Jerusalem Papers in Regulation & Governance

Working Paper No. 26
September 2010

THE REGULATION OF PRIVACY

Andreas Busch

Chair of Comparative Politics and Political Economy
Department of Political Science
University of Göttingen
Platz der Göttinger Sieben 3
37073 Göttingen, Germany

Tel. +49-551-3910611

Email: andreas.busch@sowi.uni-goettingen.de

הפורום הירושלמי
לרגולציה וממשליות

Jerusalem Forum
on Regulation & Governance

האוניברסיטה העברית
הר הצופים
ירושלים, 91905

The Hebrew University
Mount Scopus
Jerusalem, 91905, Israel

regulation@mscc.huji.ac.il :Email
http://regulation.huji.ac.il

ISSN: 2079-5882

Working Paper No. 26 | September 2010

The Regulation of Privacy

Andreas Busch

Abstract: Privacy as a basic human need has always existed and is crucial for the development of the individual as well as society. But technological developments such as the spread of computers and more recently the internet pose a threat to its protection. Attempts at regulating the collection, storage, transmission and use of person-related data to protect privacy in the face of such challenges have taken many forms which can analytically be distinguished; but the simultaneous existence of international, supranational and national level attempts have led to the emergence of a complex situation in reality. Internationally, voluntary "codes of practice" coexist with binding rules of differing legal quality; nationally, comprehensive legislation spanning the private and public sectors, with implementation overseen by an agency, can be distinguished from piecemeal legislation without specific overview. Such differences, together with competing economic and security interests as well as variations in the ultimate justification of the protection of privacy, have led to international conflicts around the transmission of person-related data for commercial and security purposes. Given the increasing economic importance of such data, as well as rising sensitivity towards the protection of privacy in many populations, regulatory competition in this field is likely to increase in the future, while the direction of that dynamic is difficult to predict.

Key words: Privacy, regulation, data protection, European Union, United States, diffusion, institutions, regulatory agencies, international disputes, safe harbor, SWIFT, anti-terrorism, international standards

Acknowledgements: Research for this chapter was supported by ESRC grant RES-062-23-0536 and by a fellowship at the Hanse Institute for Advanced Study in 2009. Both are gratefully acknowledged.

Working Paper No. 26 | September 2010

The Regulation of Privacy

Introduction

The debate about the regulation of privacy has in recent years above all been linked to technological developments and their uses. From the 1960s onwards, the emergence and spread of computers, data banks, telecommunication, and eventually the internet have led to several waves of concerned public debate about the impact they have on privacy, society, and the state (see as representative publications Packard 1964; Miller 1971; Burnham 1983; Sykes 1999; O'Harrow 2006). In this perspective, individual privacy is threatened by person-related information which can be stored electronically and easily transmitted. Such information has increased massively in recent years; the capacity for cheap storage has grown even more quickly, and since such information can be digitally processed and cross-linked, new data can be generated from very diverse sources of information, giving them a new quality and allowing very detailed portraits of individual people, their preferences and their characteristics to be created. Regulatory challenges in this field thus include the questions of who is allowed to collect and store such data; by whom and for what purposes they can be retrieved; and what legitimate uses they can be put to. In several countries, disputes about the power of internet search giant Google (whose corporate aim it is to "to organize the world's information and make it universally accessible and useful" and whose activities range from scanning books to filming streets) have recently indicated the growing fears of citizens and their representatives about losing control over valued person-related information, moving the issue of regulation in this field up on the political agenda.

Looking at privacy from that angle one could be led to believe that it is a new and modern concept. Indeed it was long assumed that primitive societies neither knew nor demanded privacy. In the late 1940s, anthropologist Margaret Mead, in her famous study on "Coming of age in Samoa" argued that in a society which lived in houses without walls, where there were no separate sleeping quarters, and little clothing was

worn, "there is no privacy and no sense of shame".[1] But further research has shown this view to be factually not correct. Even primitive societies had "distance" and "avoidance" rules to provide for some degree of individual privacy. Privacy norms were thus not absent; they were just harder to realise under the living, working and economic conditions of primitive societies (cf. the summary of research in Westin 1967, p.13-18). While privacy is a basic human need and constitutive for the individual, without a society, there would be no intrusion and hence no need for privacy as protection against intrusion. Since societies differ, however, the desire or need for privacy varies historically (Moore 1984, ch. 1), and demand for privacy has grown substantially in the process of modernisation. Nuclear families living in individual households; urbanisation and the anonymity of city life; mobility in work and residence; the weakening of religious authority — all these factors contributed to this development since they increased chances for privacy. At the same time, however, countervailing forces developed as well: greater population density and new technical instruments made possible new ways to encroach upon privacy or engage in surveillance.

