Part III

Consumer based Self-Regulation and the Law

7

The Social and Technical Self-Governance of Privacy

RALF BENDRATH

I. PRIVACY AND REGULATION IN A GLOBAL CYBERSPACE[1]

A. The Internet as a Case of Global Governance

PRIVACY PROTECTION IS a policy field with growing importance in the information society. Although its foundations date back to early liberal philosophy, which drew a clear border between the public and private spheres of a citizen's life,[2] it has only been the subject of intentional political regulation since the second half of the 20th century. This development was closely connected to the rise in computer use. The first generations of privacy and data protection laws, 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 situation drastically. Since then, self-regulatory approaches, like codes of conduct, contracts, standards, and technical means, have become more widespread. More and more personal data can be collected, processed, and transferred online. Therefore, the internet empirically is a good case to explore 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

[1] Research for this chapter was conducted in the project 'Regulation and Legitimacy on the Internet' at the Collaborative Research Centre 'Transformations of the State', Bremen University. I thank my colleagues Jeanette Hofmann, Volker Leib, Peter Mayer, Johannes Moes, Gregor Walter, and Michael Zürn for ideas and comments on the privacy case study and on earlier papers. Thanks also go to Olaf Dilling, Martin Herberg, and to two anonymous reviewers at the centre 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.

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 control. Certainly, 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. However, normal usage is not affected by this, as routing and packet switching take place in a decentralised way.

Because the internet crosses and, to some extent, ignores national borders, it undermines 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 'non-governmental 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 no longer based primarily on territorial space. This debate did not end with the bursting 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 *et al*, 2004), or the emergence of 'global civil constitutions' in cyberspace (Teubner, 2003).

No academic discussion, let alone any political vision, comes without sceptics. Already, in the initial stages of this debate, they raised their voices against the 'cyber-separatists' (for an overview of the debate, see Mayer-Schönberger, 2003). 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 and Cameron, 1995). There are two groups of scholars that still believe in a role for 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 may be more difficult, but not impossible (for a recent empirical account in this perspective see Goldsmith and Wu, 2006). The 'internationalists' are more concerned with the non-Cartesian characteristics of cyberspace, where physical distance is compressed to the question of how many hyperlinks apart two websites are, 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 a necessity 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).

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 equivalent of 'internet traditionalism' is 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.

B. 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 any more. 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 road traffic 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 kids 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 mostly it works through a legal sanctioning mechanism: the speeding ticket. If the risk—calculated from the cost of the penalty and the chances of being caught—is high enough, many drivers will refrain 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 to speed, even under legal rules.

It is different when physical or architectural constraints are involved. Imagine a street in a residential neighbourhood where the speed limit has been set to 30 kilometres per hour, but where many drivers still rush through it. This is often the case where the street is straight, paved, and has few crossroads or traffic lights. In many instances, communities that do not wish to bother with the high transactional costs of speed cameras rely on a different mechanism. They set up speed humps. These make the drivers slow down automatically, because they do not want to damage their cars' suspension, or they are afraid of losing control of the car in speeding over the humps. To most drivers, it is plainly impossible to speed over speed humps. The physical characteristics of a street—its architecture—have a huge impact on the drivers' behaviour. This does not operate through social norms and the risk of ex post sanctions, but through the architecture and ex ante enforcement. Still, in the offline world, speed humps can be ignored to some extent by acquiring very good suspension, huge tyres, or—as an extreme example—a tank. Street traffic is based on physics, and the limitations built into the infrastructure can be overcome 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 locks for backyard doors (Latour, 1994) can determine how people 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 any 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 and/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, many more constraints are possible through programming the servers, switches, and routers through which the data packets flow. A street that automatically slows down every car headed towards a particular location is unthinkable, but in cyberspace, this is reality. In Germany, the internet service provider Tiscali for example, automatically slows down all traffic from its broadband customers that comes from specific ports of their computers, namely the ports used for peer-to-peer file-sharing. There are many more examples of this, from Chinese automated content filtering to the technical blocking of specific forms of internet usage at the workplace through companies' firewalls. The Chinese government can enact a law prohibiting visits to critical websites (and has done so in the past), and companies can establish social rules that discourage their employees from using instant messaging services in the office (as many have also done). 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 also is a social space that enables, facilitates, and shapes online interactions between individuals and groups. Because all of these interactions are taking place in a technically mediated environment, the range of freedom and individual options for behaviour are also being 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,[3] but where the latter can still go on strike and leave the factory. In cyberspace, you can not leave the data 'machines' constituted by the operating systems and network protocols. It was 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 so the underlying hard-wired code in the hardware) and the networking protocols can be compared to the constitution. They provide the foundation on which other applications run, and they determine what options for user control (for example different user account settings in multi-user operating systems like Windows XP or Unix) and identification (eg dynamically or statically assigned Internet Protocol 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 in this level (and can change some settings, such as cookie policies), the design of web servers, websites, and the underlying databases is dependent on the choice of the corporation running it.

Software code does not of course work in a vacuum. Naturally, social and community norms also exist on the internet with regard to how to and how not to behave in different contexts (so-called 'netiquette'). But even some codes can still be influenced by the user, depending on the degree of access he has to the computer controlling his online behaviour. If a website filter for indecent content is running on my own 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 service provider (ISP), I would have to change ISP. If it is run by a national exchange point or international gateway, there is normally not much I can do personally. 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 lawmakers 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

[3] '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 in Winner, 1986b).

would do in the real world. If you want to read the *New York Times* (NYT) online, for example, you can only do so after registering with their customer database and giving away information about your address, age, job, and more. The NYT web server then can follow your 'click-stream', that is, the way you move around on the site, which articles you read, which advertisements you click on, 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. Online privacy, as now should be clear, is heavily dependent 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 emerged with the broader use of computers in the 1960s. As technology continues to change, so have the forms of data protection regulation. Data protection norms also have made an impact on the design of the technological architectures.

