Transformations of the State
CRC 597

TranState Working Papers

Privacy Self-Regulation and the Changing Role of the State. From Public Law to Social and Technical Mechanisms of Governance

Ralf Bendrath

No. 59

Universität Bremen • University of Bremen
Jacobs Universität Bremen • Jacobs University Bremen

Staatlichkeit im Wandel • Transformations of the State
Sonderforschungsbereich 597 • Collaborative Research Center 597

Ralf Bendrath

Privacy Self-Regulation and the Changing Role of the State

From Public Law to Social and Technical Mechanisms of Governance

TranState Working Papers

No. 59

Sfb597 „Staatlichkeit im Wandel“ – „Transformations of the State“
Bremen, 2007
[ISSN 1861-1176]

Ralf Bendrath

Privacy Self-Regulation and the Changing Role of the State. From Public Law to Social and Technical Mechanisms of Governance

(TranState Working Papers, 59)
Bremen: Sfb 597 „Staatlichkeit im Wandel“, 2007
ISSN 1861-1176

Universität Bremen
Sonderforschungsbereich 597 / Collaborative Research Center 597
Staatlichkeit im Wandel / Transformations of the State
Postfach 33 04 40
D - 28334 Bremen
Tel.:+ 49 421 218-8720
Fax:+ 49 421 218-8721
Homepage: http://www.staatlichkeit.uni-bremen.de

Diese Arbeit ist im Sonderforschungsbereich 597 „Staatlichkeit im Wandel“, Bremen, entstanden und wurde auf dessen Veranlassung unter Verwendung der ihm von der Deutschen Forschungsgemeinschaft zur Verfügung gestellten Mittel veröffentlicht.

Deutsche Forschungsgemeinschaft
DFG

Privacy Self-Regulation and the Changing Role of the State
From Public Law to Social and Technical Mechanisms of Governance

ABSTRACT

This paper provides a structured overview of different self-governance mechanisms for privacy and data protection in the corporate world, with a special focus on Internet privacy. It also looks at the role of the state, and how it has related to privacy self-governance over time. While early data protection started out as law-based regulation by nation-states, transnational self-governance mechanisms have become more important due to the rise of global telecommunications and the Internet. Reach, scope, precision and enforcement of these industry codes of conduct vary a lot. The more binding they are, the more limited is their reach, though they – like the state-based instruments for privacy protection – are becoming more harmonised and global in reach nowadays. These “social codes” of conduct are developed by the private sector with limited participation of official data protection commissioners, public interest groups, or international organisations. Software tools - “technical codes” - for online privacy protection can give back some control over their data to individual users and customers, but only have limited reach and applications. The privacy-enhancing design of network infrastructures and database architectures is still mainly developed autonomously by the computer and software industry. Here, we can recently find a stronger, but new role of the state. Instead of regulating data processors directly, governments and oversight agencies now focus more on the intermediaries – standards developers, large software companies, or industry associations. And instead of prescribing and penalising, they now rely more on incentive-structures like certifications or public funding for social and technical self-governance instruments of privacy protection. The use of technology as an instrument and object of regulation is thereby becoming more popular, but the success of this approach still depends on the social codes and the underlying norms which technology is supposed to embed.

CONTENTS

Privacy Self-Regulation and the Changing Role of the State
From Public Law to Social and Technical Mechanisms of Governance

PRIVACY AND REGULATION IN A GLOBAL CYBERSPACE[1]

The Internet as a case of global governance

Privacy protection is a policy field with growing importance in the information society. Though its foundations date back to early liberal philosophy, which drew a clear border between the public and private spheres of citizens' lives[2], it has been the subject of intentional political regulation only since the second half of the 20th century. This development was closely connected to the rise of computer use. The first generations of privacy and data protection laws that were enacted in Western Europe and the United States in the 1970s and 1980s envisaged few centralised databases that could be easily controlled. The rise of personal computers and widespread Internet use changed this picture drastically. Since then, self-regulatory approaches, like codes of conduct, contracts, standards and technical means, have become more widespread, corresponding to the spread of the use of computers and, more recently, data networks like the Internet. More and more personal data can be collected, processed and transferred online. Therefore, the Internet is empirically a good case to study recent developments in the field of privacy or data protection.

The Internet should also theoretically be a most likely case to observe changes in the type of governance structures. As a global space for all kinds of human interaction, it should show the typical signs of globalised governance beyond the nation-state (spatial dimension). As it is mainly run by private and transnational companies, with its technical standards being developed by transnational bodies, it should also be a most likely case for self-regulatory forms of private governance (organisational dimension). Unlike telephone networks, which were designed by hierarchical forms of coordination in and between nation states, the Internet seemed to be immune to any form of central steering.[3] Because the Internet crosses and to some extent ignores national borders[4], it un-

[1] Research for this paper was conducted in the project B4, “Regulation and Legitimacy on the Internet”. I thank Olaf Dilling, Martin Herberg, and two anonymous reviewers for their helpful comments. Clemens Haug, Nino Jordan, Dulani Perera, and Monika Tocha provided valuable research assistance.

[2] See Warren and Brandeis (1890) as a prominent example. Rössler (2001) provides a good systematisation of the liberal arguments for privacy.

[3] Surely, the core resources of the Internet, like the root server for the domain name system or the allocation of IP address ranges, are organised centrally. But normal usage is not affected by this, as routing and packet switching take place in a decentralised way.

dermines territorial forms of control (Drake 1993). In the view of many observers, this could only mean that cyberspace had to develop its own form of post-nation state control (Johnson/Post 1997). Consequently, the as yet young Internet community discussed various scenarios of “nongovernmental governance” for the net (Baer 1997) that ranged from Barlow’s famous “Declaration of the Independence of Cyberspace” (Barlow 1996) to articles on the “virtual state” (Rosecrance 1996) that only plays a networking role and is not primarily based on its territory anymore. This debate did not end with the burst of the dot-com bubble. Some years into the new millennium, we still find academic visions and findings of the “peer-production of Internet governance” (Johnson/Crawford/Palfrey 2004), or the emergence of “global civil constitutions” in cyberspace (Teubner 2003).

No academic discussion, not less any political vision, comes without sceptics. Already early on in this debate, they raised their voices against the “cyber-separatists” (for the following, see Mayer-Schönberger 2003: 605-673). They viewed “reports of the imminent death of the state as greatly exaggerated” (Post 1998: 521), and deconstructed the libertarian cyber-optimism as a new “Californian ideology” (Barbrook/Cameron 1995). There are two groups of scholars that still believe in a role of the state (Mayer-Schönberger 2003). The “traditionalists” insist that people and corporations acting online are still present in the physical space, and that the Internet also depends and runs on a physical infrastructure comprised of cables, servers, and routers. As these are located in national territories, they can become objects of the state monopoly of force. Implementation of regulation and enforcement of law on the Internet might be more difficult, but not impossible (for a recent empirical account in this perspective see Goldsmith/Wu 2006). The “internationalists” are more concerned about the non-Cartesian characteristics of cyberspace, where physical distance is compressed to the question of how many hyperlinks two websites are apart, and where “safe havens” – the proverbial server on the Antilles – can be used for escaping regulation while still providing worldwide services. Because of the global extension of cyberspace, the Internationalists see multilateral cooperation between states as necessary for functioning regulation. The proper medium for global governance of cyberspace therefore would be international law – still state-based, but with global reach (Berg 2000: 1305-1362).

This surely sounds familiar to scholars who study the legal forms of global governance. In the offline-world, the equivalent of “cyber-separatism” is transnational self-regulation or “Lex Mercatoria”, the realm of independent rule-making and norm-setting by private transnational actors, mostly specialised for different industry sectors. The

[4] The real borders of the Internet exist between the different transnational network providers, not between countries.

equivalent of “Internet traditionalism” is the legal traditionalism, which still sees real law as only possible within nation-states, as this is where the last resort for law enforcement – physical force applied through the police – is located. And “internationalism” resembles the traditional forms of multilateral governance, where international law is seen as the only adequate form of reacting to interdependence and globalisation.

To summarise: One aim of this paper is to track the relation between the state and self-governance, and how it has changed over the last decades. But as the next part will show, this analysis of changes in governance structures cannot be done by purely looking at the continuum between private sector autonomy and state-based legal regulation.

Social and technical governance structures

There is a different dimension to the Internet in terms of rule-setting and rule-enforcement. In the offline world (the “meat-space”, as many netizens say), norms are *social* rules. They are generated, communicated, adapted and enforced by social interactions. They may have strong compliance mechanisms, and the most successful rules are surely the ones we have internalised and do not even recognise as such anymore. But in principle, they can be followed *or not*. Let me give an example from an offline infrastructure that has many common characteristics with the Internet – the street system. If the speed limit is set to 30 kilometres per hour in residential areas, many drivers will accept this because they think it is reasonable, and they may themselves have children who play football on their own street. But a car driver in a hurry can still decide to not obey the law and drive faster. Rule enforcement then sometimes works locally and socially, for example, if pedestrians directly show their dissatisfaction with this behaviour through more or less rude gestures. But it mostly works through some legal sanctioning mechanism: the speeding fine. If the risk - calculated from the surcharge and the chances of getting caught – is high enough, many drivers will restrain from speeding in anticipation of the consequences. But the underlying mechanism here is the risk of *ex-post* sanctions. In principle, drivers are free in their individual decisions to speed or not, even under legal rules.

This is different when physical or architectural constraints come into play. Imagine a street in a residential neighbourhood where the speed limit had been set to 30 km/h, but where many drivers still rush through it. This is often the case where the street is straight, paved, and has few bends, crossroads, or traffic-lights. In many cases, communities that do not want to bother with the high transactional costs of speeding cameras rely on a different mechanism. They set up speed-bumps. These make the drivers slow down automatically, because they do not want to damage their cars’ suspensions, or they are afraid of losing control over the car in speeding over the bumps. To most drivers, it is plainly impossible to speed over speed-bumps. The physical characteristics of a street - its architecture – have a huge impact on the drivers’ behaviour. This does not

work through social norms and the risk of ex-post sanctions, but through the architecture and ex-ante enforcement. Still, in the offline-world, speed-bumps can be ignored to some extend by getting very good suspension, huge tires, or – as an extreme example – a tank. Street traffic is based on physics, and the limitations built into the infrastructure can be overcome to some extent by using the laws of physics.

The political nature of technologies and the fact that their design can influence and control social behaviour has been widely discussed in the “Science, Technology and Society” community (Bijker 1992, Winner 1986a). Structures like road bumps, bridges, and even the design of yard door locks (Latour 1994) can determine how people can move and behave. In cyberspace, architecture has an even more constraining role than in the offline-world. If you are connected to the Internet through a dial-up modem, you can have a very fast computer, but you will still not be able to have the data packets flow faster than 56 kilobits per second. And even if you have a high-speed connection, say at a university research laboratory, some websites will not respond very fast, because the servers they are running on are slow or busy, or their uplinks are congested. While this still very much resembles the street analogy, with fast or slow cars and highways or bumpy tracks, much more constraints are possible through programming the servers, switches and routers through which the data packets flow. A street that would automatically slow down all cars headed towards a particular location is unthinkable, but in cyberspace, this is reality. The German Internet service provider Tiscali, for example, automatically slows down all traffic from its DSL customers that comes from specific ports of their computers, namely the ports used for peer-to-peer file-sharing. There are many more examples for this, from Chinese automated content filtering to the technical blocking of specific forms of Internet usage at the workplace through the companies’ firewalls. The Chinese government can enact a law prohibiting visits to critical websites (and it has done so), and companies can set social rules that discourage their employees from using instant messaging services in the office (and many have done so). But they can also build these rules into the architecture of the routers, switches and firewalls – and many have done so.