Despite the intense debates about privacy in recent decades, a generally accepted definition has so far failed to emerge. "Few values so fundamental to society as privacy have been left so undefined in social theory or have been the subject of such vague and confused writing by social scientists", Westin (1967, p. 7) remarked in his seminal study on the subject many years ago. And more than four decades later, a recent major study still starts by admitting that privacy "is a concept in disarray. Nobody can articulate what it means." (Solove 2008, p. 1). The main reason for this situation is that privacy is negatively defined as an absence of intrusion and that such intrusion can both come from many directions and vary in their subjectively perceived intensity. Characterisations of privacy are manifold (cf. the discussions in Allen 2005; Waldo et al. 2007; Solove 2008) and range from an encompassing "right to be let alone" (on which see originally Warren and Brandeis 1890) to control over one's own body, including the intimate and personal aspects of conducting one's life and sexuality; from control over personal information and protection of one's reputation to protection from interrogation and searches by public authority. This non-exhaustive list combines personal, social, and political aspects, indicating the breadth of the debate.

Almost as varied have been the academic disciplines that have debated privacy over the last decades. Legal scholars have discussed the amount to which the protection of privacy is granted by constitutional protection, how it relates to the right to free speech, or how the law of torts relates to the issue (Prosser 1960). Feminist scholars have argued that existing legal provisions protecting family matters from state interference in the name of privacy can seriously disadvantage women seeking protection from abuse (Schneider 1991; see also Gavison 1992). In political philosophy, liberal thinking has been predominant, regarding privacy as a property of the individual, important for his or her self-interest mainly for self-development and/or the establishment of intimate or human relationships (Rossler 2005). But this has been criticised by authors from a communitarian perspective who argue that privacy should not be an "unbounded or privileged good" (Etzioni 1999, p. 195) because an exclusive focus on individual rights can harm the needs and values of society.

This paper looks at the regulation of privacy through a perspective of "data protection" (Bennett 1992) because use of modern technology is the main threat to privacy understood as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others." (Westin 1967, p. 7). It surveys attempts to protect privacy through regulation both on the international and national level, and analyses actors and the tools they use. In recent years, conflicts about the regulation of privacy have emerged also on the international level because of different approaches, priorities and values, and a number of them are described and analysed in the next part. A concluding part looks at the challenges for the regulation of privacy in the 21st century.

International sources of regulating privacy

Since digital data move with ease across national borders and around the globe, the international level would seem to be the right place for the regulation of privacy. Indeed several international bodies have made attempts at drawing up guidelines and

agreeing on common frameworks in recent decades.[2] Political agency has varied in this field over time; but generally one can say that the proliferation of rules protecting privacy owes a lot to the initiatives of the network of national data protection commissioners from the 1970s onwards who overcame initial resistance from national governments and industry interests (Newman 2008). Economic interests in lowering transaction costs of trade through harmonisation of national rules then supported the creation of international level rules, while civil rights action groups supported the defense of privacy protection standards against law enforcement interests in weakening them, especially in anti-terrorism after 9/11.

The Council of Europe (CoE) was the first international organisation to guarantee the "the right to respect for his private and family life, his home and his correspondence" to everyone in Article 8 of its 1950 European Convention on Human Rights (ECHR). Out of this right to privacy and discussions in the CoE's Parliamentary Assembly in 1968 about how it was to be protected in the face of emerging modern technology grew two resolutions of the CoE's Committee of Ministers in 1973 and 1974 establishing principles of data protection for computerised "data banks" in the public and private sectors. While these resolutions were not legally binding for the member states, many of them started to enact national data protection laws and / or incorporated data protection as a fundamental right into their constitutions.[3] The international "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data" was adopted by the CoE in 1980 and opened for signature on 28 January 1981 (Council of Europe 1981). It entered into force on 1 October 1985.[4]

The Convention contains basic principles for data protection which every participating country should consider in its domestic legislation. This common core contains basic information privacy principles, namely that personal data should be obtained and processed fairly and lawfully; be stored only for specified and legitimate purposes; not be excessive in relation to those purposes; be accurate and kept up to date; and permit identification of the data subjects for no longer than is required (Article 5). In addition, data security and protection against unauthorized access is called for, and individuals are vested with rights regarding data files which contain their data. Furthermore, the Convention contains regulations regarding transborder

data flows (establishing the principle of free flow of data between contracting parties) and rules for mutual assistance between the contracting parties.

As the CoE has no supranational legal structure, it has no mechanism for enforcing compliance with the rules set out in the Convention; other weaknesses of the 1981 Convention include that many of the terms used are left undefined (which has not helped in the harmonisation of national data protection legislation), and that it does not include provisions for the transfer of data to non-contracting parties.[5] Nevertheless the 1981 Convention is "a key reference point" (Bygrave 2008, p. 26) on the international level, influential in shaping the debate about data protection in Europe and beyond — and not least in the newly democratising countries of Central and East Europe after 1990, almost all of which signed and ratified the Convention.