Self-governance structures in the privacy field have not emerged in isolation. They often have often come as a reaction to consumer demands, pressure from public interest groups, and from 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 take 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 developing since the 1990s. There are now a number of different social and technical codes in the private sector, with varying degrees of scope, reach, enforcement, and control over the data by customers and companies. Self-governance is surely growing in importance within the privacy field, and some of its forms can be seen as private equivalents of legal regulation. But the story does not end here. Self-governance mechanisms of privacy protection have again recently become the subject of closer inspection by governments and other public bodies. As we will see, the state is coming back—but in a different shape. The new privacy governance pattern no longer has the state as its hierarchical enforcer, but rather a *primus inter pares* that still holds some carrot-and-stick-capacity. Indirect regulation through intermediaries and the use of network effects seem to be a more successful way of establishing the wider use and application of privacy standards in the private sector. In addition, the use of technical codes is becoming more popular, but their success is still dependent on the social codes and underlying norms which they are supposed to reflect.

II. SETTING THE STAGE: STATE-BASED PRIVACY GOVERNANCE

A. 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) contains a paragraph on privacy. The 1950 European Convention on the Protection of Human Rights and Fundamental Freedoms includes a similar clause. The United States has had a judicial tradition of privacy protection since the 1890 seminal article by Samuel Warren and later Supreme Court judge Louis Brandeis, who coined the phrase, the 'right to be let alone' (Warren and Brandeis, 1890).

These early privacy rules were originally intended as a protection against unreasonable police searches of private property and an overly intrusive press. As a result of World War II and experiences with the Nazi regime,[4] people became more afraid of leaving too much personal information in the hands of powerful government bureaucracies. The use of computers in 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' or 'fair information practices' (the US version) and 'data protection' (in Europe) (Schwarz and Reidenberg, 1996). The discussion on the 'Big Brother state' was also growing.[5] Thus began parliaments' first efforts in drafting 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 suit. A bit later, West Germany at the federal level (1977), Denmark, Austria, France, Norway and Luxembourg (all 1978) also introduced privacy protection laws. Up to 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 United States, Germany, Sweden and the United Kingdom from 1960 to 1980, see

[4] 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 of all occupied countries in Western Europe. See Seltzer and Anderson (2001).

[5] Lyon (2001) has elaborated the thesis that 'privacy' only became a social value when the technologically enabled surveillance society was already a fact.

Bennett, 1992). By the 1990s, 22 more states from all continents had joined the throng, followed by a smaller number into the new millennium. The reasons for this general spread of privacy legislation are not the topic of this chapter.[6] We can keep in mind that there were several 'waves' or 'generations' of data protection legislation (Mayer-Schönberger, 1998).

Technical systems at the time were envisioned as centralised large computer facilities that would be easy to control and supervise, and where the data, once entered, would remain.

> In other words, there were huge cabinets full of digitised data where before there had been huge cabinets full of files, but still, they were huge cabinets. (Fink, 2002: 85, my translation)

By the 1980s, the picture had already begun to significantly change. The globalisation of the economy had 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 became more widely available than before, also became a valuable commodity (Weichert, 2000). As early as 1970, an expert group in the Council of Europe identified the transnational character of the computer and the according need for international regulatory harmonisation (Bennett, 1992: 134). Due to the fact that various national data protection laws often contain differing procedural regulations with regard to transnational data transfers, difficult legal conflicts still arose, even though they rested on the same basic set of principles (EU JRC, 2003: 90). In the late 1970s, the Council of Europe and the European Parliament began discussions on how to remove these trade barriers whilst 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).

During the following years, several international treaties and documents were developed in an attempt 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 (or incorporate) its rules into national law. Citizens of one country party to the treaty now had the right to legally fight any misuse of their personal data in another country that had ratified the treaty. The Convention included regulations on transborder data flows and also allowed restrictions in cases where the data was to be transferred to a country with lower protection levels. This

[6] 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).

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 which had not signed the treaty. This remained a matter of national legislation. The Council of Europe subsequently adopted a number of recommendations for implementing the Convention in specific areas that ranged from medical databases (1981) to privacy protection on the internet (1999) (EU JRC, 2003: 120).

In order to avoid further complications, the OECD developed its 1980 Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (OECD, 1980) in close coordination with the Council of Europe. Unlike the Council of Europe's 1981 Convention, the guidelines are not binding, 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 that behind it was an attempt to globalise the dominance of the US computer industry with the buzz phrase 'free flow of information'. The United States in turn accused the Europeans of protectionism by means of data protection (Bennett, 1992: 136*f*). 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).

The OECD for a decade was the only supra-regional international organisation that dealt with privacy and data protection. It was only in 1990 that the UN General Assembly adopted the, also voluntary, Guidelines concerning computerised data files, which had no follow-up mechanism and therefore no real impact.

The European Parliament, as mentioned above, had adopted several resolutions on data protection since 1976 and urged the EC Commission to draft an EC Directive for the harmonisation of national legislation. The Commission was rather hesitant and until 1982 requested only that Member States join the Council of Europe Convention (Bainbridge, 1996: 22). Not until 1990, with the European common market fast approaching, did the Commission react by presenting a draft European data protection Directive. 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. It referred to Article 100a of the EC Treaty and presented its move as necessary for the functioning of the European common market. It took five more years of negotiations in Brussels and the Bangemann report, *Europe and the global information society* (EU, 1994) that made the common European information space its utmost priority, before the Directive was enacted as Directive 95/46/EC (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 regulations on the private and public sectors' use of personal data, applies to manual and automated data processing, has detailed rules on implementation and mandatory data protection commissioners, and creates a coordination body at 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 has since 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, 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 supervisory 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 executive 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 is 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 although it is a binding international treaty, it provides only a basic set of fundamental data protection principles. It is less precise in giving institutional directions to its parties, having created no day-to-day supervisory body, instead relying 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. However, 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 regulations are therefore the strongest at the national level within the EU, weakening in concentric circles that are constituted by the EU, the OECD, and the United Nations.