The Internet is a technical infrastructure, but it is also a social space that enables, facilitates and shapes online interactions between individuals and groups. Since all of these interactions take place in a technically mediated environment, the range of freedom and individual options for behaviour is also determined by the way the network architecture is built. This differs from large industrial socio-technical systems, which by technical design impose a strong discipline on the workers[5], but where the latter can still

[5] “The automatic machinery of a big factory is much more despotic than the small capitalists who employ workers ever have been”, (Engels 1978: 731; quoted after Winner 1986b).

go on strike and leave the factory. In cyberspace, you cannot leave the data “machines” constituted by the operating systems and network protocols. It is these regulatory characteristics of cyberspace that made Joel Reidenberg (1998) speak of a “Lex Informatica” that is different from state-based law, in resemblance to the “Lex Mercatoria” of international private trade regulation. Lawrence Lessig (1999) in a similar way has called the software code – which makes the Internet and our computers run – the “law of cyberspace”. Very much to the point, he distinguishes “West-coast code” (Silicon-Valley based software) from “East-coast code” (Capitol-Hill-based laws). We can distinguish different levels of rigidity for Lex Informatica. The operating systems our computers run on (and even more the underlying hard-wired code in the hardware) and the networking protocols can be compared to the constitution. They provide the fundament on which other applications run, and they determine what options for user control (e.g. different user account settings in multi-user operating systems like Windows XP or Unix) and identification (e.g. dynamically or statically assigned IP numbers) are possible. The equivalent of common “laws” then are applications like office software, mail clients, and web browsers and servers. While the users have some choice on this level (and can change some settings like cookie policies), the design of web servers, websites and the underlying databases depends on the choice of the corporation running it.

Software code does of course not work in a vacuum. Certainly, social and community norms also exist on the Internet about how to behave and not to behave in different contexts (the so-called “netiquette”). But even some codes can still be influenced by the user, depending on the degree of access he or she has to the computer controlling his or her online behaviour. If a website filter for indecent content is running on my personal computer which I have root access to, I can deactivate it or change its settings. If it is running on my company’s web proxy server, I would have to convince the network administrator to let me visit specific websites that would normally be blocked. If it is run by my internet provider, I would have to change the ISP. If it is run by a national exchange point or international gateway, there is normally not much I can do. What is even more interesting for political scientists as well as legal scholars are the complicated and still emerging links between state-based law, self-regulatory norms, and the Lex Informatica. How are law-makers and private norm-setting bodies reacting to technological change, and how are the technical codes influenced by law and social norms?

Applied to privacy issues, the design of websites can force users to give away more personal data than they would like to do – and more than they would do in the real world. If you want to read the New York Times online, for example, you can only do so after registering to their customer database and giving away information about your address, age, job and more. The NYT web server can then follow your “click-stream”, i.e. the way you move around on the site, which articles you read, which ads you click

and more. With “cookies” or other means, this information can even be linked to the databases of large marketing companies like DoubleClick that earn their revenues by profiling customers for other corporations. Privacy online, as should be clear now, therefore strongly depends on the technical design of the Internet. This chapter sets out to contribute to this debate with empirical findings on the role of self-regulatory norms for the protection of privacy on the Internet, and especially how social and technical codes interrelate here. Data protection (the European term) or informational privacy (the American term) as a subject of regulation has emerged with the broader use of computers in the 1960s. As the technology has changed, so have the forms of data protection regulation. Data protection norms have also had an impact on the design of the technological architectures.

Self-governance structures in the privacy field have not emerged in isolation. They were often a reaction to consumer demands, pressure from public interest groups, and the usual widely reported data-leak scandals. But the general norms of privacy protection have developed mostly in the state-based national and international governance structures of Western Europe and North America. In order to understand the emergence and growing importance of privacy self-governance, it is therefore necessary to first have a brief look at the history of public and law-based privacy and data protection regulation. Against this backdrop, we can then better understand the different self-regulatory instruments for privacy protection that have been developed since the 1990s. There are a number of different social codes and technical codes in the private sector now, with varying degrees of scope, reach, enforcement, and control over the data for customers and companies. Self-governance is surely gaining in importance in the privacy field, and some of its forms can be seen as private equivalents of legal regulation. But the story does not end there. Self-governance mechanisms of privacy protection have recently become the subject of closer influence by governments and other public bodies again. As we will see, the state is coming back - but in a different shape.

SETTING THE STAGE: STATE-BASED PRIVACY GOVERNANCE

National laws and international harmonisation

„Privacy“ has been internationally regarded as a fundamental civil liberty since the 1940s. The Universal Declaration of Human Rights (1948) already had a paragraph on privacy. The 1950 Council of Europe’s Human Rights Convention included a similar clause, and even established a court for enforcement.[6] The United States already had a judicial tradition of privacy protection since the 1890 seminal article by Samuel Warren

[6] Citizens could sue their governments in case they did not translate the convention’s protections to the national level.

and later Supreme Court judge Louis Brandeis, who coined the phrase of the “right to be left alone“ (Warren/Brandeis 1890).

These early privacy rules were originally intended as a protection against unreasonable police searches of private property or against an overly intrusive press. As a result of World War II and the experiences with the Nazi regime[7], people became more afraid of too much personal information in the hand of powerful government bureaucracies.[8] The use of computers for accounting and personnel management that emerged in the 1960s transformed the policy problem of limiting the compilation, access and use of personal files from a purely bureaucratic task into a political-technological endeavour. Now, it became „informational privacy“ (the American version) and “data protection” (in Europe) (Schwarz/Reidenberg 1996).[9] The discussion on the „Big Brother state“ was also growing.[10] The first parliaments started to draft laws to protect personal information against unlimited computer use.

The world’s first data protection law was enacted in the German state of Hessen in 1970. Shortly afterwards, Sweden (1973) and the United States (1974) followed, and slightly later West-Germany on the federal level (1977), Denmark, Austria, France, Norway and Luxembourg (all 1978) also had privacy protection laws. Until the beginning of the 1980s seven countries – all in Western Europe – had enacted data protection laws, and in the 1980s ten more followed, among them Israel, Japan, Canada and Australia (for a systematic four-country comparison between the USA, Germany, Sweden and the UK from 1960-1980, see Bennett 1992). In the 1990s, 22 more states from all continents followed, in the new millennium a few more.[11] The reasons for this general spread of privacy legislation are not the topic of this paper.[12] We can keep in mind that

---

7 The Netherlands had maintained comprehensive population registers since the 1930s, which were seized by the German government in the first three days of the occupation. The Dutch Jews as a result had the highest death rates in all occupied countries in Western Europe – including Germany. See Seltzer/Anderson (2001).

8 This historical memory had a much bigger impact on European than on American privacy debates, as U.S. political culture has always had a more sceptical view of the government, and therefore it affected the framing of the first data protection laws in Europe, see Bennett (1992).

9 In the U.S., the term „fair information practices“ is also widely used.

10 Lyon (2001) has elaborated the thesis that “privacy” only became a social value when the technologically enabled surveillance society was already a fact.

11 In 2004, the annual survey done by EPIC and Privacy International lists 62 States, among them only two from Africa, see EPIC (2004).

12 Bennett and Raab (2003) mention a change in public opinion, policy-learning, diffusion through epistemic communities and the influence of external actors (EU, Council of Europe, OECD).

there were some “waves” or “generations” of data protection legislation (Mayer-Schönberger 1998).

The technical systems then were envisioned as centralised large computer facilities which were easy to control and supervise, and where the data, once entered, would stay.

> *„In other words: There were huge cabinets full of digitised data where before there had been huge cabinets full of files, but still, it were huge cabinets.“ (Fink 2002: 85, translation RB)*

In the 1980s, the picture had already changed significantly. The globalisation of the economy led to an increase in transborder data flows. On the other hand, one of the official goals of international economic policy was (and is) free trade. Personal data, as soon as it was more widely available than before, also became a commodity (Weichert 2000). An expert group in the Council of Europe as early as 1970 had already stated the transnational character of the computer, which in turn would create a need for international regulatory harmonisation (Bennett 1992: 134). Because the different national data protection laws often had different procedural regulations for transnational data transfers, even though they rested on the same set of basic principles, this could lead to difficult legal conflicts (EU-JRC 2003: 90). In the late 1970s, the Council of Europe and the EC Parliament started to discuss how to dispose of these trade barriers while preserving data protection. The objective soon became clear: International harmonisation of data protection was needed. The European Parliament even called for the “creation of a genuine common market in data-processing” (European Parliament 1979).

Several international treaties and documents were developed in the following years that tried to harmonise international data protection. The most binding international agreement for 15 years was the Council of Europe’s 1981 „Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data“. This „influential treaty“ (Bennett and Raab 2003: 3) mandated the signatories to translate its rules into national law. Citizens of one party to the treaty now had the right to legally fight any misuse of their personal data in another country that had ratified it. The convention also included regulations on trans-border data flows and allowed restrictions on these if the data was to be transferred to a country with lower protection levels. This rule had a harmonising impact within Europe, especially on the second generation of data protection laws that were enacted in the 1980s. The convention was not relevant for data flows to third party countries who had not signed the treaty. This stayed a matter of national legislation. The Council of Europe subsequently adopted a number of recommendations for implementing the convention in specific areas that range from medical databases (1981) to privacy protection on the Internet (1999) (EU-JRC 2003: 120).

The OECD developed its 1980 „Guidelines on the Protection of Privacy and Transborder Flows of Personal Data“ in close coordination with the Council of Europe, in

order to avoid further complications. The guidelines are not binding like the Council of Europe's convention, and they had been preceded by fierce conflicts between the United States and some European governments. The Europeans perceived the very low or (for the private sector) non-existing level of data protection in the United States as unacceptable and suspected behind it an attempt to globalise the dominance of the American computer industry with the buzz phrase „free flow of information“. The U.S. in turn accused the Europeans of protectionism by means of data protection (Bennett 1992: 136f). The guidelines themselves are only a short document listing basic fair information practices. The OECD followed up in 1985 with another declaration on „transborder data flows“ that dealt with data flows within transnational corporations, trade barriers and related aspects of data protection, and envisioned better cooperation and harmonisation (OECD 1985).

For a decade, the OECD stayed the only supra-regional international organisation that dealt with privacy and data protection. Only in 1990 did the UN General Assembly adopt the voluntary „Guidelines concerning computerised data files“, which had no follow-up mechanism and therefore no real impact.

The European Parliament, as was mentioned above, had adopted several resolutions on data protection since 1976 and urged the EC Commission to draft an EC directive for harmonising national legislation. The commission was rather hesitant and only asked the member states to join the Council of Europe's Convention until 1982 (Bainbridge 1996: 22). Not until the end of the 1980s, with the common European market approaching fast, did the Commission react and hence presented a draft European data protection directive in 1990. This step was a surprise to many, as the EC was still seen as an economic community that did not deal with human rights issues. But the Commission used the same argument as the EC parliamentarians, the OECD and the Council of Europe did: It referred to article 100a of the EC treaty and presented its move as necessary for the functioning of the common European market. It took five more years of negotiations in Brussels and the Bangemann report on “Europe and the global information society” (EU 1994) that made the common European information space a highest priority, before the directive was enacted as EC95/46 (EU 1995; see Bainbridge 1996: 23-32).

The EU data protection directive is unanimously described as „the most influential international policy instrument to date“ (Bennett and Raab 2003: 5). It contains regulation on the private and public sector use of personal data, applies to manual and automated data processing, has detailed rules on implementation and mandatory data protection commissioners, and creates an oversight body on the European level (the “Article 29 Working Party”) as well as a Commission-chaired committee that can make binding decisions. It was supplemented in 1997 by a special directive for privacy in the electronic communications sector, which was further amended in 2002 to include latest

technological developments (EU 1997; EU 2002). Here, the EU tried to take into account caller-identification for telephone calls, location data for mobile phones, cookies, spam, and other new technological possibilities. Since the 1999 treaty of Amsterdam the directive also applies to data processing within the EU bureaucracy, which since then has had its own internal data protection commissioner.