The Organisation for Economic Cooperation and Development (OECD) had been invited to cooperate in the drafting of the CoE convention, and representatives of the organisation and its four non-European member countries (Australia, Canada, Japan and the United States) participated in the work of the CoE's drafting committee. The OECD, as an organisation of economically advanced liberal democracies which included important data processing countries among its members, had already taken an early interest in the issue (cf. Niblett 1971). In 1978, it set up its own group of experts to draw up guidelines which would help to harmonize the different national data protection legislations. Since this forum included the United States as the country with the dominant data processing industry, negotiations were difficult (Bennett 1992, p. 136f.). But it was possible for the group to agree on certain principles, finishing a draft in 1979 that was adopted in September 1980. The "Guidelines governing the protection of privacy and transborder flows of personal data" (Organisation for Economic Co-operation and Development 1981) contain eight specific "basic principles", namely collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual rights, and accountability (ibid., Part Two). There are evident parallels to the CoE Convention, and similarly the wording is somewhat vague, leaving room for interpretation (which was probably necessary to reach agreement). As the guidelines are explicitly labelled as "minimum standards" and since they are voluntary and not legally binding, their enforceability is even weaker than that of the CoE Convention. Not all member states even adopted

legislation or created data protection authorities, opting instead for the expressed preference for self-regulation (Article 19 b). But despite these shortccomings, the OECD guidelines have been influential, especially for the data protection legislation outside Europe, in countries like Japan, Australia, New Zealand, Canada and Hong Kong (Bygrave 2008: 28).

As the issue of transborder data flows became more important, the OECD in 1985 adopted a "Declaration on Transborder Data Flows" which pledged support for international exchange of data and information and opposed "unjustified barriers" to it; and in 1998, a "Declaration on the Protection of Privacy on Global Networks" followed, acknowledgeding the different approaches taken by member countries in their data protection policies while confirming the importance of effective privacy protection for the future development of e-commerce. The OECD even set up an online "Privacy Statement Generator" which allowed easy complilation of a specific privacy statement for websites.[6]

While the focus of the OECD was clearly on privacy with a view to commercial and economic issues, the United Nations' "Guidelines Concerning Computerized Personal Data Files" were primarily motivated by human rights considerations. Following from the Universal Declaration of Human Rights (1948) which contained privacy protection provisions in its Article 12, the Guidelines adopted by the General Assembly on 14 December 1990 contained principles that formulate "minimum guarantees that should be adopted in national legislations". Again similarities exist with the CoE Convention and the OECD Guidelines, but two innovations are the "principle of accuracy" which calls for data holders "to conduct regular checks on the accuracy and relevance of the data recorded"; and the application of the guidelines to personal data files kept by governmental international institutions. The most important fact, however, is that with the UN taking up a stance on privacy the topic had clearly started to move beyond the developed "Western world".

During the 1990s, the increasing use of the internet brought the issues of electronic commerce and the privacy implications of transborder data flows on the agenda. In 1995, the European Union passed its "Directive on the Protection of Personal Data with Regard to the Processing of Personal Data and on the Free Movement of Such Data" (95/46/EC) which harmonised data protection regulations across the then 15

member states (European Union 1995).[7] This directive had been discussed over a couple of years and was a consequence of the completion of the Union's single internal market in goods and services in 1992. Since the European Union is a supranational body, its directive was legally binding and enforceable, which set it apart from the international rules discussed so far. It also had substantial reverberations beyond Europe: Since Article 25 of the directive included restrictions on the transfer of personal data to third countries which did not have an "adequate level of protection", areas outside Europe with significant data processing industries feared that they might be cut off from European business. Most prominently the Asia-Pacific Economic Coooperation (APEC), an intergovernmental organisation of 21 Pacific Rim countries including Australia, Canada, Japan, South Korea, Taiwan, and the United States, started to work on a "Privacy Framework" in 1998 which was adopted in late 2004 (Asia-Pacific Economic Cooperation 2004). The APEC Framework, too, builds on privacy principles; however, compared to the CoE and EU approaches, several elements are missing (such as the purpose specification and the openness principle), and no rules about data exports to countries with lower data protection standards are set. The APEC Framework thus seems less motivated by human rights protection than by economic interests and sets a comparatively "low standard" of data protection (Greenleaf 2005). In Africa, legal regimes for data privacy are least developed: the "African Charter on Human and People's Rights" (1981) omits mentioning a right to privacy in its catalog of basic human rights, and none of the African countries has enacted comprehensive data privacy laws, although South Africa has started to make steps towards one (Waldo et al. 2007, p. 394).

National tools of regulating privacy

Despite the efforts at harmonisation on the international level, different national approaches to the regulation of privacy still dominate in the early 21st century. Moreover, these national regimes do not necessarily follow a rational blueprint — indeed, they sometimes rather resemble a patchwork quilt, having evolved over the decades and adapted step-by-step to technological progress rather than making a clean regulatory break by imposing a new and consistent approach. This section gives an

overview of the principal tools available for the regulation of data privacy on the national level, and characterises the basic approaches that can be distinguished.

Regulation theory distinguishes between performance- or principles-based and rules-based regulation (see May in this volume; also Australian Law Reform Commission 2008, vol 1, p. 234ff.). Both approaches have advantages and disadvantages: Performance-based regulation sets an overall objective rather than detailing steps that must be complied with. It can thus be described as focused on outcomes, with the advantages of flexibility but at the cost of potential ambiguity and imprecision.[8] Rules-based regulation, in contrast, provides for clarity about the actions regulatees have to perform, creating certainty of expectations for all sides concerned. On the other hand, such an approach may invite "box ticking", and appear rigid in the face of shifting circumstances, thus disconnecting the situation from the desired outcomes.