B. The Internet, Safe Harbour, and the Rise of Self-governance

Thirty years after the first generation of data protection laws were enacted, the technological developments turned out less like 'Big Brother' and more as 'Little Sisters'. Centralised control by hierarchically structured, but territorially bound bureaucracies no longer seemed to be the main problem. The European model of registering and overseeing a few large databases hosted in large computer facilities was already reaching its limits in the late 1970s, spurred on by 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 put beyond reach of effective government supervision. After the advent of the internet as a mass medium in the 1990s, this problem became even worse, as the trade and flow of personal data across borders now took only a matter of seconds. The big corporations were still easy to control, but they also had the resources to fight encroaching 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, however, is that the mice—the small companies that can easily relocate—are hard to control and 'breed annoyingly quickly' (Swire and Litan, 1998: 201). Data protection, therefore, could only work if government supervision was combined with functioning self-regulation in the private sector. This has been the US approach since the enactment of their first Privacy Act controlling government use of data in 1974. The EU Directive also reflected this approach, because it discontinued the mandatory registration of databases with the data protection supervisory authorities. Companies can instead now appoint internal data protection commissioners (or even outsource this job to specialised service providers) and thereby comply with the directive and the relevant national laws.

The driving force behind the move towards a more self-regulatory approach in data protection therefore was a change in the structure of the regulated problem. If everybody becomes a potential user and collector of personal data, then top-down enforcement and central supervisory mechanisms do not work any more—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 European governments and the US government.

The conflict between American ‘free flow of information’ and European ‘privacy’ was barely covered in the guidelines. On one hand, the guidelines are completely voluntary by nature, which was desired by the United States, but on the other hand, at least they have set some lowest common denominator for fair information principles and therefore met the interests of the Europeans.

In 1995, the problem became more apparent following the enactment of the EU directive. For the first time, the directive as an international instrument harmonised and regulated data transfers to third party countries. This feature made its impact felt far beyond the European Union, and that 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’ present in the recipient country. If there is no comparable legislation in place, the companies wanting to export the data can only do so if it 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). In addition, the EU later developed 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 was no comprehensive data protection legislation for the private sector in the United States, but binding third party data export rules in the EU, there existed a dilemma: Either the EU Commission could have treated the US data protection regulation as ‘not adequate’ and risked another transatlantic trade war, or it could have turned a blind eye on the United States and heavily damaged the credibility of the whole directive. Even before the transatlantic conflict was resolved, the EU Directive helped create pressure on the United States to raise its level of data protection for the private sector. The Clinton administration was afraid that the EU Commission could lock US companies out of the large European market for e-commerce, because the lack of comprehensive data protection legislation in the United States could mean an ‘inadequacy’ rating. Before the Directive had to be implemented at national level in 1998, the US government therefore tried to convince the EU that self-regulation worked (for example 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. As a result, the self-regulatory instruments have been referred to as ‘the Directive’s bastard offshoots’ (Shaffer, 1999: 433). The international trade regulation provided some unexpected assistance with regard to this matter. The World Trade Organization’s 1994 General Agreement on Trade in Services (GATS) makes reference to privacy, not so much as an obstacle to trade, but as an exception from otherwise liberalised trade in services, including data services (WTO, 1994).[7] By doing this, trade liberalisation not only curbed the need for the United States to raise its level of privacy protection, but limited its ability to retaliate (Shaffer, 2000: 86).

After long negotiations, the EU Commission and the US Department of Commerce sealed a 'Safe Harbour' agreement in July 2000 (Fink, 2002; Farrell, 2003; Heisenberg, 2005). It has been described as a 'hybrid' or 'interface solution' (Farrell, 2002), as it links two different regulatory approaches: the European, law-based and comprehensive privacy regulation; and the American, private sector-based and sectoral privacy regulation. Under the Safe Harbour agreement, the object of the Commission's important adequacy rating is no longer a country, but a single company. Therefore, the United States could keep its data processing industry partly unregulated, and the EU could allow data transfers to US companies under the condition they subjected themselves to the Safe Harbour 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. (US DoC, 2005)

As of January 2008, 1,353 companies had entered the Safe Harbour (US DoC, 2008). The agreement is—as is natural for a compromise—weaker than the EU regulation. There is no possibility for EU citizens to legally insist on being given information about what is happening to their data in the United States, or for European data protection commissioners to inspect the processing companies on the other side of the Atlantic. The European Parliament strongly resisted the agreement, but as judgment on 'adequacy', in accordance with the 1995 Directive, is delegated to the Commission, could do little against it. But the agreement still involves some public supervision and enforcement as it utilises a general clause in US trade regulation. Companies that have joined Safe Harbour and are caught red-handed can be fined by the Federal Trade Commission for 'unfair and deceptive trade practices'. There is also an arbitration procedure for cases of complaint, where the arbitrator can be chosen from either private providers like TRUSTe or public authorities like the EU data protection commissioners (US DoC, 2005).

The regulatory regime of Safe Harbour therefore consists of several layers. The EU sets the substantive data protection standards, the companies

[7] '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, Art XIV).

voluntarily commit to them, private or public bodies provide arbitration services, public enforcement is carried out by a US agency, and the EU Commission still has the last word and can terminate the whole agreement if compliance or public supervision in the US is not working. It can therefore be described as a hybrid arrangement that combines transnational self-regulation on the one hand, and nation-state-based intergovernmental public regulation on the other hand, to produce a complex, multi-layered regime.