The brief overview of international state-based privacy regulation shows a familiar pattern: The more binding the regulatory instruments are, the shorter their reach is. National data protection laws, even if harmonised through the EU directive, are still the most precise legal regulations, and they can also be enforced by oversight authorities (the public data protection commissioners) and, as a last resort, by the courts. The EU directive is wider in scope and still fairly detailed. It has the Commission committee and the Article 29 Data Protection Working Party as oversight bodies, and it stipulates some fundamental - substantial and institutional – provisions for the national laws. But as it is an EU directive, specific implementation and direct compliance control over the private sector are still delegated to the national level, according to the subsidiarity principle. The Council of Europe’s Privacy Convention is wider in reach than the EU directive, as the organisation includes European states that are not EU members. But even though it is a binding international treaty, it only provides a basic set of fundamental data protection principles. It is less precise in giving institutional directions to its parties, and it has created no day-to-day oversight body and instead relies on the European Court of Human Rights. The OECD guidelines not only apply to Europe, but also to North America and the Asian developed countries. But they are completely voluntary and do not constitute international law. Instead, they rely on the OECD Committee for Information, Computer and Communications Policy’s attempts to achieve adoption of the guidelines by the private sector. The UN Guidelines are, in principle, global in reach, but they are neither precise nor binding, and they do not have any follow-up or implementation mechanism. Precision and enforcement of state-based privacy regulation are therefore the strongest at the national level within the EU, and they get weaker in concentric circles which are constituted by the EU, the OECD, and the United Nations.

The Internet, Safe Harbor, and the rise of self-governance

Thirty years after the first generation of data protection laws had been enacted, the technological developments turned out less as “Big Brother”, but more as “Little Sisters”. The European model of registering and overseeing few large data bases hosted in large computer facilities was already reaching its limits in the late 1970s, with the emergence of mini-computers. In the mid-1980s, when the personal computer hit the market, the use and processing of all kinds of data – including personal data – was finally beyond the reach of effective government oversight. After the advent of the Internet as a mass medium in the 1990s, this problem became even worse, as the trade and flow of per-

sonal data across borders was only a matter of seconds now. The big corporations were still easy to control, but they also had the resources for fighting against too tight government controls and prohibitions. Swire and Litan (1998: 200-204) use the instructive metaphor of elephants and mice: Elephants are large and easy to spot, but they also have the ability to inflict considerable damage on their environment. The problem, though, are the mice – the small companies that easily re-locate, are hard to control, “and breed annoyingly quickly” (ibid: 201). Data protection therefore could only work if government oversight was combined with functioning self-regulation in the private sector. This had been the U.S. approach all along the way since the first privacy act for control of government use of data had been enacted in 1974. The EU directive also reflected this approach, because it discontinued the mandatory registration of databases with the data protection supervisory authorities. Nowadays companies can appoint internal data protection commissioners (or even outsource this job to specialised service providers) and thereby comply with the directive and the according national laws.

The driving force behind the move towards more self-regulatory approaches in data protection was therefore a change in the structure of the regulated problem. If everybody became a potential user and collector of personal data, then top-down enforcement and central oversight mechanisms would not work anymore – at least this was the perception. The answer was an attempt to infuse data protection ideas and their social agents into the private sector itself.

The other influence beyond these technological developments was political, and here, transatlantisation was more important than globalisation. The negotiations over the OECD guidelines from 1980 had already led to heavy conflicts between the Europeans and the U.S. government. The conflict between American „free flow of information“ and European „privacy“ was barely covered in the guidelines. On one hand, the guidelines are totally voluntary in nature, which was intended by the U.S.; on the other hand, they at least set some lowest common denominator for fair information principles and therefore met the interests of the Europeans.

The problem became more apparent in 1995, after the EU directive had been enacted. For the first time, the directive, as an international instrument, harmonised data transfers to third-party countries. Because of this feature, it had an impact far beyond the European Union, and this is why we can speak of “globalisation” here, not just “Europeanisation”. EU Member states are only allowed to approve data exports of personal data if there is an “adequate level of protection” in the recipient country. If there is no comparable legislation in place, the companies wanting to export the data can do so only if this is based on a contract with the company that receives the data. The contract also has to ensure adequate protection for further re-export. This clause has created a significant adaptational pressure on third countries (Charlesworth, 2000). The EU later also devel-

oped standard contract clauses for data exports (EU Commission, 2002). The EU's adequacy provisions are "the *de facto* rules of the road" for global data processing (Bennett and Raab 2003: 6).

As there is no comprehensive data protection legislation for the private sector in the U.S., but binding third-party data export rules in the EU, there seems to be a dilemma: Either the EU Commission could have treated the United States data protection regulation as "not adequate" and risked another transatlantic trade war, or it could have turned a blind eye on the U.S. and heavily damage the credibility of the whole directive. Even before the transatlantic conflict was resolved, the EU directive helped create pressure against the United States to raise its level of data protection for the private sector. The Clinton administration was afraid the EU Commission could lock American companies out of the large European market for e-commerce, because the lack of comprehensive data protection legislation in the U.S. could mean an "inadequacy" rating. Before the directive had to be implemented on the national levels in 1998, the U.S. government therefore tried to convince the EU that self-regulation worked (e.g. with a comprehensive compendium, US DoC, 1997). At the same time, it also started pushing the private sector into seriously self-regulating data protection. Some parts of the administration, especially in the Federal Trade Commission, even threatened to adopt legal measures if self-regulation would not work quickly. Therefore, the self-regulatory instruments have been called „the Directive's bastard offshoots“ (Shaffer, 1999: 433). Unexpected help for this came from international trade regulation. The World Trade Organisation's 1994 General Agreement on Trade in Services (GATS) mentions privacy, but as an exception from otherwise liberalised trade in services, including data services (WTO, 1994).[13] By doing this, trade liberalisation did not curb the need for the U.S. to raise their level of privacy protection, and even limited their ability retaliate (Shaffer, 2000: 86).

After long negotiations, the EU commission and the U.S. Department of Commerce sealed a „Safe Harbor“ agreement in July 2000 (Fink 2002; Farrell 2003; Heisenberg 2005). It can be called "hybrid" or "interface solution" (Farrel 2002), because it is a link between two different regulatory approaches: The European, law-based and comprehensive privacy regulation and the American, private sector-based and sectoral privacy regulation. Under Safe Harbor, the object of the important adequacy rating by the Commission is not a country anymore, but a single company. Therefore, the U.S. could keep its data processing industry partly unregulated, and the EU could allow data trans-

[13] "nothing in this Agreement shall be construed to prevent the adoption or enforcement by any Member of measures (…) necessary to secure compliance with laws or regulations (…) including those relating to (…) the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts." (WTO 1994, article XIV).

fers to American companies under the condition they subjected themselves to the Safe Harbor principles. The mechanism is quite simple:

> *“The decision by U.S. organizations to enter the safe harbor is entirely voluntary. Organizations that decide to participate in the safe harbor must comply with the safe harbor's requirements and publicly declare that they do so.” (U.S. DoC 2005)*

As of May 2006, 950 companies have entered the Safe Harbor (U.S. DoC 2006). The agreement is – naturally for a compromise – weaker than the EU regulation. There is no possibility for EU citizens to legally insist on getting information about what is happening to their data in the U.S., or for European data protection commissioners to inspect the processing companies on the other side of the Atlantic. The European Parliament therefore strongly resisted the agreement, but because the judgment on “adequacy” according to the 1995 directive was delegated to the Commission, could not do much against it. But the agreement still comes with public oversight and enforcement, because it used a general clause in U.S. trade regulation. Companies that have joined Safe Harbor and get caught red-handed can be fined by the Federal Trade Commission for “unfair and deceptive trade practices”. There is also an arbitration procedure in cases of complaints, where the arbitrator can be chosen between private providers like TRUSTe or public authorities like the EU data protection commissioners.

The regulatory regime of Safe Harbor therefore consists of several layers: The EU is setting the substantive data protection standards, the companies voluntarily commit to them, private or public bodies provide arbitration services, public enforcement is done by a U.S. agency, and the EU commission still has the last word and can terminate the whole agreement if compliance or public oversight in the U.S. are not working. Safe Harbor therefore can be seen as a hybrid arrangement that integrates transnational self-regulation on the one hand, and nation-state based and intergovernmental public regulation on the other hand, into a complex, layered regime.

SELF-GOVERNANCE INSTRUMENTS OF PRIVACY PROTECTION

In the Safe Harbor regime, the private sector has a much more important role than in the traditional European regulation model, which was mainly based on public oversight and inspection bodies. Under Safe Harbor, most of the oversight functions as well as the day-to-day supervision are done by the private sector itself. The states only set the minimum data protection level, and it has the means of last resort in case there are serious non-compliance problems. The process leading up to the agreement in this regard was a learning experience for European data protection commissioners and regulators, and it has greatly enhanced the acceptance for private-sector self-regulation instruments. In this part, I will give an overview of the different instruments that are available today.

As we will see, they still differ greatly in terms of precision, reach, scope, and enforcement mechanisms.

Social codes

Internal corporate rules

The simplest form of self-regulation is when a company publicly declares that it adheres to a minimum set of privacy principles. This has become quite popular on the Internet. A “privacy policy” is nowadays found on most corporate websites, but the idea dates back to the early days of transborder data flows. The OECD has repeatedly urged the private sector to adopt the 1980 privacy guidelines. It has even developed an online privacy-statement generator to help website providers be more transparent about what data they collect, how they use it, what dispute-resolution mechanisms are available and so on.[14] According to OECD staff, this is not meant as a legal instrument, but rather as a means of making corporate data handlers think more closely about the mechanisms and organisational requirements for a sound data protection policy. Often, corporate privacy commitments are rather a reaction to bad publicity and a public relations operation than a serious attempt to change the company’s internal and external data usage. They more resemble indications of what the management or the customer relations department believe should happen than an internal policy for employees or a guide for binding organisational practices (Bennett and Raab 2006: 154).

More recently, companies have started to translate their privacy statement into clear guidelines for their employees, so-called “organisational codes”. Early examples of these were developed by multinational companies like American Express or Readers’ Digest, some of them followed as a result of customer surveys. Some global corporations have also started to adopt “binding corporate rules” for privacy protection that apply to all subsidiaries worldwide, no matter if their country of residence has privacy legislation in place or not. Prominent examples are DaimlerChrysler, General Electric or Siemens. They come closest to a new form of an internal corporate private law of data protection.

Many companies have also now established internal oversight mechanisms for ensuring compliance with the organisational privacy codes. This model goes back to early German data protection legislation, which from the beginning had a unique model of institutionalising self-regulation in the private sector. Here, companies can avoid the burden of registering their data banks with the public oversight bodies if they create the position of an independent corporate data protection commissioner. This model has been incorporated into the 1995 EU directive (EU 1995, recital 49) and since then has

[14] <http://www.oecd.org/sti/privacygenerator>

been widely accepted all over the corporate world. These “chief privacy officers”, as they are mostly called now, are organised in transnational professional organisations such as the International Association of Privacy Professionals (IAPP), and they regularly meet with the public privacy commissioners.

Codes of conduct for business associations

More encompassing are the codes that have been developed for whole industry sectors („sectoral codes“, Bennett and Raab 2006: 155-157). A number of codes of conduct are now available from different industry and trade associations, mainly in the United States, ranging from the Direct Marketing Association to the Associated Credit Bureaus. These sectoral codes have become quite popular in the last few years. If they do not apply to a specific sector but to generic business functions like customer relations management or human resources management, they are also called “functional codes” (ibid: 157).

Different from organisational codes, application of and adherence to these sectoral or functional codes are often mandatory for members of the respective trade or business association. They are also offered by specialised third-party entities like auditing services or consultancy firms. Many of these self-regulating mechanisms are giving “privacy seals” to websites that publicly declare their adherence to the specific data protection standard. The most popular ones are TRUSTe and Better Business Bureau (BBB) Online. Enforcement in general is not very strict, but business associations play an increasing role in educating their members about privacy best practices. The inherent problem is that the certification providers depend on funding by their members or customers, so tough measures against the ones who break the rules are unlikely. TRUSTe, for example, got under public pressure after it did not properly follow accusations against its member Microsoft (Boutin 2002; Richardson 2000). A study conducted in 1999 by Forrester Research concluded that privacy seal providers become more an advocate for the industry than for consumers (EPIC 2004: 110). On the other hand, business associations (s.o.) play an increasing role in educating their members about privacy best practices, through specialised seminars, training services, and newsletters. This form of self-regulation, therefore, resembles the “managed compliance” approach more than the enforcement approach.