In privacy regulation, both performance-based and rules-based regulation can be found. Bennett and Raab (2006) find the three main classes of policy tools in this area to be legal instruments and regulatory agencies, self-regulatory instruments, and technological instruments. Relating them to the theoretical distinction introduced above, we find that both the first and the second bridge rules- and performance-based regulation (since legislation as well as self-regulation can follow either strategy), and the third is highly privacy-specific and cannot be mapped onto the distinction.

Legal instruments regulating privacy vary in two dimensions, namely their focus on either performance or rules, and the degree to which they are comprehensive or issue-specific. In the form of "fair information practices" (FIP), performance-based regulation emerged first in the United States in the early 1970s. The "Advisory Committee on Automated Personal Data Systems" established by the US Department of Health, Education and Welfare (HEW) contained the first such code, and defined the core of a policy solution to personal data protection in terms of fairness and hence justice (Regan 2008, p. 55f.). This approach has proven influential in subsequent years in shaping the information practices of numerous private and governmental institutions, and it became the dominant US approach to information-privacy protection for the next decades (Westin 2003, p. 436). Privacy principles can be defined as an attempt to balance competing business and consumer interests in the

private sector (and bureaucracy and citizen interests in the public sector) based on general considerations of justice. To implement such principles and put them into practice, however, requires further steps, namely either legislation or agency regulation, or self-regulation. While some legislation in this field exists in all countries, it varies considerably in character: there are privacy laws that cover both the private and public sectors (dominant for example in European countries); and there are cases where a multitude of privacy laws exists that regulates only very specific areas (for example the United States Video Privacy Protection Act of 1988 which only provides rules for the use of video rental information). For the implementation of such legislation, governments normally set up or designate an agency responsible for its implementation — usually called the "Privacy Commissioner", "Data Commissioner" or "Data Protection Commissioner".[9] The degree of resources devoted to such an agency, its independence from the national executive, and the degree to which they are active participants in the national regulatory debates, however, vary considerably between countries (Bennett 1992; Bennett and Raab 2006; Newman 2008).

Self-regulation is a mode of regulation that works without direct government involvement, but may exist "in the shadow of public power" (Newman and Bach 2004). Industry is usually the initiator of self-regulation, and the likelyhood of using this instrument is linked to the structure of sectoral interest representation: If strong associations exist that have the dominant firms on board, the adoption, implementation and enforcement of rules will be easier than if several associations compete for industry representation and/or dominant firms remain absent. Authored by industry, self-regulation will normally consist of codes of practice of different varieties; but in contrast to the privacy principles discussed above, they will be much more specific in the level of detail they employ (Bennett and Raab 2006: ch. 6). Doubts exist, however, about the effectiveness of self-regulation in the field or privacy protection, both with respect to the underlying theory and the practical experience (Papakonstantinou 2002, p. 143).

Regulation through technology is a third principal regulatory instrument that is highly specific as it builds privacy rules into the machinery and protocols of the communication flows dealing with personal data. Such "privacy-enhancing

technologies" (PETs)[10] include public key encryption, anonymisation servers, software that blocks "cookies" for browsers, or the use of privacy preferences such as P3P to ensure users' informed consent with a website's privacy policy. In spite of the obvious benefits, PETs have not (yet?) been widely implemented, and further research into them has been called for (Royal Academy of Engineering 2007, p. 40-43).

The instruments described in this section constitute a toolbox from which governments can choose in their attempt to regulate the field of person-related data privacy. In spite of the commonality of the challenge, however, countries' regulatory approaches continue to differ. No "best practice" has emerged so far, and while the piece-by-piece emergence of regulation over time may have contributed to this situation, it also points to differences in the fundamental approaches to the regulation of person-related privacy. In Europe, differences have narrowed substantially through the adoption of EU Data Protection Directive in 1995; but a substantial divergence exists with the United States which can perhaps most succinctly be summarized as a "human right" approach versus a "property right" approach (cf. Zwick and Dholakia 2001; Kobrin 2004). The European approach sees privacy as a fundamental human right, which is a precondition for the individual's autonomy and thus cannot be traded away. The burden of protection rests not with the individual, but with society. Explicit statutes and regulatory agencies to oversee enforcement are the chosen mechanisms for this, and protection can be seen as being proactive, not reactive. Historical experiences with dictatorships such as the Nazis (who used census data for the holocaust) and repressive regimes in East Europe have sensitized Europeans to the importance of data protection. In contrast, the absence of such experiences, combined with a tradition of distrust against government, led to a preference for markets and self-regulation in privacy in the United States. Privacy is seen as a property right rather than a human right, a commodity that is tradeable, and the legal system treats it like private property. Therefore the private sector and free market are seen as the most effective mechanisms for protecting privacy, with the focus being more on the consumer than the citizen. Consequently protection is often more reactive than proactive.