III. SELF-GOVERNANCE INSTRUMENTS OF PRIVACY PROTECTION

In the Safe Harbour regime, the private sector has a much more important role than in the traditional European regulation model, which is predominantly based on public supervision and inspection bodies. Under Safe Harbour, most of the regulatory functions, as well as the day-to-day supervision, are carried out by the private sector itself. States only set the minimum data protection level, but may employ means of last resort in cases of serious non-compliance. In this regard, the process leading up to the agreement 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 section, I will give an overview of the different instruments available today. As we will discover, they still differ greatly in terms of precision, reach, scope, and enforcement mechanisms.

A. Social Codes

1. *Internal Corporate Rules*

The simplest form of self-regulation is where a company publicly declares its adherence 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.[8] 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

[8] See http://www.oecd.org/sti/privacygenerator.

are more a reaction to bad publicity or 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 statements into clear guidelines for their employees—so-called 'organisational codes'. Early examples of these were developed by multinational companies such as American Express and Readers' Digest, some of which 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 worldwide subsidiaries, regardless of whether their country of residence has privacy legislation in place or not. Prominent examples are DaimlerChrysler, General Electric, and Siemens. They have come closest to inventing a new form of internal corporate private laws for data protection.

Many companies have also now established internal supervision mechanisms for ensuring compliance with 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 supervisory bodies if they appoint an independent corporate data protection commissioner. This model has been incorporated into Directive 95/46/EC (recital 49) and since then has been widely adopted all over the corporate world. These 'chief privacy officers', as they are mostly called now, are organised in transnational professional bodies like the International Association of Privacy Professionals (IAPP), and they regularly meet with the public privacy commissioners.

2. *Codes of Conduct for Business Associations*

More widely encompassing are the codes that have been developed for whole industry sectors ('sectoral codes': Bennett and Raab, 2006: 155–57). Found mainly in the United States, a number of codes of conduct are now available from different industry and trade associations, 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 is 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 are TRUSTe and Better Business Bureau (BBB) OnLine. Enforcement in general is not very strict, but industry associations play an increasing role in educating their members about privacy best practices. The inherent problem is that the certification providers are dependent on funding from their members or customers, so it is extremely unlikely that tough measures will be taken against those who break the rules. TRUSTe, for example, was placed under public pressure after it failed to adequately address accusations made against one of its members, Microsoft (Richardson, 2000; Boutin, 2002). A 1999 study, carried out by Forrester Research, concluded that privacy seal providers had become more of an advocate for the industry than for the consumer (EPIC and Privacy International, 2004: 110). On the other hand, industry associations are playing an increasing role in educating their members about privacy best practices, through specialised seminars, training services, and newsletters. This form of self-regulation more closely resembles the ‘managed compliance’ approach 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 its 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 at a later stage. Even more stringent is a programme called WebTrust, developed jointly by the US 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 with these self-regulatory mechanisms lie elsewhere. First, they only certify adherence to a minimal set of fair information practice principles. These are often less supportive of privacy than comparable EU legislation, for example with opt-out instead of opt-in mechanisms for commercial marketing as the norm. That is, unless the customer objects, his data will be used for marketing purposes. Second, these voluntary agreements have a relatively low level of participation and naturally can only regulate the behaviour of companies that subscribe to them. In January 2008, only 724 websites participated in the BBBOnLine privacy programme (BBBOnLine, 2008), and 2,490 sites had been certified by a TRUSTe seal (TRUSTe, 2008).

Mandatory membership of 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, which have a direct influence on their individual members, but not on companies. Well-known examples are the age-old codes for physicians and lawyers, who are bound to professional discretion in their relationships with their patients or clients. As membership of professional organisations such as medical associations or the Bar is made mandatory in order to practise in that respective profession, misconduct can potentially lead to exclusion and loss of professional licence.

Today, codes of conduct are a standard instrument of privacy governance and their mechanisms for compliance and certification have become stronger. Most of them have emerged in the United States, as their prime users are US 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's 'Global Code of Conduct'. Other global efforts in this direction have begun in the International Air Traffic Association (IATA) and the Federations of Direct Marketeers (Bennett and Raab, 2006: 156). Typically, these transnational codes of conduct have been developed in close connection with the international community of data protection commissioners, some even involving the active participation of privacy advocacy groups. TRUSTe was actually founded by a joint effort of the Boston Consulting Group and the Californian NGO Electronic Frontier Foundation (EFF). But this is not a typical example, as cooperation between corporate entities, NGOs, and public commissioners is normally much less institutionalised and less formalised. Instead of the highly formalised 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 comprising public commissioners, privacy advocates, and corporate chief privacy or chief technology officers.

3. *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 that hold large amounts of personal data about customers and employees and contract out (or outsource) some of the related work. The business agreement then has sections that regulate how the contractor may use the data, who holds property rights to it, if and how it can be transferred to third parties, and so on. Specific privacy contracts have been used since the late 1970s to allow transborder data flows under national data protection laws. In France, the use of private contracts has been quite popular since the early days of data protection regulation, but other European states have also relied on contracts to ensure that personal data exported to other countries is handled according to the legislation in force in the country of origin. The national data protection authorities have played a crucial role in pushing for the use of this private-law instrument (Ellger, 1996).

By as early as 1992, the Council of Europe had developed a template contract for transborder data flows with the cooperation of the EU Commission and the International Chamber of Commerce. Other groups, such as the 'Düsseldorfer Kreis' of German data protection commissioners, have also been active in this area (Ellger, 1996). The EU followed after 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 since.