The purely technical environment of the Internet and the World Wide Web allows for new forms of oversight. TRUSTe has started to automate the compliance checks through a mechanism called “seeding”, whereby unique data is entered into websites, allowing the detection of privacy-invasive data handling by the respective web-service later on. Even more stringent is a programme called WebTrust, developed jointly by the U.S. and Canadian associations of certified public accountants. Based on the high professional standards of the accounting profession, it is now being offered throughout

North America as well as in Hong Kong, Australia and a growing number of European Countries (Bennett and Raab 2006: 166). It can be expected that these professional efforts, combined with public pressure from consumer groups and privacy advocates, will serve as a strong incentive for self-regulatory bodies to strengthen their privacy compliance and control mechanisms.

The main problems of these self-regulatory mechanisms lie elsewhere. First, they only certify the adherence to a minimal set of fair information practice principles. These are often less privacy supportive than comparable EU legislation, e.g. with opt-out instead of opt-in mechanisms for commercial marketing as the norm. Second, the seal providers also cannot do anything against companies that are not participating in these voluntary agreements. In July 2006, only 694 websites participated in the BBBOnline privacy programme (BBBOnline 2006), and in 2005, 1975 sites had been certified by the TRUSTe seal (TRUSTe 2006).

Mandatory membership in professional associations can therefore be a strong support for self-regulatory privacy protection instruments. A very strong version of privacy codes of conduct are “professional codes” (Bennett and Raab 2006: 14). They apply to professional associations and have a direct influence on their individual members, not on companies. Well-known examples are the age-old codes for physicians or lawyers, who are bound to professional discretion in the relationships with their patients or clients. As the membership in these professional organisations like medical associations or the bar is mandatory for conducting the respective profession, misconduct can lead to exclusion and a loss of the professional license.

Codes of conduct have become a standard instrument of privacy governance by now, and their mechanisms for compliance and certification have strengthened. Most of them have emerged in the United States, as their prime users are American companies, but due to the transnational nature of many businesses, they have been constantly growing in their spatial reach. Some of these efforts are now being developed on a global scale, the most prominent being the Global Business Dialogue on electronic Commerce’s guidelines for „consumer confidence“ (GBDe 2001) and the International Commerce Exchange on a “Global Code of Conduct”. Other global efforts in this direction have started in the International Air Traffic Association and the Federations of Direct Marketers (Bennett and Raab 2006: 156). Typically, these transnational codes of conduct have been developed in close contact with the international community of data protection commissioners, and some even with active participation by privacy advocacy groups. TRUSTe was even founded as a joint effort of the Boston Consulting Group and the Californian NGO Electronic Frontier Foundation (EFF). But this is not a typical example, as the cooperation between corporate entities, NGOs and public commissioners is normally much less institutionalised and formalised. Instead of the highly formal-

ised forms of business-NGO-cooperation found in other industry sectors, the field of privacy policy is still dominated by a loose diffusion of ideas through constant and decentralised discussions within an epistemic community that comprises public commissioners, privacy advocates, and corporate chief privacy or chief technology officers.

Contractual solutions in business networks

Contracts are often used as a case-by-case substitute for missing privacy legislation. They are common in big corporations who hold large amounts of personal data about customers and employees and contract out some of the work related to these. The business agreement then has sections that regulate how the contractor can use the data, who holds property to it, if and how it can be transferred to third parties etc. Specific privacy contracts have been used since the late 1970s for allowing transborder data flows under national data protection laws. In France, the use of private contracts has been quite popular early on, but other European states have also relied on contractually ensuring that personal data exported to other countries is handled according to the legislation in the country of origin. The national data protection authorities have played a crucial role in pushing for the use of this instrument (Ellger 1996).

As early as 1992 the Council of Europe developed a model contract for transborder data flows with the cooperation of the EU commission and the International Chamber of Commerce. Some other groups like the “Düsseldorfer Kreis” of German data protection commissioners have also been active in this area (Ellger 1996). The EU followed this path with the adoption of its data protection directive in 1995, which accepts standard contractual clauses to ensure an adequate level of protection for transborder data flows to third countries. These standard clauses must be verified or developed by the EU Commission, which has updated them several times.

There are several limitations to this approach. First of all, what follows from the fact that the affected party – the citizen, customer, or user – is not subject to the contract? This might not be a problem in the continental European tradition, but the Anglo-Saxon *common law* countries do not have the concept of third party rights derived from a contract between two other parties. Therefore, the legal enforcement of these contract clauses is difficult.[15] Enforcement of contract clauses depends not only on the legislation (i.e. the country) chosen as the basis, but also on the national laws in the import country and on the interests of the receiving party. Specific laws (e.g. for intelligence agencies) might override strong protections in private contracts.

On the other hand, these contracts are even used to raise the data protection level within a country. If companies want to ensure their contractors adhere to high data pro-

[15] The United States have given up the strict use of the privity-of-contract doctrine and allow third party beneficiaries in private contracts (Ellger 1996: 765).

tection standards, they can insist on incorporating EU-certified standard data protection clauses into the business agreement. Also, government agencies with their huge purchasing power have used this as leverage where mandatory data protection laws are lacking.

This private data protection law of contracts has proven to be a useful instrument especially to extend the European Union’s data protection standards to countries where national legislation is lacking or not deemed adequate. Thereby, the use of EU data protection standard is slowly being incorporated into private sector data usage all over the world. This shows how private law can help spreading a regional legal standard through the use of mandatory data export control clauses (Reidenberg 1999).

Standards

Privacy standards go further than commitments of voluntary codes of conduct, because they provide a set of objective criteria and at the same time a defined process by which compliance can be tested. Standards here do not mean technical standards or networking protocols, but a standardised way of measuring the performance of how technology and social practice are integrated into an organisation. There has been some discussion about general privacy standards linked to the generic quality management standards of the ISO 9000 series. Standards normally also have strict oversight and compliance mechanisms that go further than voluntary codes and are more comparable to professional codes.

The first real privacy standard was the Canadian „Model Code for the Protection of Personal Information“. It had been developed since 1992 by trade associations and consumer organisations together with the Canadian government and the Canadian Standards Association (CSA). The objective was to harmonise the different self-regulatory codes, but it was also a reflection of the failed attempts of the OECD in this field. The model code was officially recognised as a „National Standard of Canada“ in 1996. Organisations that voluntarily adopt the standard are then bound to mandatory quality controls by the CSA. Standards similar to the Canadian Model Code have also been developed elsewhere. The Japanese Standards Association in 1999 published the standard JIS Q 15001 (“Requirements for Compliance Program on Personal Information Protection”), which is modelled in detail after the structure of the environmental management standard ISO 14001 (Bennett 2004a: 234). JIS Q 15001 was developed out of a government-issued norm, the 1997 Data Protection Guidelines from the Ministry of International Trade and Industry (MITI) (Privacymark.org 2006). The Australian Privacy Commissioner in 1998 published “National Privacy Principles” that resemble the Canadian model (Bennett 2004a: 234).

On the international level, the Council of the International Standards Organisation (ISO) in 1996 initiated a process for the development of an international privacy stan-

dard after pressure from ISO's Consumer Policy Committee. Because of heavy lobbying from U.S. corporations and criticism from European data protection commissioners, ISO has not yet been able to agree on a standard. The European standards body Comité Européen de Normalisation (CEN) has also been studying the feasibility of an international privacy standard. CEN works together with the EU's data protection commissioners (Bennett 2004a: 236).

Comparison

While national privacy standards have been successful in a few cases, an agreement on a global privacy standard has proven to be very difficult. On the other hand, privacy codes of conduct within single corporations are very binding and detailed. Sectoral codes and global industry guidelines still tend to be more lists of general principles rather than specific routines. Those codes of conduct that have institutionalised compliance mechanisms are somewhat in the middle. Theoretically, they apply to a large number of corporations across the globe, but practically, these still have to subscribe to them (and pay for them) individually. Contractual solutions only apply to the trading partners that include them in their business agreements, and they are mostly used by EU-based corporations that want to transfer data to third countries. As there are no highly integrated "supply chains" for personal data, the network of contractual privacy protections is still rather loose, and it does not have a broad trickle-down effect like e.g. product standards do in the car manufacturing sector. The most binding forms of privacy self-regulation are still the very old professional codes for lawyers, physicians, and priests. Here, compliance is to a large extent self-enforcing, because customer confidence in the secrecy of their information is at the core of the business model. Additionally, non-compliance can also mean loosing the licence to practice the profession any longer.

This resembles what we found above about the state-based privacy regulation efforts: There is a trade-off between reach on the one hand, and precision and enforcement on the other hand. At first sight the same pattern seems to apply to privacy self-regulation. The more detailed the privacy codes are in terms of regulating data use (limited scope), the less likely they have a wide applicability (global reach). But whereas state-based regulation differs along territorial or regional borders (nation, Europe, OECD), private self-regulatory instruments apply to organisations or sectors and to a growing extent ignore geography. While DaimlerChrysler's internal binding rules for privacy only apply to the corporations' employees and data subcontractors, they are valid and enforceable all over the world, from Stuttgart and Detroit to Johannesburg or Mumbai. The IATA privacy code of conduct applies to all air carriers that are members of this organisation, just like the confessional secret is binding to priests of the Catholic Church all over the world. The "death of distance" through the Internet as well as the general growing integration of the global economy have also made privacy self-governance instru-

ments grow out of their territorial origins and see worldwide adoption. The privacy seals for websites that are provided by companies like TRUSTe or BBBOnline, while they were a purely U.S.-based reaction to the EU directive and the transatlantic Safe Harbor agreement, are now also available for and used by companies in the Far East. The Japanese Information Processing Development Centre (JIPDEC) in 2000 entered into a mutual privacy seal recognition programme with BBBOnline (Bennett and Raab 2006: 167). Standard contract clauses for business-to-business data transfers first emerged in the EU, in order to make data exports possible to countries that lack adequate legislation. But they have been developed in close cooperation with the International Chamber of Commerce, which now recommends their use to corporations all over the globe.

As the futile efforts for a global privacy standard show, a homogenous regime for the self-governance of privacy is not in sight. While there is a global consensus on basic principles (more or less already based on the 1980 OECD guidelines), the instruments differ in scope, reach, precision, and enforcement mechanisms. But they are gradually making their way through the global network of private business governance structures, and they are becoming more and more interlinked with each other. More recently, they have also found their implementation in the form of technical codes.

Technical codes

The regulatory efforts for privacy protection of the 1970s were already attempts by the states to more or less directly regulate the technology. The first data-protection laws were a response to electronic data banks run by governments and large corporations (Mayer-Schönberger 1998). The computer was the problem, and the privacy laws of the first generation therefore aimed at the technical systems that stored and processed data. They set up registration or even licensing mechanisms for databases, they regulated access controls, and they were full of terms like “data”, “data file” or “data record”. In some countries like Sweden, the public oversight agency had the power to direct specific design changes for data banks, access controls, data transfers, and the like. When international harmonisation started in the Council of Europe, the OECD, and later the EU and transatlantic agreements, privacy governance instruments lost their technological focus and concentrated on the normative principles and institutional mechanisms. Only with the emergence of the Internet, the privacy implications of technological design gained wide attention again. In this case, though, the development towards privacy-friendly technologies did neither start among governments nor corporations, but because of user concerns and demands.

User self-help tools

The ubiquitisation of data processing converged with another development that had also started in the 1980s - the new legal and political concept of “informational self-determination” that the German constitutional court had developed in a landmark census ruling in 1983 (Bundesverfassungsgericht 1983). Contrary to the first generation of data protection laws that tried to regulate the corporations, the new laws and amendments, and the developing case law in the 1980s gave the citizens a say in the process. Their consent – at least in Europe – became a precondition for the use and processing of personal data. “Informational self-determination” also reached further than just the collection of the data and included the control of the individual over all later stages of the processing and use of the data (Mayer-Schönberger 1998).