International disputes about regulating privacy

The different approaches taken to the protection of person-related data on both sides of the Atlantic have contributed to disputes in this area since the 1990s. Their root cause, however, lies primarily in competing economic interests and different security strategies that became evident because of the massive growth of electronic commerce and the fight agains international terrorism after 9/11/2001. But already long before that, differences had emerged. Given their early advantage in the IT industry in the 1960s and 1970s, United States' representatives had been sceptical about European moves towards data protection in the 1970s, at least as far as transborder data flows were concerned. Already on the occasion of an OECD workshop in 1977, sharp contrasts had emerged between US and the European approaches towards international data protection: Europeans saw the American championing of freedom of information and free flows of data across national borders primarily as designed to protect the advantage of the US data processing industry, while Americans suspected Europeans of erecting protectionist barriers to trade in the name of protecting privacy (Bennett 1992, p. 137; see also Bygrave 2008, p. 21).

Since the mid-1990s, past suspicions have turned into concrete conflicts across the Atlantic. Starting in the area of economic interests, their focus has shifted to issues of security policy over the last decade, thus demonstrating that the regulation of privacy is an issue which has been broadening in scope and importance. The expansion of electronic commerce, with double digit growth rates continuously surpassing those of overall economic activity, put the issue of access to electronic markets high on the agenda of policy makers: in 2001, total e-commerce (including business-to-business transactions) amounted to $1080 bn. in the United States, and $430 bn. in Europe,[11] making access to overseas markets a matter of supreme economic importance. But access to the promising European market was threatened for the United States by adoption of the 1995 EU data protection directive,[12] which limited transfer of personal data to countries with an "adequate level of protection". Despite the warnings in a legal study on privacy protection in the United States commissioned by the European Commission (Schwartz and Reidenberg 1996), the US government initially did not take the threat of trade disruption in e-commerce seriously; thus negotiations between

the two sides only began shortly before the directive was about to enter into effect in October 1998. And for a year, they were stuck as each side demanded the other adapt to its own modus operandi: EU officials wanted the United States to introduce appropriate formal legislation and authorities to protect privacy; US representatives insisted that their strategy to rely on independent privacy auditing agencies awarding seals for websites was the only possible solution to the conflict.[13] The logjam in the negotiations was only overcome when American lead negotiator David Aaron suggested the concept of a "safe harbor" – a set of principles to which companies would be able to subscribe and which would be considered "adequate" under the EU Directive. On this basis — and the assurances of the Federal Trade Commission to initiate legal action if companies failed to comply with their obligations — a compromise was struck which became known as the "Safe Harbor" agreement.[14] In July 2000, the EU Commission issued a decision certifying the adequacy of the agreement with respect to the data protection directive.

Only a year later, after the terrorist attacks of 9/11/2001, the focus of transatlantic disputes about person-related data regulation shifted from the economic to the security sphere. Negotiated compromise gave way to unilateral imposition of preferences, and the hopes expressed in academic literature that "Safe Harbor" had set an example for solving the problem of regulatory spill-over across jurisdictions and would become a model of future solutions for problems of this kind (Farrell 2003, p. 297) became dubious as two more conflicts emerged. The first was a dispute about airline passenger name records (PNRs), which included confidential information such as home addresses, credit card details, religious meal preferences and physical or medical conditions (Lyon 2003, p. 126ff.). After US Congress passed the "Aviation and Security Act" in November 2001, airlines flying from, to or through the United States were required to give the US Bureau of Customs and Border Protection electronic access to PNR data contained in their reservation and departure control systems. Since these were personal data protected under the EU directive, airlines only had the choice to either breach US law or European law and face the respective consequences ranging from penalties to landing rights withdrawal. Negotiations between the EU and the US took place, but far from reaching a compromise, analysis makes clear that the US side largely prevailed with its demands (Busch 2006, p. 312-314). When the EU Commission issued an adequacy ruling for the PNR agreement in

May 2004, the European Parliament decided to take the Commission to the European Court of Justice to demand an annulment of both the agreement and the ruling, thus adding an intra-European dimension to the conflict.

In 2006, another transatlantic dispute arose over person-related data and privacy. Through investigative reporting by the New York Times (Lichtblau and Risen June 23, 2006), it emerged that since late 2001 the US administration had gained access to the data of worldwide financial transactions held by the Society for Worldwide Interbank Financial Telecommunication (SWIFT) for the purposes of the "Terrorist Finance Tracking Program". 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. With over 8000 customers in more than 200 countries, it routes up to 12 mio. transactions per day with a volume of up to 6 trillion US-Dollars. The data had been subpoenaed in the United States, where one of the two data centres of SWIFT happened to be located. As the huge data transfer had been kept secret, the reaction across Europe was one of indignation from governments and privacy supporters, but also from business associations who feared the data might be used for the purposes of industrial espionage. Reactions included the decision by SWIFT to subscribe to the "Safe Harbor" agreement and to move its data centre out of the US, while negotiations between the EU and the United States resulted in the Europeans agreeing in principle to the use of financial data for anti-terrorism purposes if a degree of data protection was ensured. However, both the PNR case and the SWIFT case became politicised because of growing worries in Europe about the increasingly restrictive stance of anti-terrorism policy and the extension of police and secret service powers. The European Parliament took up these complaints, and through its increased powers under the Lisbon Treaty was able to vote down existing agreements with the United States in early 2010, thus forcing a renegotiation.