There are several limitations to this approach. First of all, what consequences arise from the fact that the affected party—the citizen, customer, or user—is not subject (or privy) to the contract? This may not be a problem in the continental European tradition, but the Anglo-Saxon *common law* countries traditionally do not recognise the concept of third parties' rights derived from a contract between two other parties. However, the United States has given up the strict use of the privity of contract doctrine and now allows third party beneficiaries from private contracts (Ellger, 1996: 765). The legal enforcement of these contract clauses is still difficult. Enforcement of contract clauses depends not only on the jurisdiction chosen as the basis, but also on the national laws in the import country and on the interests of the receiving party. Specific laws (for example for intelligence agencies) may override strong protections in private contracts.

On the other hand, these contracts are also used to raise the data protection level within a country. If organisations, either voluntarily or due to public pressure, want to mandate high data protection standards for their contractors, they can insist on incorporating standard data protection clauses into their business agreement. 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 in extending the EU's data protection standards to countries where national legislation is lacking or not deemed adequate. Thus, the use of EU data protection standards is slowly being incorporated into private sector data usage all over the world. This demonstrates how private law can help to spread a regional legal standard through the use of mandatory data export control clauses (Reidenberg, 1999).

4. *Harmonisation by Standardisation Organisations*

Privacy standards go further than commitments to voluntary codes of conduct, because they simultaneously provide a set of objective criteria and 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 within an organisation. There has been some discussion going on about general privacy standards, based on the generic quality management standards of the ISO 9000 series. Standards normally also have strict supervision 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 was developed in 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 also reflected 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 adopted the standard were then bound to mandatory quality controls by the CSA. Similar standards to the Canadian Model Code have been developed elsewhere. In 1999, the Japanese Standards Association published the standard JIS Q 15001 ('Requirements for Compliance Program on Personal Information Protection'), which is modelled in detail on the structure of the environmental management standard ISO 14001 (Bennett, 2004a: 234). JIS Q 15001 was developed from a government-issued norm, the 1997 Data Protection Guidelines from the Ministry of International Trade and Industry (MITI) (Privacymark.org, 2006). In 1998, the Australian Privacy Commissioner published National Privacy Principles that also resemble the Canadian model (Bennett, 2004a: 234).

At the international level, the Council of the International Standards Organisation (ISO) initiated a process for the development of an international privacy standard in 1996, as a result of pressure from ISO's Consumer Policy Committee (Bennett, 2004a: 236). Because of heavy lobbying from US corporations and critique from European data protection commissioners, ISO has not been able to agree on a standard as yet. A more modest approach to '"set a common privacy terminology, define privacy principles when processing PI information, categorize privacy features and relate all described privacy aspects to existing security guidelines"' was started within ISO in 2006 under the leadership of the German standards institute, DIN (ISO/IEC, 2006). 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. (CEN, 2002)

5. *Comparison*

Compared against each other, the mechanisms analysed above reflect different characteristics with respect to their level of protection and reach. While privacy requirements of national standardisation organisations have been successful in a number of cases, an agreement on a global privacy standard has proven to be extremely difficult. At the other extreme, 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. Other codes of conduct with institutionalised compliance mechanisms are somewhere in the middle. Theoretically, they apply to a large number of corporations across the globe, but, in practice, these corporations still must subscribe to them (and pay for them) individually. Contractual solutions only apply to those 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 pretty loose, and it does not have the broad trickle-down effect that can be seen in the product standards of 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, as customer confidence in the secrecy of their information is at the core of the business model. On top of this, non-compliance may also lead to losing the licence required to further practise in that profession.

This resembles what we have discovered above in regards to state-based privacy regulation efforts. There is a trade-off between reach on the one hand, and obligation, precision, and enforcement on the other. At first glance, the same pattern seems to apply to privacy self-regulation. The more detailed the privacy codes are in terms of regulating data use, the less likely they are to have a wide applicability. 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 to Detroit, Johannesburg to 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 on priests of the Catholic Church. The 'death of distance' brought on by the internet and the increasing trend of integration within the global economy have also made privacy self-governance instruments outgrow their territorial origins and realise worldwide adoption. The privacy seals for websites that are provided by companies like TRUSTe or BBBOnLine, while they were a purely US-based reaction to the EU Directive and the transatlantic Safe Harbour agreement, are now also available for and used by companies in the Far East. In 2000, the Japanese Information Processing Development Centre (JIPDEC) 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 as a means of making data exports possible to countries that lacked adequate legislation. But they have 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 to develop a global privacy standard show, a homogenous regime for the self-governance of privacy is not yet within sight. While there is a global consensus on basic principles (more or less based on the 1980 OECD guidelines), the instruments differ in scope, reach, precision, and enforcement mechanisms. Albeit, they are gradually making their way through the global network of private business governance structures, becoming more and more interlinked with each other. More recently, they have also found their implementation in the form of technical codes.

B. Technical Codes

The regulatory efforts for privacy protection in the 1970s were early attempts by the states concerned 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 the data. They set up registration and even licensing mechanisms for databases. They regulated access controls and were filled with terms like ‘data’, ‘data file’ and ‘data record’. In some countries such as Sweden, the public supervisory agency possessed 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 did the privacy implications of technological design gain wide attention again, although in this case, the development towards privacy-friendly technologies came neither from governments nor from corporations, but as a result of user concerns and demands.

1. *User Self-help Tools*

The growing ubiquity of data processing converged with another development that had also begun 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 attempted to regulate the corporations, the new laws and amendments, and the developing case-law in the 1980s, gave 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 beyond just the collection of the data and included control of the individual over all later stages of the processing and use of the data (Mayer-Schönberger, 1998).

This development received a new boost from the internet. Cyberspace was initially seen as a great place for user empowerment. Until the mid 1990s, most of the ‘netizens’ did not want the government to have a role 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, were 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 heavily 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 is telling, as it 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 was—and for many still is—the best and only chance for users to ensure their privacy online. A number of privacy-enhancing end-user tools have been developed in the last 10 years. As personal computers became easier to use with graphical user interfaces like Windows, MacOS, and the 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 now readily accessible to all. Many of them are available for free distribution, and some of them work directly online. The first widespread tool for encrypting data on personal computers was Phil Zimmerman's 'Pretty Good Privacy' (PGP). It triggered a landslide of attention and after a six-year long legal and political struggle in the United States, resulted in a liberalisation of export control restrictions on cryptography technology in 1999 (Bendrath, 2001).