This development got a new boost with the Internet. In the beginning cyberspace was seen as a great place for user empowerment. Until the mid-1990s, most of the netizens did not want a role of the government in the new final frontier land. John Perry Barlow’s “declaration of the independence of cyberspace” (Barlow 1996) is a famous example of the high expectations people had for the power of cyber self-regulation without government involvement. This “Californian Ideology” (Barbrook and Cameron 1995) was mirrored in the Clinton administration’s policy towards the new medium. A majority in Washington and elsewhere was strictly against disturbing the growth dynamic of the “new economy” by government interventions or regulations. “Government has largely taken a hands-off approach to the new economy”, as the report “State of the Internet” concluded even as late as 2000 (United States Internet Council 2000: 29).

The reaction in Europe was more sceptical, but also relied very much on the users. The Council of Europe issued a set of recommendations for privacy on the Internet in 1999, following up on its 1980 convention. The wording reads like a capitulation of state regulation:

> *“For Users: Remember that the Internet is not secure. However, different means exist and are being developed enabling you to improve the protection of your data. Therefore, use all available means to protect your data and communications.” (Council of Europe 1999)*

Technology has been – and for many still is – the best and only choice for users to ensure their privacy online. A number of privacy-enhancing end-user tools have developed in the last ten years. As personal computers became easier to use with graphical user interfaces like Windows, MacOS, and several Linux desktop managers, privacy-enhancing technologies were also developed from cryptic command-line tools into user-friendly packages. Because of the Internet, they are also accessible to anyone today. Many of them are available for free distribution, and some of them work directly online. The first wide-spread tool for encrypting data on personal computers was Phil Zim-

merman’s “Pretty Good Privacy” (PGP), which sparked a lot of attention and after a 6-years legal and political struggle in the U.S. in 1999 led to a liberalisation of export control restrictions on cryptography technology (Bendrath 2001).

The tools available nowadays include strong encryption software for data, emails, and web access; web anonymising proxies; tools that automatically delete cookies; anonymous re-mailers; blocking software for advertisement banners and pop-up windows; disposable email-addresses and even databases with fictional individual data sets to anonymously use websites that require registration; traffic scrambling networks; and furthermore.[16] They generally offer two kinds of privacy protection. Most of the encryption and traffic scrambling tools help their users hide data, internet traffic patterns, and the traffic’s content from prying eyes, be they law enforcement agencies or network providers. They therefore allow online interactions between trusted parties, be they friends, business partners, or political activists. The threat scenario for their users is still more or less based on the “Big Brother” image, and this has also become popular through movies such as “Enemy of the State” as through widely reported snooping activities by intelligence agencies like the NSA. The other group of privacy-enhancing tools is directed against corporate data collectors who track the visitors of their websites and online services. They include tools that allow deleting corporate tracing instruments like cookies and “web bugs” on the hard drives of the users computers’, as well as online services that provide disposable identities to anonymously access registration-based online services.

These privacy-enhancing tools give the users considerable protection. Many of them are still not widely used, but some functions like the automatic cookie-deletion have been included in newer versions of most web browsers and therefore have become mainstreamed into most computer desktops.

Negotiation-based codes

There is one problem that all these privacy-enhancing tools listed above cannot address: If the user is doing an online purchase, he or she has to enter the real name, credit card number and more information into a corporate website. In case the item bought is not a digital good like a music file, the company also needs the address and more information for the delivery. How can the users be sure this information is not being misused afterwards? This is where negotiation-based technical codes come into play, which act like an agent between the user and the companies. The user can use tools that automatically negotiate his privacy preferences with the website he or she visits. A well-known example for this is the P3P standard („Platform for Privacy Preferences Project“) for websites. It was developed by the World Wide Web Consortium (W3C) with the inclusion

[16] For an overview, see <http://www.epic.org/privacy/tools.html>.

of corporations, technology experts, and data protection commissioners (Cranor 2002). P3P presumes no set level of privacy protection, but enables the user to define his privacy “choices” for different types of websites. The concrete data transactions are then automatically negotiated between the user’s web browser and the company’s web server. The standard has been applauded by public data protection commissioners as a model for technological enforcement of privacy protection mandated by law. The European Commission is also following this approach. In 2003, it stated that technological measures “should be an integral part in any efforts to achieve a sufficient level of privacy protection.” (EU Commission 2003: 16)

On the other hand, privacy advocates have criticised P3P as just being an automation of the data collection that many websites do anyway. The standard development process for P3P even started under the name „Open Profiling Standard“ (Article 29 Working Party 1998). An assessment by the Electronic Privacy Information Centre mentioned the lack of enforcement options, because “P3P provides no means to ensure enforcement of the stated privacy policies” (EPIC 2000). About ten per cent of all major websites nowadays have some P3P functionality (Byers et al 2003), and most web browsers support P3P. Before the standard was adopted, the EU’s data protection commissioners had already asked that the default settings in the browsers should reflect the highest level of protection (Article 29 Working Party 1998). This was not the case, and with the Internet becoming a mass medium, the average user is even less familiar with these technological solutions or with how to set the personal privacy preferences in the browsers.

Privacy and identity infrastructures

These technological approaches are currently being developed into more comprehensive infrastructures under the label „Privacy and Identity Management” (PIM). They are expected to provide two features at the same time: A simple and user-friendly administration of his or her online identity, and a technological implementation of data protection standards. Most PIM concepts include some kind of single-sign on service that makes the handling of different logins and passwords for several websites and online services easier for its users.

It is not yet clear if in the end this will lead to better data protection or even to the end of anonymity on the net. Microsoft’s heavily criticised „Passport“ / „.Net“ programmes with central databases are regarded PIMs, as are decentralised online infrastructures that ensure far-reaching anonymity and pseudonymity (so-called “federated” PIMs). Sophisticated designs include public-key encryption schemes that would allow the individual to not only control the delivery of his or her personal data to corporations and other users, but the use of this data after it has been submitted (for an overview, see ICPP 2003). Complementary to the P3P front-end standard that allows the user to con-

trol which data he gives to websites, meta-data protocols are currently being developed to ensure that once personal data has entered the corporate data warehouses (back-end), its processing can only be done according to the preferences of the person it belongs to. The Enterprise Privacy Authorisation Language (EPAL), such a privacy meta-data standard, is already in use at companies like eBay. Like P3P, the EPAL standard was submitted for adoption to the World Wide Web Consortium, and like P3P, it has been developed by industry (IBM Laboratories Zürich) in cooperation with data protection commissioners (Borchers 2004).

Recently, a lively debate has started online and at a number of meetings and conferences about “user-centric identity management”. It has actively been driven by Microsoft’s privacy and identity staff, which - after the market failure of “Passport” – seems to have understood that a single customer database controlled by a monopoly-like corporation is neither what users are looking for, nor what companies want as an intermediary for their customer relations. The basic idea for the design of this new identity management architecture is the use of credentials. This would allow only transferring the minimal amount of personal data needed. To use an example from the streets again: If stopped by the police on a highway, drivers would only prove the fact that they have a driving license (legal driver credential), not their names, addresses or other personal information which is not relevant in that specific context. Most of the participants in these developments towards identity management are from large, U.S.-based information technology corporations, with a few academics and freelance consultants also taking part. Privacy advocates as well as public data protection commissioners are largely missing.[17]

The development of these infrastructural concepts is still in an early phase, and a broad user-base is still lacking. But if successful, the technical design of the systems will have a broad impact on how anonymously people can move on the Internet in the future. Thinking of the famous cartoon “on the Internet, nobody knows you’re a dog” (Steiner 1993), companies now might not always have to know that there is a dog, but would ask for the dog’s age, gender, credit card number, or other information depending on the service provided. The technical differences between the several emerging identity management standards can be overcome through interfaces and gateways, but the different levels of data protection incorporated within them are more difficult to harmonise (Farber 2003). Therefore, EPAL allows for the creation of templates through which the different legal data protection provisions in different countries can be implemented (Borchers 2004).

[17] A central hub for this development is a loose network called the “Identity Gang”, <http://www.identitygang.org>.

Comparison

Like in the realm of social codes for privacy self-governance, there is no single technical standard for privacy protection on a global scale. This is partly due to the different threats to privacy, which need different tools for protection. On the other hand, it also reflects the different interests and needs of corporate data processing and the respective policies and technical architectures. In the technical field, we can again observe a trade-off between the reach of the technical codes and the privacy protection they provide. But different from the social codes, the individuals do not necessarily depend on private corporations and their privacy codes of conduct. Instead, their level of control over their own data as well as the variety of tools available for protecting it varies with the architectural scope of the technical codes. For users who individually want to hide their data while surfing the web or sending emails, there is a whole range of tools available that allows for more or less perfect protection. Still, it depends on the computer literacy and the personal privacy preferences if and how intensively people use these tools, and many of them use different combinations of them.

For exchanging private information with other parties, there are still a number of different privacy tools available, but because of interoperability needs, there are only a few standards that are widely adopted. These also still have a growing user-base, because of the network effects: The more users a communications standard has, the more it will attract new users. This is especially true for tools that aim at protecting the communications privacy or at exchanging encrypted data between trusted parties. Pretty Good Privacy (PGP) has become the de-facto standard for private data security with this mechanism, with the OpenPGP standard having been submitted to the Internet Engineering Task Force (IETF 1998) and providing the basis for many other implementations (Bendrath 2001). Here, if the parties to a communication use the same standard, they can still be considerably sure that their personal information and communication is protected.

Internet users who have to give some personal data to website providers because of a business relationship can use the Platform for Privacy Preferences' web standard P3P to automatically negotiate their privacy preferences with the respective corporation. But user control has its limits here, because only a minority of websites support P3P, and even if they do, there are no technical measures available yet that let the individuals control what happens to their information once it has entered the corporate data warehouses. Comprehensive and strong user-centric privacy and identity management architectures are still under development, and technical back-office privacy standards like EPAL that limit data use within the corporate data warehouse only provide a generic framework. The level of privacy protection they implement depends on the social codes that apply to the respective company, be they self-governance codes of conduct or legal obligations. This lack of technically supported users' control over their personal data

once they have given it to private corporations, combined with ongoing compliance problems in the private sector and constant consumer mistrust into e-commerce, have fuelled new state-based regulation efforts in recent years.

COMPLIANCE PROBLEMS AND THE NEW ROLE OF THE STATE

Ongoing low compliance

In 1997, the OECD Committee for Information, Computer and Communications Policy conducted a survey of websites that openly questioned the effectiveness of any of the official mechanisms like the OECD privacy guidelines or national privacy legislation. The researchers found

> *“a marked discrepancy between the world of the various institutions and organisations that develop ideas and instruments for data protection on the one hand, and the world of Web sites on the other.“ (OECD 1998a: 23)*

Around the same time, some well-published cases of misuse of personal information by companies like online marketing giant DoubleClick, the steady rise of spam and junk mail, security holes in customer databases, and a growing fear of credit card data being stolen on the net (for an overview, see Junkbusters 2005) led to a public demand for more effective privacy protection online. The users, according to a number of other surveys, are not satisfied with the state of online data protection (for an overview: Bennett, 2004b). In March 2004, a EuroBarometer survey found that of the 84% of EU citizens who do not shop online, 25% of them do not trust the medium (EuroBarometer 2004).

This was noted by many. A number of governments and international organisations tried to work on online privacy under a general “trust” framework. Missing consumers’ trust in privacy and other rights on the web were and still are perceived as major problems that stand in the way of a large-scale breakthrough of e-Commerce. This was stated repeatedly from 1997 to 2003 in a number of national and international forums, from the White House to the EU, the OECD, and the World Summit on the Information Society.[18]

Two approaches can be distinguished that have become more popular in the last few years. States have been trying to directly or indirectly influence the development of technical codes for privacy protection, and they have started public auditing and certification programmes for social codes of privacy self-governance. The most recent devel-

[18] See e.g. the the EU Commission’s 1997 “European Initiative in Electronic Commerce” (EU Commission 1997), the White House’s 1997 “Framework For Global Electronic Commerce” (White House 1997), the OECD 1997 Turku conference on “Dismantling the Barriers to Global Electronic Commerce” (OECD 1998b), the OECD 1998 Ottawa ministerial conference on “Realising the Potential of Global Electronic Commerce” (OECD 1998c), the 2003 World Summit on the Information Society’s “Declaration of Principles” (WSIS 2003).

opment, adding to these two, is the return of the traditional state-centrist model of regulation: A public demand for legislation in the absence of meaningful private sector regulation can now be heard louder.