Challenges for regulating privacy in the 21st century

As a political issue, the regulation of privacy is more likely to gain in salience than to lose in the years to come. This is due to the increased importance of the issue on the international level as described in the previous section, but also to growing demand from the population to protect privacy better as demonstrated by opinion polls. For irrespective of the different regulatory approaches across the Atlantic, citizens both in Europe and in the United States feel that their privacy is increasingly under threat. In the United States, already in the 1990s, the share of respondents who were "very" or "somewhat" concerned about their personal privacy rose from 80 per cent in 1990 to 94 per cent in 1999; in 2002, 34 per cent of respondents felt "basically safe" about their right to privacy, and 65 per cent thought it was either "under serious threat" or had "already been lost"; by 2005, the respective numbers had dropped to 16 per cent and risen to 82 per cent (National Research Council 2008, p. 288, 290). In the European Union, concern about data privacy varies considerably between countries, with a mean of 64 per cent being "very" or "fairly" concerned about data privacy (with variations ranging from 32 per cent in the Netherlands to 86 per cent in Germany and Austria); over the past decade, concern has clearly been on the increase, with particularly strong upticks in countries where citizens had previously been highly concerned about the issue (Gallup Europe and European Commission 2008, p.7-9). In Europe, recent worries about privacy protection have helped spawn a new political movement in the shape of the "Pirate Party", which has an international umbrella organisation that helps coordinate the national parties.[15] Starting from Sweden in 2006, Pirate Parties have started to contest elections and in 2009 won two seats in the European Parliament election (from 7.13 per cent of the vote in Sweden) as well as polling two per cent in the German general election (making it the strongest party not to enter parliament).

In the decades since the 1970s, data protection legislation has spread across the globe from its origins in West Europe to North and South America, East and Central Europe, Australasia, the Middle East and Asia (see the helpful overview in Bennett and Raab 2006, p. 127). Much of that legislation has been influenced by diffusion,

policy learning, and a network of policy experts largely consisting of data protection commissioners, and this at an early point led scholars to diagnose policy convergence which was expected to continue as privacy legislation spread to more countries (Bennett 1992, chs 3 and 4). Especially United States' privacy standards were expected to see some "ratcheting up" through a variety of mechanisms such as EU collective action and market clout, firms' desire to expand their markets and the constraints of supranational trade rules (Regan 1993; Shaffer 2000). And some projected the EU Data Protection Directive to establish itself as a "global standard" (Heisenberg and Fandel 2004).

In reality, things have moved far more slowly than had been expected. This may have been influenced by the international fight against terrorism since 2001, which saw a strengthening of state law enforcement and secret service powers — not least in information technology and surveillance capabilities — around the world, accompanied by (as critics state) a weakening of privacy and data protection (Klosek 2007; National Research Council 2008). But besides that, divergent economic interests as well as the slow march of international negotiations have also hampered convergence developments more than had been expected. European standards of data protection as embodied in the 1995 EU Directive have for example influenced Australian privacy legislation (Westin 2003). However, as information becomes a key asset in the twenty-first century world economy, OECD countries' role in the global IT industry is changing, and with it the regulatory landscape. As countries such as the BRIC economies develop their IT industry capabilities and compete in the worldwide market for data processing, the question of privacy standards gains new importance. The race for the setting of a global standard in this field is dominated by two competing approaches, namely the European and the United States' ones outlined above. Both sides are positioning themselves, and the United States have been using their membership of APEC to influence that organisation's Privacy Framework to advocate their own (and, compared to the European level, lower) standards of privacy protection (Greenleaf 2003, 2005) and help create a competitor for the EU directive.

Regulatory competition can lead to different dynamics which can either lead to tighter regulation (a "race to the top") or to lighter regulation (a "race to the bottom") (Vogel 1986). But which of the two dynamics is likely to prevail in the competition

for an international standard in privacy regulation? While a lower standard, in so far as it carries lower compliance costs, may bring a cost advantage to national industry and thus help compete in the marketplace, this need not be an advantage in the competition for setting an international standard. For regulatory standards are a public good which creates a common point of reference and can contribute to overall market growth. In banking regulation, for example, agreements about minimum capital adequacy standards and their quick international dissemination have shown that tighter regulation may actually become a market advantage (Genschel and Plümper 1997). As a consequence, a rationale exists for non-OECD economies such as India which compete for outsourcing of North American and European data processing to adopt the tighter European standards of privacy protection which helps them gain access to that particular market. However, whether the market logic that underlies the process outlined here will prevail remains to be seen. Others have pointed to factors impeding convergence on an international standard, including the lack of an international organisation sufficiently strong to bridge the differences in national approaches (Bygrave 2004, p. 347-348) and the importance of "legal transplantation" between national legal systems (Reidenberg 2000, p. 1370f.). In addition, the possible influence on such a process through political pressure is an aspect that should not be discounted when trying to make probability assessments about future developments, especially in an area that is of such strategic and economic importance as regulation affecting the international exchange of data and information.