The tools available today 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 for anonymously using websites that require registration; traffic scrambling networks; and much more.[9] They generally offer two kinds of privacy protection. Most of the encryption and traffic scrambling tools help their users to hide data, internet traffic patterns, and the traffic's content from prying eyes, whether law enforcement agencies or network providers. They therefore allow online interactions between trusted parties, be they friends, business partners, or political activists. The main threat from the perspective of their users is still more or less based on the 'Big Brother' scenario, one also made popular by movies such as 'Enemy of the State' and widely reported snooping activities carried out by intelligence agencies like the National Security Agency. The other group of privacy-enhancing tools are directed against corporate data collectors who track visitors to their websites and online services. They include tools that allow the deleting of 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 for anonymously accessing registration-based online services.

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

2. *Negotiation-based Codes*

There is one problem that all of the above mentioned privacy-enhancing tools fail to address. If the user is doing an online purchase, he or she must enter their real name, credit card number, and other information into a corporate website. If the item bought is not a digital item like a music file, the company also needs the address and further information for delivery. How can users be certain this information will not be misused at a later date? This is where negotiation-based technical codes come into play, which act like an agent between the user and the companies. The user can apply tools that automatically negotiate his privacy preferences with the website

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

he visits. A well-known example of this is the P3P standard ('Platform for Privacy Preferences Project') for websites. It was developed by the World Wide Web Consortium (W3C) with the involvement 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 being merely 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 Center mentioned the lack of enforcement options, because 'P3P provides no means to ensure enforcement of the stated privacy policies' (EPIC and Junkbusters, 2000). Nowadays, about 10 per cent of all major websites have some P3P functionality (Byers *et al*, 2003), but most web browsers except Internet Explorer have ceased to support P3P, while still keeping privacy settings as part of their functionality. The EU's Data Protection Commission had already requested that the default settings in browsers should reflect the highest level of protection, even before the P3P standard was adopted (Article 29 Working Party, 1998). This was not the case, and with the internet becoming a mass medium, the average user now is even less familiar with these technological solutions or with how to set up personal privacy preferences in browsers.

3. *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: (1) a simple and user-friendly administration of a person's online identity; and, (2) 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 users.

It is not yet clear if whether this will actually lead to better data protection or even to the end of anonymity on the net. Microsoft's heavily criticised 'Passport'/'.Net' programs with centralised databases are regarded as PIMs, as are decentralised online infrastructures that ensure role-based pseudonymity (so-called 'federated' PIMs). Sophisticated designs include public key encryption schemes that allow the individual to not only control the delivery of his or her personal data to corporations and other users, but also the use of this data after it has been submitted (for an overview, see ICPP Schleswig-Holstein and Studio Notarile Genghini IMS, 2003). Complementary to the P3P front-end standard that allows the user to control 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 in accordance with the preferences of the person it belongs to. The Enterprise Privacy Authorisation Language (EPAL), such a privacy meta-data standard, is already being used by companies like eBay. As with P3P, the EPAL standard was submitted to the World Wide Web Consortium for adoption, and again like P3P, has been developed by the industry (IBM Laboratories Zürich) in cooperation with data protection commissioners (Borchers, 2004).

Recently, a lively debate has kicked off online and at various meetings and conferences concerning 'user-centric identity management'. It has been actively driven by Microsoft's privacy and identity staff, who—after the market failure of 'Passport'—seem to now understand 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 only allow the transfer of the minimum amount of personal data required. To return to our earlier road traffic analogy, if stopped by a police officer on a highway, drivers would only have to provide proof that they in fact possess a driving licence (legal driver credential), but not further details such as their name, address or other personal information that is not relevant in that specific context. Most of the participants in the development towards identity management come from large, US-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.[10]

The development of these infrastructural concepts is still in its early phase, and a broad user-base is still lacking. But, if successful, the technical design of the systems will have a broader impact on how anonymously people can 'move' on the internet in the future. In reference to 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

[10] A central hub for this development is a loose network called the 'Identity Gang' (http://www.identitygang.org) and the 'Identity Commons' group (http://www.idcommons.net). I regularly discuss developments around these issues in my blog (http://bendrath.blogspot.com).

would ask for the dog's age, gender, credit card number, or other pieces of information, depending on the service provided. The technical differences between the various 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).

4. *Comparison*

As 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 fact that different threats to privacy require 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 once more observe a trade-off between the reach of the technical codes and the privacy protection they provide. But, differing from the social codes, 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, is varying 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. Nevertheless, whether people use these tools, how intensively they use them, and in what combination still depends on their computer literacy and personal privacy preferences.

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. The user base for these tools is growing due to the network effects—that is, the more users a communications standard has, the more it will attract new users. This is especially true for tools that aim at protecting communications privacy or at exchanging encrypted data between trusted parties. Pretty Good Privacy (PGP) has become the de facto standard for private data security for this mechanism, with the OpenPGP standard having been submitted to the Internet Engineering Task Force (IETF, 1998) providing the basis for many other implementations (Bendrath, 2001). Here, if the parties to a communication use the same standard, they can be confident that their personal information and communication is protected.

Internet users who must provide 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, as only a minority of websites and browsers support P3P, and even if they do, there are no technical measures available yet that allow the individual control over 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 in the respective company, be they self-governance codes of conduct or legal obligations. This lack of technically supported control for users 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 in e-commerce, has fuelled new state-based regulation efforts in recent years.