The state’s seal on social codes

The “adequacy” rating for the privacy protection level in third countries by the EU Commission in a way equals the job of rating agencies in the financial sector. Elsewhere in the data protection universe, states have also started to certify private instruments like privacy standards, organisational procedures, or private contractual arrangements. The Canadian „Model Code for the Protection of Personal Information“, for example, is a model in a twofold sense: A model for good privacy practices, and a model for the creeping-in of a more prominent role of the state. The code had been developed since 1992 by trade associations and consumer organisations together with the Canadian government and the Canadian Standards Association (CSA). It was officially recognised (“rated”) as a „National Standard of Canada“ in 1996. Organisations that voluntarily adopt the standard are then bound to mandatory quality controls by the CSA, comparable to the web privacy seals in the United States. The model code even served as the basis for comprehensive privacy legislation for the private sector – the 2001 Personal Information Protection and Electronic Documents Act (PIPEDA) (Bennett and Raab 2006: 162). Under PIPEDA, audits of corporate data handling in turn can be delegated from privacy commissioners to accounting firms or standards certification bodies (ibid: 138).

The 1995 EU directive also contains options for the certification of private self-governance instruments by public authorities. They had been conceived as exceptions that should be rarely used, but after the Safe Harbor breakthrough even the European data protection commissioners have actively supported and promoted them. The basic idea is to let business associations develop privacy codes of conduct, but to embed them in a legal framework and have them certified by public authorities. The data protection commissioners have a strong role here. Several adoptions of this certified self-regulation have been developed on the national level. Under the reformed German Federal Data Protection Law of 2001, trade associations can submit their codes of conduct to the data protection authorities, which check these against compliance with data protection law. These decisions are not binding, though, and therefore the individual data processors (corporations, website owners, other entities) can submit their individual products or privacy policies to an audit mechanism and thereby get an official certificate and a seal of approval. This is also regulated in the Data Protection Law and in the new Media-Services Treaty between the federal states of Germany (Berlin Data Protection Commissioner 2001; Rossnagel 2000). The German federal state of Schleswig-Holstein has been offering such an audit mechanism since the year 2001, with the Data Protec-

tion Commissioner’s independent centre as the official public certification authority. Interest among corporations for this official auditing is high, which shows a greater trust in the state’s legitimising function even in the private sector. Ironically, what is still missing is a federal law that regulates the exact auditing process, including certification and selection of the official experts supposed to do the auditing (Sietmann, 2004). A similar movement can be observed in Australia, where the standard principles have been incorporated into national law in 2001. The Privacy Act allows organisations and industries to have and to enforce their own privacy codes in order to allow for some flexibility of the application of the privacy law. The codes developed by the different industry associations then have to be certified by the national privacy commissioner (Australian Privacy Commissioner, 2005b).

Some public certification schemes even work with additional incentives. One method is minimising the risk of lawsuits. In the United States, the 1998 *Children’s Online Privacy Protection Act* also introduced the possibility of an official certification of private privacy programmes by the FTC. Companies which receive this certificate significantly reduce the risk of liability lawsuits in case problems still occur. Because it fits into the American model of privacy protection through the courts, it could become a model for other areas of privacy protection as well (Cranor/Reidenberg 2002: 19). It also goes along with the general trend among U.S. companies to focus on formalised compliance methods with legal obligations in order to minimise risks that has made some people speak about the emergence of an “audit society” (Power 2002). Another model is reducing the bureaucratic task of getting a new privacy certificate for each jurisdiction a company wants to do business in. The EU directive envisions consultations between privacy commissioners and business associations on the national level for country-wide codes of conduct, and an examination by the group of national commissioners (the “Article 29 Working Party”) for EU-wide regulation. The European Union has recently started using this model of regulated self-regulation in order to certify the global adherence of its data protection standards within multinational corporations. The procedure for this has already been harmonised among the EU data protection commissioners (Article 29 Working Party 2005), thereby providing a one-stop certification mechanism for the whole EU. In May 2005, DaimlerChrysler became the first corporation that was awarded a certificate which is valid in the whole EU for its global Privacy Code of Conduct from the French supervisory agency CNIL. Others like General Electric have been following them. The EU Commission, in its first report on the implementation of the 1995 Data Protection Directive in 2003, noted that “certification schemes play a crucial role“ (EU Commission 2003: 16).

The state's impact on technical codes

Some states have begun to mandate so called "privacy impact assessments" (PIAs) for government databases. The first country to make PIAs mandatory for federal agencies and departments in the early stages of system development was Canada (EU Commission, 2003: 16). In the United States, with the "E-Government Act" of 2002, every federal agency has to do a PIA before it can develop or introduce new information systems that use personally identifiable data. The PIAs have to be published, and oversight is provided by the Office of Management and Budget. The P3P standard for websites is also mandated by the abovementioned E-Government Act, as are privacy notices on all government websites. These privacy notices have to include: which information is collected, why it is collected, with whom the information is shared, which „notice“ is available to the individual, and how the information is secured (Privacy-Times, 2 December 2002). The U.S. government will certainly help to spread the broader use of P3P with the E-Government Act. Government *use* of these technological systems, standards and protocols of data protection is of course not regulation of the private sector, but it will help to spread adoption of them beyond the public sector. The large number of computers the government can leverage can create the critical mass for the widespread adoption through network externalities, and the use by public authorities also functions like a certificate of quality.

Another approach for government agencies is to actively participate in and support the development of privacy-enhancing technologies. As mentioned above, public data protection authorities and commissioners are regularly participating in industry expert groups that design technical codes for privacy protection like P3P and EPAL. The European Union has also funded a large part of the P3P development and has supported several privacy and identity management projects within its 6th framework research programme.[19] The German Federal Ministry of Economics has financed the GNU Privacy Guard – a free software implementation of the OpenPGP standard for encryption. Other governments have done extensive studies of privacy enhancing technologies to further the debate and the exchange of knowledge (see Borking/Hes 2000 as a prominent example).

In a few cases, state-based governance structures have intervened directly in the technological design of computer systems sold by private corporations. Microsoft's "Passport" programme is such an example of how the European Union now has an impact on global technical developments – and thereby on global data protection compliance. In its original architecture, Microsoft planned for the centralisation of all data col-

[19] PRIME (Privacy and Identity Management for Europe), FIDIS (Future of Identity in the Information Society), and RAPID (Roadmap for Advanced Research in Privacy and Identity Management).

lected from visitors to its affiliates' websites in order to provide authentication services for the latter. Microsoft, however, gave up this plan following privacy complaints from consumer groups and pressure from EU data protection commissioners. (EPIC 2004: 131) Another example is search engine giant Google's free email service "GMail", which automatically scans all mails of its users and then places context-sensitive advertisements within them. After strong protests from a number of privacy NGOs and an official complaint with several European data protection authorities by Privacy International, the EU group of data protection commissioners stated that Google's service might violate the European data protection directive (Links & Law 2004). Google had to ensure that mail scanning is only done by machines and after an explicit agreement by the users. While the EU data protection bodies only threatened to start legal action against Microsoft and Google in these cases, and later entered into discussions with the companies, the California State Senate even adopted a bill restricting Google's search and transfer abilities of GMail users' data (Hansen 2004).

The state, it seems, is again starting to focus on the technological design of the computer and the networks and relying less purely on the users' self-help or industry self-regulation. But instead of regulating individual data banks and data centres like in the 1970s, it is concentrating on technical infrastructures and standards that will have a widespread impact on the use of personal data.

The return of legal enforcement

The call for government regulation over private sector privacy policies and behaviour has been constantly growing in the past few years. Beth Givens, director of the privacy rights clearinghouse, concluded a comment on the 1999 Georgetown privacy survey with a recommendation that the Federal Trade Commission should "exert a stronger leadership role in evaluating the adequacy of privacy protection policies and practices in e-commerce" (Givens 1999). Even the FTC itself in its 2000 report on online profiling made a significant change. It now – to the surprise of many - said that legislation would be needed to complement industry initiatives like the standard proposed by the Network Advertising Alliance's (NAI) and others. The most important reason given was the defection problem still prevalent with most self-governance mechanisms.

> *"Self-regulation cannot address recalcitrant and bad actors, new entrants to the market, and drop-outs from the self-regulatory program. (...) Only legislation can guarantee that notice and choice are always provided in the place and at the time consumers need them." (FTC 2000)*

The FTC's call was a clear sign that the official "do self-regulation, or else we regulate you" approach, which had been a constant pattern in the U.S., is reaching its limits. The Bush administration has hesitated to adopt a comprehensive data protection law for the

private sector. Since the attacks of 2001 it is not known as a strong supporter of privacy protection in general, but Congress has seen a rising number of initiatives for data protection legislation since then (Smith 2006). Several U.S. states have already moved further and passed laws that protect data more comprehensively than current federal legislation.[20] In 2003, California passed the “Shine the Light” law which enables customers to find out how businesses sell their personal information. Since then, companies that do business with Californian residents have to either allow customers to opt out of information sharing, or in detail disclose to them how their personal information is shared with others. The bill was a landmark because it was one of the first legislative attempts in the U.S. to address “list brokerage,” the compilation and sale of individuals' personal information for marketing campaigns, including spamming, telemarketing, and junk mail. Before that, businesses did not have to inform customers and visitors of their information business activities, and many companies, both online and offline, sell their customer lists to list brokers (EPIC 2005a).

The persistence of consumer distrust in corporate privacy self-governance as well as the growing burden of having to comply with a number of different national and state-level privacy laws recently has led some large corporations in the information sector to rethink the need of state-based governance of privacy. In a widely perceived move, in November 2005 Microsoft called for a comprehensive privacy law in the United States (Smith 2005)[21]. The same call was repeated in June 2006 by an industry consortium including Microsoft, Oracle, Intel, Hewlett-Packard, Google and other big players in the information technology field (Consumer Privacy Legislative Forum 2006).

CONCLUSION: THE COMPLEX NETWORK OF PRIVACY GOVERNANCE

The role of the state in a different shape

We have seen that even in private sector self-regulation, there is a growing interest in getting the state “back in”, while on the other hand the failures of pure private sector regulation have created a rising public demand for more state control and enforcement. Be it public funding and promotion for privacy-enhancing technologies, government oversight over private seal mechanisms, officially certified auditing of privacy policies, or the recent U.S. developments in favour of private sector regulation mandated by law, the state is getting a more prominent role than it used to have – especially if we consider the “hands-off” approach towards the Internet that was prevalent ten years ago.

What is different, though, from the state-centric approach to privacy and data protection regulation of the first generations, is a more prominent role for intermediaries. The

[20] See <http://www.epic.org/privacy/consumer/states.html> for an older, but very comprehensive overview.

[21] The author is Senior Vice President, General Counsel and Corporate Secretary of Microsoft.

state does not regulate big databases and computer centres directly as in the 1970s and 1980s. This would be unfeasible at least since the rise of the Internet. Instead, the state is now trying to control or steer what the important agents set as standards and procedures. The public governance of privacy is not pursued directly anymore, but through private intermediaries (Perritt 1997). These are:

- trade associations that get their privacy codes of conduct sealed;
- technology companies like Microsoft who develop identity-management infrastructures;
- standards organisations like the World Wide Web Consortium (for the P3P web privacy standard);
- consortiums that develop new infrastructural designs under an explicit mandate of the state, like the EU's funding for the "Privacy and Identity" projects or the P3P development;
- organisations that develop model contracts for transborder data flows between private parties like the ICC.

This all is happening in the "shadow of the law" (in the United States) or even within a legal framework (in other OECD countries), and with an important part still being private sector self-governance. The agents and tools of data protection regulation are therefore diverse, with an again growing role for the state. The distributed nature of this new regulatory pattern shows the new role of the state, which is more an "enabler" than an "enforcer" and has to work with all kinds of other agents - sometimes cooperating, sometimes enforcing, and sometimes enabling. This convergence of the EU and U.S. patterns of privacy regulation (and with other regions following) is one striking result of the globalisation of personal data flows through the Internet. The states in general are not willing anymore to tolerate every use of personal data in the online environment. The growing problem of "spam" (unsolicited email) is adding to this. It has already been subject of UN discussions, and even under the lax CAN-SPAM act of 2003[22], there have been the first large court cases against spammers in the U.S.[23] The Safe Harbor agreement of 2000 embodies the paradigmatic convergence between the self-governance and law-based approaches. It is still based on public law and an intergovernmental agreement, but it leaves the certification and operation of privacy-governance to the private sector. It has also limited the scope of privacy adequacy ratings from

[22] The full title is „Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003", Public Law 108-187. Critics say the "CAN" refers not to canning the spam but allowing it, as only fraudulent emails and a lack of opt-out information is considered a breach of the law. See EPIC (2005b) for an overview.