Bibliography

Allen, Anita L. (2005), 'Privacy', in: Hugh LaFollette (ed.), *The Oxford Handbook of Practical Ethics*, Oxford: Oxford University Press, 485—513.

Asia-Pacific Economic Cooperation (2004), *APEC Privacy Framework: 16th APEC Ministerial Meeting*, Santiago, Chile, 17-18 November 2004, www.apec.org/

Australian Law Reform Commission (2008), *For your Information: Australian Privacy Law and Practice,* Report, Canberra, Law Reform Commission.

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 (2006), *The Governance of Privacy: Policy Instruments in Global Perspective*, Cambridge, MA, London: MIT Press, 2. ed.

Black, Julia (2008): *Forms and paradoxes of principles-based regulation*. London School of Economics and Political Science. (LSE law, society and economics working papers, 13-2008).

Brands, Stefan A. (2000), *Rethinking Public Key Infrastructures and Digital Certificates: Building in Privacy*, Cambridge, MA, London: MIT Press.

Burnham, David (1983), *The Rise of the Computer State*, London: Weidenfeld and Nicolson.

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), 304-321. www.law.ed.ac.uk/ahrc/script%2Ded/vol3-4/busch.asp

Bygrave, Lee A. (2004), 'Privacy Protection in a Global Context — A Comparative Overview', *Scandinavian Studies in Law,* 47, 319-348.

Bygrave, Lee A. (2008), 'International agreements to protect personal data', in James B. Rule and Graham Greenleaf (eds) (2008), *Global Privacy Protection*, Northampton, MA: Edward Elgar, pp. 15-49.

Council of Europe (1981), *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data,* (Convention 108), Strasbourg: Council of Europe.

Council of Europe (2001), *Additional Protocol to the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data Regarding Supervisory Authorities and Transborder Data Flows,* (Convention 181), Strasbourg: Council of Europe.

Electronic Privacy Information Center (2007), *Privacy and human rights 2006: An international survey of privacy laws and developments*, Washington, D.C.: Electronic Privacy Information Center et al.

Etzioni, Amitai (1999), *The Limits of Privacy*, New York: Basic Books.

European Union (1995), 'Directive 95/46/EC of the European Parliament and of the Council on the protection of personal data with regard to the processing of personal data and on the free movement of such data', *Official Journal of the European Communities* (L 281/31).

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

Gallup Europe and European Commission (2008), *Data Protection in the European Union*: *Citizens' perceptions: Analytical Report*, Brussels.

Gavison, Ruth (1992), 'Feminism and the Public/Private Distinction', *Stanford Law Review* 45, 1-45.

Genschel, Philipp and Thomas Plümper (1997), 'Regulatory competition and international co-operation', *Journal of European Public Policy* 4 (4), 626-642.

Greenleaf, Graham (2003), 'APEC Privacy Principles: more Lite with every version', *Privacy Law and Policy Reporter* 10 (6). www.austlii.edu.au/au/journals/PLPR/2003/50.html

Greenleaf, Graham (2005), 'APEC's Privacy Framework: A new low standard', in *Privacy Law and Policy Reporter* 11 (5). www.austlii.edu.au/au/journals/PLPR/2005/1.html

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

Heisenberg, Dorothee and Marie-Hélène Fandel (2004), 'Projecting EU Regimes Abroad: The EU Data Protection Directive as Global Standard', in Sandra Braman (ed.), *The Emergent Global Information Policy Regime, International Political Economy Series*, Basingstoke: Palgrave Macmillan, pp. 109-129.

Klosek, Jacqueline (2000), *Data Privacy in the Information Age*, Westport, Conn: Quorum Books.

Klosek, Jacqueline (2007), *The war on privacy*, Westport, Conn.: Praeger Publishers.

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

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

Lyon, David (2003), *Surveillance after September 11, Themes for the 21st Century*, Cambridge: Polity Press.

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

Moore, Jr., Barrington (1984), *Privacy: Studies in Social and Cultural History*, Armonk, N.Y, London: M.E. Sharpe.

National Research Council (ed.) (2008), *Protecting Individual Privacy in the Struggle against Terrorists: A Framework for Program Assessment*, Washington D.C.: National Academies Press.

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

Newman, Abraham L. and David Bach (2004), 'Self-regulatory trajectories in the shadow of public power: Resolving digital dilemmas in Europe and the United States', *Governance* 17 (3), 387-413.

Niblett, G. B. F. (1971), *Digital Information and the Privacy Problem*, *OECD informatics studies*, vol. 2, Paris: Organisation for Economic Co-operation and Development.

O'Harrow, Robert (2006), *No Place to Hide: Behind the Scenes of of our Emerging Surveillance Society*, New York: Free Press.

Organisation for Economic Co-operation and Development (1981), *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, Paris, Washington, D.C: Organisation for Economic Co-operation and Development.

Organisation for Economic Co-operation and Development (2002), *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, Paris: Organisation for Economic Co-operation and Development.