IV. COMPLIANCE PROBLEMS AND THE NEW ROLE OF THE STATE

A. Ongoing Low Compliance Rates

In 1997, the OECD Committee for Information, Computer and Communications Policy conducted a survey of websites that openly questioned the effectiveness of the official mechanisms like the OECD privacy guidelines, and 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, several well-published cases of misuse of personal information from companies such as 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 online privacy protection. Users, according to a number of other surveys, were not satisfied with the state of online data protection (for an overview, see Bennett, 2004b). A March 2004 EuroBarometer survey found that of the 84% of EU citizens who did not shop online, 25% said it was because they did 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. Consumers' lack of trust in privacy and other rights on the web was and is still perceived as a major problem standing in the way of a large-scale breakthrough for e-commerce. This was repeatedly stated between 1997 and 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.[11]

Therefore, states have been trying, either directly or indirectly, to influence the development of technical codes for privacy protection, and have also started public auditing and certification programmes for social codes of privacy self-governance. In addition, the most recent development is the return of the good-old state-centrist model of regulation. A public demand for legislation in the absence of meaningful private sector regulation can now loudly be heard.

B. The State's Seal on Social Codes

The 'adequacy' rating for the privacy protection levels in third countries by the EU Commission in a way equates to the job done by rating agencies in the financial sector. Elsewhere in the data protection universe, states have 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 has 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 can in turn 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 were conceived as exceptions that should rarely be used, but since the Safe Harbour 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

[11] See, eg, 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, 'Dismantling the Barriers to Global Electronic Commerce' (OECD, 1998b), the OECD 1998 Ottawa ministerial conference, 'Realising the Potential of Global Electronic Commerce' (OECD, 1998c), the 2003 World Summit on the Information Society's 'Declaration of Principles' (WSIS, 2003).

commissioners have a strong role here. Several adoptions of this certified self-regulation have been developed at 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 laws. These decisions are not binding, however; and therefore the individual data processors (corporations, website owners, or 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 2001, with the Data Protection Commissioner's independent centre as the official public certification authority. Interest among corporations in 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 who are supposed to do the auditing (Sietmann, 2004). The privacy seal nevertheless is currently being taken to the European level by the EU-funded project "European Privacy Seal" (ICCP, 2008). A similar movement can be observed in Australia, where the standard principles were incorporated into national law in 2001. Here, the Privacy Act allows organisations and industries to have and to enforce their own privacy codes in order to allow for some flexibility in 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, 2005).

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 Federal Trade Commission (FTC). Companies that receive this certificate significantly reduce the risk of liability lawsuits in case problems do arise. As it fits into the US model of privacy protection through the courts, it could possibly be used as a model in other areas of privacy protection as well (Cranor and Reidenberg, 2002: 19). It also follows the trend in the United States by focusing on formalised compliance methods, with legal obligations, in order to minimise risks, prompting calls of an emerging 'audit society' (Power, 2002). Another model is reducing the bureaucratic task of having to get a new privacy certificate for each jurisdiction that a company wishes to do business in. The EU Directive envisions consultations between privacy commissioners and business associations at the national level for countrywide 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, DaimlerChryser became the first corporation to receive a certificate that was valid throughout the entire EU for its global Privacy Code of Conduct from the French supervisory agency CNIL. Others, such as General Electric, have been following in their footsteps. In its first report on the implementation of the 1995 Data Directive in 2003, the EU Commission noted its importance, stating that 'certification schemes play a crucial role' (EU Commission, 2003: 16).

C. 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, under the E-Government Act of 2002, every federal agency must conduct a PIA before it can develop or introduce new information systems that use personally identifiable data. These PIAs must be published and supervision is provided by the Office of Management and Budget. The P3P standard for websites is also mandated by the above-mentioned E-Government Act, as are privacy notices on all government websites. The privacy notices must include which information is collected, why it is collected, with whom the information is shared, what form of 'notice' is available to the individual, and how the information is secured (*Privacy Times*, 2 December 2002). Government *use* of these technological systems, standards, and protocols of data protection, such as P3P, is of course not a regulation of the private sector, but it can help spread their adoption beyond the public sector. The large number of its own computers, which the government can use as a leverage, can create the critical mass for widespread adoption through network externalities, and the official use also functions like a certificate.

Another approach is for government agencies to actively participate in and support the development of privacy-enhancing technologies. As mentioned above, public data protection authorities and commissioners regularly participate in industry expert groups that design technical codes for privacy protection like P3P and EPAL. The European Union has funded a large section of P3P development and supports several privacy and identity management projects within its framework research programmes.[12]

[12] 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).

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 carried out extensive studies on privacy-enhancing technologies to further the debate and the exchange of knowledge (as a prominent example, see Borking and Hes, 2000).

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' program is such an example of how the European Union is now making an impact on global technical developments and thus on global data protection compliance. In its original architecture, Microsoft planned for the centralisation of all data collected from visitors to its affiliates' websites in order to provide authentication services for the latter. Microsoft abandoned this plan following privacy complaints from consumer groups and pressure from EU data protection commissioners (EPIC and Privacy International, 2004: 131). Another example is search engine giant Google's free email service 'Gmail', which automatically scans all its users' mail and places context-sensitive advertisements within them. After strong protests from a number of privacy NGOs and an official complaint to several European data protection authorities by Privacy International, the EU group of data protection commissioners stated that Google's service may be in violation of the European data protection Directive (Links & Law, 2004). Google had to ensure that mail scanning was only done by machines and only with the explicit consent of the users. Whilst the EU data protection bodies merely threatened to initiate legal action against Microsoft and Google in these cases, later entering into discussions with both companies, the California State Senate 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 is less reliant purely on users' self-help or industry self-regulation. But instead of regulating individual data banks and data centres, as was the norm in the 1970s, it is concentrating on technical infrastructures and standards that will potentially have a widespread impact on the use of personal data.