[23] In April 2005, the first spammer was sentenced to nine years in prison; see *Der Spiegel*, 18 April 2005 at 73: 'Sie haben Post!'

whole countries to individual companies. By doing this, it allowed for a transnational trading up of protection levels with potentially global reach.

At first sight, this resembles the trading up effect of Californian rules for car emissions (Vogel 1995): If you are able to change the privacy policy of a big corporation in one jurisdiction, you will help spread this standard worldwide. There is certainly some truth in this, as the example of Microsoft's Passport project has shown. But car manufacturing is based on economies of scale. These are different in the computer world. It certainly makes sense to have *one* version of a new Microsoft operating system on global sale, but if you maintain only a few localised websites and your business model basically rests on one huge customer database, then it is much easier to re-programme it so you can distinguish between the use of personal data of EU and U.S. citizens. The external effects of specific privacy regulations are therefore much more effective if they explicitly focus on extraterritorial and third-party effects, as the 1995 EU directive did, and they are more effective if based on law rather than voluntary compliance.

The trading up-effect through transnational business networks is still in place, too. It works more through the interoperability of standards and the reduction in transaction costs they provide. These standards can be technical codes like P3P or social codes such as standard contract clauses or a privacy management standard. They will produce a learning effect (if I use this standard here, I know how to use it there), and they also produce a network effect (if everybody else uses this standard, it is much easier for me if I also use it). The critical mass to generate these network effects can be generated by a critical mass of state and corporate users, or by a critical mass of states that mandate the use of privacy codes for corporate users.

The role of social and technical codes

The distinct technical nature of the Internet allows for other means of regulating behaviour than social or legal norms and rules. *Lex Informatica*, the ex-ante enforcement of specific behaviour in online environments, can certainly be a strong regulator of citizens' and corporate use of personal data. The way websites and servers are programmed can force users to reveal their personal data or else be locked out of a service – or it can free them from these obligations. Political discussions of the technical design of new infrastructures have certainly become more popular in recent years, with data protection agencies and parliaments trying to enforce more user and customer-friendly systems design.

A growing nuisance for companies as well as privacy advocates has been that there is now a wide variety of national, sectoral and international privacy laws, codes, standards and commitments. Although they are more or less based on the same privacy principles, they have different levels of protection, different compliance and public oversight mechanisms, and different degrees of control by the users and customers over their data.

Because they work under conditions of global transnational communications, they cannot neatly be separated along territorial borders or industry sectors anymore. In a global cyberspace, where proximity and distance in the classical territorial sense have vanished, re-zoning the Internet into separate national or organisational sub-nets has so far not been possible, and it is certainly something most users, companies and developers would oppose anyway.[24] In a way, this is the return of the “conflict of law” problem, this time for transnational self-governance. Reidenberg’s (2000: 1358) hope that “multiple technical standards can coexist for information flows in cyberspace” - which would reflect the multiple regulatory approaches - has failed to materialise so far. Applying and translating the several national, international, and private sector privacy governance instruments into technical protocols that automatically manage compliance across different jurisdictions and organisations - and then even giving users some choice - has yet been too complex a task to find workable applications and convenient wide-spread use. We will therefore for some more time be witnessing a global privacy regime that is diverse, overlapping, and contradictory. Until truly global privacy norms and standards have emerged, the second-to-best model is therefore the “adequacy” rating method, which will increasingly be applied to social and technical codes alike.

The attempts of governments and the European Union to push technological regulation schemes can have a harmonising effect, and they might bring a wider use of privacy-enhancing technologies. As most of the developments described in this paper are very recent, it is too early to judge their effectiveness. Especially approaches like privacy impact assessments in the early stages of systems development or the EU’s research funding for privacy enhancing technologies will only play out in the mid-term. But their widespread adoption will only happen if there is a global agreement on the *content* of the technical rules, on the level of privacy protection that is wanted. The seed crystals for such a global privacy standard are slowly emerging as the result of regional mandatory laws like the EU data protection directive, their third-party effects which have a globalising impact, the development of privacy standards schemes and global sectoral codes of conduct, the political influence on the design of large technical infrastructures, and the private transnational contracts that reference standards and codes of conduct. Technical codes can help enforcement and are a new kind of binding regulation for computer-mediated social interaction spaces. But their widespread adoption still depends on a political consensus that defines the material content of the *Lex Infor-*

[24] This will only be possible if the underlying Internet addresses (IP numbers and domain names) are re-zoned according to national boundaries. Even for countries that have established border gateways for Internet traffic like the proverbial “Great Firewall of China”, circumvention has been a constant nuisance. For a different view, see Goldsmith/Wu (2006).

matica. Social codes in the end still reflect social values and norms, and as long as there are different opinions on them, we will not see globally harmonised privacy protection.

REFERENCES

Article 29 Working Party (1998) Opinion 1/98. Platform for Privacy Preferences (P3P) and the Open Profiling Standard (OPS) Document WP 11 (Brussels: EU Commission)

-- (2005) Working Document: Setting Forth a Co-Operation Procedure for Issuing Common Opinions on Adequate Safeguards Resulting From “Binding Corporate Rules” Document WP 107 (Brussels: EU Commission)

Australian Privacy Commissioner (2005) Privacy Codes <http://www.privacy.gov.au/ business/codes/index.html>

Baer, WS (1997) ‘Will the Global Information Infrastructure Need Transnational (or Any) Governance?’ in Kahin and Wilson (eds), National Information Infrastructure Initiatives: Visions and Policy Design (Cambridge/Ma.: MIT Press) at 532-552.

Bainbridge, D (1996) The EC Data Protection Directive (London: Butterworths)

Barbrook, R and Cameron, A (1995): The Californian ideology; different versions available at <http://www.hrc.wmin.ac.uk/theory-californianideology.html>

Barlow, J P (1996) A Declaration of the Independence of Cyberspace, Davos, Switzerland, 8 February 1996, <http://homes.eff.org/~barlow/Declaration-Final.html>

BBBOnline (2006) Consumer Privacy Website, <http://www.bbbonline.org/consumer/privindex.aspx>

Bendrath, R (2001) ‘PGP – die ersten zehn Jahre’ in Telepolis 19 March 2001 <http://www.heise.de/tp/deutsch/inhalt/te/7175/1.html>

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

-- (2004a) Privacy Self-Regulation in a Global Economy: A Race to the Top, the Bottom or Somewhere Else? in Webb (2001): Voluntary Codes, Private Governance, the Public Interest and Innovation 227-248 <http://www.carleton.ca/spa/VolCode/Ch8.pdf >

-- (2004b) Privacy in the Political System: Perspectives from Political Science and Economics <http://web.uvic.ca/~polisci/bennett/pdf/westinbook.pdf>

Bennett, C J and Raab, C D (2003) The Governance of Global Issues: Protecting Privacy in Personal Information paper presented at the ECPR Joint Sessions of Workshops Edinburgh, 28 March - 2 April 2003

-- (2006) The Governance of Privacy. Policy Instruments in Global Perspective (Cambridge/MA: MIT Press, 2nd and updated edition)

Berg, T (2000) ‘www.wildwest.gov: The Impact of the Internet on State Power to Enforce the Law’ in Brigham Young University Law Review 25 at 1305-1362.

Berlin Data Protection Commissioner (2001) Berliner Beauftragter für Datenschutz und Informationsfreiheit / Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein Neuregelungen im Bundesdatenschutzgesetz, Berlin

Bijker, W E (ed.) (1992) Shaping Technology, Building Society: Studies in Sociotechnical Change (Cambridge/MA: MIT Press)

Borchers, D (2004) ‘Eine Sprache für den Datenschutz’ in heise news 14 May 2004 <http://www.heise.de/newsticker/meldung/47361>

Borking, J and Hes, R (eds.) (2000) Privacy-Enhancing Technologies. The path to anonymity, revised edition (Den Haag: Registratiekamer)

Boutin, P (2002) Just How trusty is TRUSTe? Wired News 9 April 2002 <http://www.wired.com/news/exec/0,1370,51624,00.html>

Bundesverfassungsgericht (1983) BVerfGE 65, 1 – Volkszählung. Urteil des Ersten Senats vom 15. Dezember 1983 - 1 BvR 209, 269, 362, 420, 440, 484/83, <http://www.datenschutz-berlin.de/gesetze/sonstige/volksz.htm>

Byers, Simon and Cranor, Lorrie Faith and Kormann, David (2003) ‘Automated analysis of P3P-enabled Web sites’ in Proceedings of the 5th international conference on Electronic commerce (Pittsburgh: The Association for Computing Machinery) <http://doi.acm.org/10.1145/948005.948048>

Charlesworth, A (2000) ‘Clash of the Data Titans? US and EU Data Privacy Rules’ in European Public Law 6 at 253-274

Consumer Privacy Legislative Forum (2006) Statement of Support in Principle for Comprehensive Consumer Privacy Legislation 20 June 2006 <http://www.cdt.org/privacy/20060620cplstatement.pdf>

Council of Europe (1999) Recommendation No R(99)5 of the Committee of Ministers to Member States for the Protection of Privacy on the Internet. Guidelines for the Protection of Individuals with Regard to the Collection and Processing of Personal Data on Information Highways, adopted by the Committee of Ministers on 23 February 1999 at the 660th meeting of the Ministers' Deputies

Cranor, L F (2002) ‘The role of privacy advocates and data protection authorities in the design and deployment of the platform for privacy preferences’ in Association of Computing Machinery (ed.), Proceedings of the 12th Computers, Freedom and Privacy Conference, San Francisco/Cal. at 1-12

Cranor, L F and Reidenberg, J R (2002) Can user agents accurately represent privacy notices? paper for the Telecommunications Policy Regulation Conference 2002 <http://tprc.org/papers/2002/65/tprc 2002-useragents.PDF>

Der Spiegel, 18 April 2005 at 73: ‚Sie haben Post!’