Organisation for Economic Co-operation and Development (2003), *Privacy Online: OECD Guidance on Policy and Practice*, Paris: OECD.

Packard, Vance Oakley (1964), *The Naked Society*, London: Longmans.

Papakonstantinou, Vagelis (2002), 'Self-regulation and the protection of privacy', *Frankfurter Studien zum Datenschutz*, vol. 22, Baden-Baden: Nomos.

Prosser, William (1960), 'Privacy', *California Law Review* 48 (3), 383-423.

Regan, Priscilla M. (1993), 'The Globalization of privacy: Implications of recent changes in Europe', *American Journal of Economics and Sociology* 52, 257-274.

Regan, Priscilla M. (2003), 'Safe harbors or free frontiers? Privacy and transborder data flows', *Journal of Social Issues* 59 (2), 263-282.

Regan, Priscilla M. (2008), 'The United States', in James B. Rule and Graham Greenleaf (eds.), *Global privacy protection*, Northampton MA: Edward Elgar, pp. 50-79.

Reidenberg, Joel R. (2000), 'Resolving Conflicting International Data Privacy Rules in Cyberspace', *Stanford Law Review* 52, 1315-1371.

Rössler, Beate (2005): *The value of privacy*. Cambridge UK, Malden MA.: Polity.

Royal Academy of Engineering (2007), *Dilemmas of Privacy and Surveillance: Challenges of Technological Change*, London: Royal Academy of Engineering.

Schneider, Elisabeth M. (1991), 'The violence of privacy', *Connecticut Law Review* 23, 973-999.

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

Shaffer, Gregory (2000), 'Globalization and social protection : the impact of EU and international rules in the ratcheting up of US. Privacy standards', in *Yale Journal of International Law* 25 (1), 1-88.

Solove, Daniel J. (2008), *Understanding Privacy*, Cambridge, Mass.: Harvard University Press.

Solove, Daniel J.; Marc Rotenberg and Paul M.Schwartz (2006), *Information Privacy Law*, New York, NY: Aspen Publishers, 2nd (ed ed. / edn ??)

Sykes, Charles J. (1999), *The End of Privacy*, New York: St. Martin's Press.

UNCTAD (2004), *E-Commerce and Development Report 2004*, New York, Geneva: United Nations.

Vogel, David (1986), *National Styles of Regulation: Environmental policy in Great Britain and the United States, Cornell Studies in Political Economy*, Ithaca: Cornell University Press.

Waldo, James; Herbert L. and L. I. Millett (eds) (2007), *Engaging Privacy and Information Technology in a Digital Age,* Washington, DC: National Academies Press.

Warren, Samuel D. and L. D. Brandeis (1890), 'The Right to Privacy', *Harvard Law Review* IV (5), 193-220.

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

Westin, Alan F. (2003), 'Social and political dimensions of privacy', *Journal of Social Issues* 59 (2), 431-453.

Zwick, D. and N. Dholakia (2001), 'Contrasting European and American approaches to privacy in electronic markets: Property right versus civil right', *Electronic markets* 11 (2), 116-120.

[1] Quoted after Westin (1967, p. 12).

[2] A recent summary of international agreements to protect personal data can be found in Bygrave (2008). A comprehensive review of transnational policy instruments in this area is chapter 4 of Bennett and Raab (2006). Excellent sources for information about international privacy law are Solove et al. (2006) and Electronic Privacy Information Center (2007).

[3] See the "Explanatory Report" about Convention 108 at http://conventions.coe.int/Treaty/EN/Reports/HTML/108.htm (19.2.2010).

[4] As of February 2010, 41 of the 47 member states had signed and ratified the convention. Russia, Turkey and Ukraine had signed but not ratified it, and Armenia, Azerbaijan, and San Marino had done neither.

[5] This latter deficiency has been corrected by explicitly adding a protocol addressing the subject of transborder data flows in 2001 (Council of Europe 2001) which makes these subject to the non-contracting countries possessing an "adequate level of protection" (Article 2 Para. 1).

[6] The generator is available at http://www2.oecd.org/pwv3/ (last accessed 20 Feb 2010). The other documents cited are printed or reprinted in Organisation for Economic Co-operation and Development (2002) and Organisation for Economic Co-operation and Development (2003).

[7] For an analysis, see for example Klosek (2000: ch. 3).

[8] See Black (2008) on the dependence of such an approach on pre-existing trust between the parties involved.

[9] The United States is the only OECD country without such an agency; in Japan, "competent ministers" for the implementation of the data protection act are designated by the Prime Minister.

[10] The United States is the only OECD country without such an agency; in Japan, "competent ministers" for the implementation of the data protection act are designated by the Prime Minister.

[11] Data after UNCTAD (2004) and *The Economist*, 15 May 2004: 9.

[12] A succinct summary of the directive can be found in Heisenberg (2005, p. 27-32).

[13] For a detailed analysis of the case, see Regan (2003); Heisenberg (2005).

[14] Details can be found at http://www.export.gov/safeharbor/ (3.3.2010).

[15] See http://en.wikipedia.org/wiki/Pirate_Parties_International for an introductory overview (2 March 2010).