationales des Sciences Politiques
Sabanci University of Istanbul
Chatham House
European University Institute
University of Siena
Charles University of Prague
University of Mannheim
TNS Opinion
American University of Washington

Advisory Board

WWW.TRANSWORLD-FP7.EU