DoC (2005) U.S: Department of Commerce Safe Harbor List <http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe+harbor+list>

Drake, W J (1993) ‘Territoriality and Intangibility’ in Nordenstreng and Schiller (eds) Beyond National Souvereignty: International Communications in the 1990s (Norwood/NJ.) at 259-313

Ellger, R (1996) ‘Vertragslösungen als Ersatz für ein angemessenes Schutzniveau bei Datenübermittlungen in Drittstaaten nach dem neuen Europäischen Datenschutzrecht’ in Rabels Zeitschrift für ausländisches und internationales Privatrecht 60 at 738-770

Engels, F (1978) ‘On Authority’ in Robert Tucker (ed), The Marx-Engels Reader ed. 2 (New York: W. W. Norton)

EPIC (2000) Electronic Privacy Information Center / Junkbusters: Pretty Poor Privacy: An Assessment of P3P and Internet Privacy, <http://www.epic.org/reports/prettypoorprivacy.html>

-- (2004) Electronic Privacy Information Center / Privacy International: Privacy & Human Rights 2004 An International Survey of Privacy Laws and Developments (Washington D.C.: EPIC)

-- (2005a) Electronic Privacy Information Center: California S.B. 27 "Shine the Light" Law <http://www.epic.org/privacy/profiling/sb27.html>

-- (2005b) Electronic Privacy Information Center: SPAM - Unsolicited Commercial E-Mail <http://www.epic.org/privacy/junk_mail/spam/>

EU (1994) Europe and the global information society. Recommendations to the European Council. Report of the High-Level Group on the Information Society 26 May 1994 <http://europa.eu.int/ISPO/infosoc/backg/bangeman.html>

-- (1995) Directive 95/46/EC of the European Parliament and of the Council, on the protection of individuals with regard to the processing of personal data and on the free movement of such data 24 October 1995

-- (1997) Directive 97/66/EC of the European Parliament and of the Council, concerning the processing of personal data and the protection of privacy in the telecommunications sector 15 December 1997

-- (2002) Directive 2002/58/EC of the European Parliament and of the Council, concerning the processing of personal data and the protection of privacy in the electronic communications sector 12 July 2002

EU Commission (1997) COM(97) 157: A European Initiative in Electronic Commerce. Communication to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions 15 April 1997

-- (2002) 2002/16/EC, Commission Decision on standard contractual clauses for the transfer of personal data to processors established in third countries, under Directive 95/46/EC, notified under document number C(2001) 4540 27 December 2001 with annex “Standard Contractual Clauses”

-- (2003) Report from the Commission. First report on the implementation of the Data Protection Directive (95/46/EC), COM (2003) 265 final 15 May 2003

EU-JRC (2003) European Union Joint Research Center: Security and Privacy for the Citizen in the Post-September 11 Digital Age: A Prospective Overview. Report to the European Parliament Committee on Citizens Freedoms and Rights, Justice and Home Affairs (LIBE)

EuroBarometer (2004) E-Commerce Survey March 2004 <http://europa.eu.int/comm/consumers/topics/btoc_ecomm.pdf>

European Parliament (1979) ‘Resolution on the protection of the rights of the individual in the face of technical developments in data processing’ in Official Journal of the European Communities, No. C 140/35 5 June 1979

Farber, D (2003) ‘Federated identity, PingID and standards cartels’ in ZDNet Tech Update 19 October 2003 <http://techupdate.zdnet.com/Federated_identity_PingID_standards_cartels.html>

Farrell, H (2002) ‘Hybrid Institutions and the Law: Outlaw Arrangements or Interface Solutions?’ in Zeitschrift für Rechtssoziologie 1 at 25-40.

-- (2003) ‘Constructing the International Foundations of E-Commerce: The EU-U.S. Safe Harbor Arrangement’ in International Organization 2 at 277-306

Fink, S (2002) Datenschutz zwischen Staat und Markt. Die „Safe Harbor“-Lösung als Ergebnis einer strategischen Interaktion zwischen der EU, den USA und der IT-Industrie Master Thesis Department of Political and Adminstrative Science, University of Konstanz November 2002 <http://www.ub.uni-konstanz.de/v13/volltexte/2003/1012//pdf/magarbsfink.pdf>

FTC (2000) U.S. Federal Trade Commission: Online Profiling. A Report to Congress, Part 2: Recommendations July 2000 (Washington, D.C.: Federal Trade Commission) <http://www.ftc.gov/os/2000/07/onlineprofiling.htm>

GBDe (2001) ‘Global Business Dialogue on electronic commerce’ Consumer Confidence: Trustmarks <http://www.gbd.org/pdf/recommendations/trustmark00.pdf>

Givens, B (1999) The Emperor's New Clothes: Privacy on the Internet in 1999 <http://www.privacyrights.org/ar/emperor.htm>

Goldsmith, J and Wu, T (2006) Who Controls the Internet? Illusions of a borderless world (New York: Oxford University Press)

Hansen, E (2004) ‘California Senate approves anti-Gmail bill’ in CNET News.com 27 May 2004 <http://news.com.com/2100-1028_3-5222062.html>

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

ICPP (2003) Independent Centre for Privacy Protection (ICPP) Schleswig-Holstein and Studio Notarile Genghini Identity Management Systems (IMS): Identification and Comparison Study for the EU Joint Research Centre Kiel <http://www.datenschutzzentrum.de/idmanage/study/ICPP_SNG_IMS-Study.pdf>

IETF (1998) Internet Engineering Task Force RFC 2440. OpenPGP Message Format <http://www.ietf.org/rfc/rfc2440.txt>

Junkbusters (2005) News and Opinion on Marketing and Privacy constantly updated <http://www.junkbusters.com/new.html>

Johnson D R, Crawford, S P, and Palfrey, J G jr. (2004) The Accountable Net: Peer Production of Internet Governance (Cambridge/Ma.: The Berkman Center for Internet & Society Research) <http://ssrn.com/abstract=529022>

Johnson, D R and Post, D G (1997) ‘The Rise of Law on the Global Network’ in Kahin and Nesson (eds), at 3-7

Kahin, B and Nesson, C (eds) (1997) Borders in Cyberspace. Information Policy and the Global Information Infrastructure (Cambridge/MA: The MIT Press)

Latour, B (1994) Der Berliner Schlüssel WZB Working Paper FS II 94-508 (Berlin: Wissenschaftszentrum Berlin für Sozialforschung)

Lessig, L (1999) Code and other Laws of Cyberspace (New York: Basic Books)

Links & Law (2004) Google's GMail - Privacy concerns <http://www.linksandlaw.com/gmail-google-privacy-concerns.htm>

Lyon, D (2001) Surveillance Society. Monitoring Everyday Life (Buckingham and Philadelphia: Open University Press)

Mayer-Schönberger, V (1998) ‘Generational Development of Data Protection in Europe’ in Agre, Philip E. and Rotenberg, Marc (eds), Technology and Privacy: The New Landscape (Cambridge/MA: MIT Press) at 219-241

-- (2003):‘The Shape of Governance: Analyzing the World of Internet Regulation’ in Virginia Journal of International Law 43 at 605-673

OECD (1980) Organisation for Economic Cooperation and Development Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, Adopted by the Council 23 September 1980

-- (1985) Declaration on Transborder Data Flows, Adopted by the Governments of OECD Member countries 11 April 1985

-- (1998a) Directorate for Science, Technology, and Industry, Committee for Information, Computer and Communications Policy, Group of Experts on Information Security and Privacy Practices to Implement the OECD Privacy Guidelines on Global Networks OECD Doc. No. DSTI/ICCP/REG (98)6/FINAL 23 December 1998

-- (1998b) Directorate for Science, Technology, and Industry, Committee for Information, Computer and Communications Policy “Dismantling the Barriers to Global Electronic Commerce”, An International Conference organized by the OECD and the Government of Finland in Cooperation with the European Commission, the Government of Japan and the Business and Industry Advisory Committee to the OECD, Turku, Finland, 19-21 November 1997, OECD Doc. No. DSTI/ICCP(98)13/FINAL 3 July 1998

-- (1998c) Directorate for Science, Technology, and Industry, Committee for Information, Computer and Communications Policy, Working Party on Information Security and Privacy Ministerial Declaration on the Protection of Privacy on Global Networks, Ottawa, 7-9 October 1998, OECD Doc. No. DSTI/ICCP/REG(98)10/FINAL published 18 December 1998

Perritt, H H (1997) ‘Jurisdiction in Cyberspace: The Role of Intermediaries’ in Kahin and Nesson (eds) at 164-202

Post, D G (1998) ‘The "Unsettled Paradox": The Internet, the State, and the Consent of the Governed’ in Indiana Journal of Global Legal Studies 5 at 521-539

Power, M (2002) The Audit Society. Rituals of Verification, 3rd edition (Oxford: Oxford University Press)

Privacy-Times, 2 December 2002

Privacymark.org (2006) References <http://privacymark.org/ref>

Reidenberg, J R (1998) ‘Lex Informatica: the Formulation of Information Policy Rules Through Technology’ in Texas Law Review 76 at 553-584

-- (1999) ‘The Globalization of Privacy Solutions. The Movement towards Obligatory Standards for Fair Information Practices’ in Bennett, C J and Grant, R (eds.)(1999) Visions of Privacy. Policy Choices for the Digital Age (Toronto: University of Toronto Press)

-- (2000) ‘Resolving Conflicting International Data Privacy Rules in Cyberspace’ in Stanford Law Review 52 at 1315-1371

Richardson, L (2000) ‘History of Self-Regulation Cast Doubt on its Effectiveness’ in Privacy Times 12 July 2000 at 7-11

Rosecrance, R (1996) ‘The Rise of the Virtual State’ in Foreign Affairs 4 at 45-61

Rossnagel, A (2000) Datenschutzaudit. Konzeption, Durchführung, gesetzliche Regelung (Braunschweig and Wiesbaden: Fr. Vieweg & Sohn)

Rössler, B (2001) Der Wert des Privaten (Frankfurt a.M.: Suhrkamp)

Schwarz, P M (2000) ‘Internet Privacy and the State’ in Connecticut Law Review 32 at 815-859

Schwarz, P M and Reidenberg, J R (1996) Data Privacy Law (Charlottesville/VA: Michie Law Publisher)

Seltzer, W and Anderson, M (2001) ‘The Dark Side of Numbers: The Role of Population Data Systems in Human Rights Abuses’ in Social Research 68 at 481-513

Shaffer, G (1999) ‘The Power of Collective Action: The Impact of EU Data Privacy Regulation on US Business Practice’ in European Law Journal 5 at 419-437

Sietmann, R (2004) ‘Bundestag will Datenschutzreform anmahnen’ in Heise News 1 December 2004 <http://www.heise.de/newsticker/meldung/53816>

Smith, B (2005) Protecting Consumers and the Marketplace: The Need for Federal Privacy Legislation (Redmond: Microsoft Corp.)

Smith, M S (2006) Internet Privacy: Overview and Legislation in the 109th Congress, 1st Session, CRS Report to Congress RL31408 (Washington D.C.: Congressional Research Service)

Steiner, P (1993) On the Internet, nobody knows you’re a Dog (Cartoon) in The New Yorker 61 5 July 1993 <http://www.cartoonbank.com/product_details.asp?sitetype=1&sid=22230003>

Swire, P P and Litan, R E (1998) None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive (Washington DC: Brookings Institution Press)

Teubner, G (2003) ‘Globale Zivilverfassungen: Alternativen zur staatszentrierten Verfassungstheorie‘ in Zeitschrift für ausländisches öffentliches Recht und Völkerrecht 63 at 1-28.

TRUSTe (2006) TRUSTe Fact Sheet <http://www.truste.org/about/fact_sheet.php>

U.S. DoC (1997) United States Department of Commerce: Privacy and Self-Regulation in the Information Age, <http://www.ntia.doc.gov/reports/privacy/privacy_rpt.htm>

-- (2005) United States Department of Commerce: Safe Harbor Overview <http://www.export.gov/safeharbor/sh_overview.htm>

-- (2006) United States Department of Commerce: Safe Harbor List <http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe+harbor+list>

United States Internet Council (2000) State of the Internet 2000 (Washington D.C.: U.S. Internet Council)

Vogel, D (1995) Trading Up. Consumer and Environmental Regulation in a Global Economy (Cambridge/MA: Harvard University Press)

Warren, S and Brandeis, L (1890) ‘The Right to Privacy’ in Harvard Law Review 4 193-220

Weichert, T (2000) ‘Zur Ökonomisierung des Rechts auf informationelle Selbstbestimmung’ in Bäumler, Helmut (ed), E-Privacy. Datenschutz im Internet (Braunschweig and Wiesbaden: Vieweg) at 158-184

White House (1997) A Framework For Global Electronic Commerce 1 July 1997

Winner, L (1986a) The Whale and the Reactor. A Search for Limits in an Age of High Technology (Chicago: University of Chicago Press)

Winner, L (1986b) ‘Do artifacts have politics?’ in Winner (1986a) at 19-39

WSIS (2003) World Summit on the Information Society: Declaration of Principles. Building the Information Society: a global challenge in the new Millennium, Geneva, 12 December 2003 <http://www.itu.int/wsis/docs/geneva/official/dop.html>

WTO (1994) General Agreement on Trade in Services (GATS), Geneva 15 April 1994

BIOGRAPHICAL NOTE

Ralf Bendrath is a researcher at the Collaborative Research Center “Transformations of the State”, University of Bremen. His blog on privacy theory and developments can be found at http://bendrath.blogspot.com.

Telephone: +49 421 218 8735
Fax: +49 421 218-8721
E-Mail: ralf.bendrath@sfb597.uni-bremen.de
Address: University of Bremen, Collaborative Research Center „Transformations of the State“, Linzer Strasse 9a, D 28359 Bremen