D. The Return of Legal Enforcement

The call for government regulation over private sector privacy policies and behaviour has been continually growing over the past few years. Beth Givens, director of the privacy rights clearinghouse, concluded her comments on the 1999 Georgetown privacy survey with a recommendation that the FTC 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. To the surprise of many, it said that legislation was needed to complement industry initiatives like the standard proposed by the Network Advertising Alliance and others. The most important reason given was the defection problem, still prevalent within 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 United States, is reaching its limits. The Bush administration has hesitated to adopt a comprehensive data protection law for the private sector and since the attacks of 2001 is not known as a strong supporter of privacy protection in general; however, Congress has seen a rising number of initiatives for data protection legislation since then (Smith, 2006). Several US States have already moved further and passed laws that protect data more comprehensively than current federal legislation.[13] In 2003, California passed the 'Shine the Light' law, enabling customers to find out how businesses sell their personal information. Since then, companies that do business with Californian residents must either allow customers to opt out of information-sharing, or disclose to them in detail how their personal information is shared with others. The Bill was a landmark because it was one of the first legislative attempts in the United States to address 'list brokerage', the compilation and sale of individuals' personal information for marketing campaigns, including spamming, telemarketing, and junk mail. Prior to this, businesses were under no obligations to inform customers and visitors of their information business activities even though 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, has recently led to a number of large corporations in the information sector rethinking the need for state-based governance of privacy. In November 2005, in a widely perceived move, Microsoft called for a comprehensive privacy law in the United States (Smith, 2005)[14]. The 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).

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

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

V. CONCLUSION: THE COMPLEX NETWORK OF PRIVACY GOVERNANCE

A. The Role of the State in a Different Shape

Even in private sector self-regulation, there is a growing interest by corporations in getting the state 'back in' ('pull'), while at the same time the failures of pure private sector regulation have created a rising public demand for more state control and enforcement ('push'). Be it public funding and promotion of privacy-enhancing technologies, government supervision over private seal mechanisms, officially certified auditing of privacy policies, or the recent US developments in favour of private sector regulation mandated by law, the state is gaining a more prominent role than it used to have, especially when we consider the 'hands-off' approach towards the internet that was prevalent 10 years ago.

However, what is different from the state-centric approach to privacy and data protection regulation of the first generations is the more prominent role of intermediaries. The state does not regulate big databases and computer centres directly, as it did in the 1970s and 1980s. This would be unfeasible, especially 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 no longer pursued directly, but through private intermediaries (Perritt, 1997). These are:

— trade associations that receive 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 from 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 is all happening within the 'shadow of the law' (in the United States) or even within a legal framework (in other OECD countries), and with an important role still being played by private sector self-governance. The agents and tools of data protection regulation therefore are diverse, with a growing role for the state again. The distributed nature of this new regulatory pattern shows the changing role of the state, which is more an 'enabler' than an 'enforcer' and must work with all types of other agents, sometimes cooperating, sometimes enforcing, and sometimes enabling. This convergence of the EU and US patterns of privacy regulation (and with other regions following) is one striking result of the globalisation of personal data flows through the internet. States in general are no longer willing to tolerate every possible use of personal data in the online environment. Issues with increasing 'spam' are adding to the problem. This has been the subject of several UN discussions, and under the lax CAN-SPAM Act of 2003,[15] we have already witnessed the first big court cases against spammers in the United States.[16]

The Safe Harbour 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 leaves the certification and operation of privacy governance to the private sector. It also limits the scope of privacy adequacy ratings from whole countries to individual companies. By doing this, it allows 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. Things are different in the computer world. It certainly makes sense to have *one* version of a new Microsoft system operating on global scale, 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 reprogramme it so you can distinguish between the use of personal data of EU and US citizens. The external effects of specific privacy regulations are therefore much more effective when they explicitly focus on extraterritorial and third party effects, as the 1995 EU Directive did, and where they are based on law, rather than voluntary compliance.

The trading-up effect through transnational business networks is also still in place. 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 like 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 use it too). 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.

[15] 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.

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

B. The Role of Social and Technical Codes

The distinct technical nature of the internet allows for means of regulating behaviour other 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 either: (a) forces users to either reveal their personal data or be locked out of a service; or (b) 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 is 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 and different compliance and public supervision mechanisms, as well as different degrees of control by users and customers over their data. Because they work under conditions of global transnational communications, they cannot be neatly separated by territorial borders or industry sectors any more. In a global cyberspace where proximity and distance in the classical territorial sense have vanished, rezoning the internet into separate national or organisational sub-nets has not been possible as yet, and it is certainly something most users, companies, and developers would oppose anyway.[17] In many respects, it is a return to 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 offering users some choice in the matter—has yet proven too complex a task to find workable applications and convenient widespread use. We will therefore witness for some time to come, a global privacy regime that is diverse, overlapping, and contradictory. Until truly global privacy norms and standards are established, the next best thing we must settle on is the 'adequacy' rating method, which is increasingly being applied to social and technical codes alike.

[17] This will only be possible if the underlying internet addresses (IP numbers and domain names) are rezoned 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 and Wu, 2006.

The attempts of governments and the European Union to encourage technological regulation schemes may have a harmonising effect, and possibly create a wider use of privacy-enhancing technologies. As most of the developments described in this chapter 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 take place if there is a global agreement on the *content* of the technical rules, on the level of privacy protection that is desired. The seed crystals for such a global privacy standard are slowly emerging as the result of regional mandatory laws such as 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 informatica*. In the end, social codes 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) *Platform for Privacy Preferences (P3P) and the Open Profiling Standard (OPS)*, Opinion 1/98, Document WP 11 (Brussels, EU Commission).

—— (2005) 'Setting Forth a Co-operation Procedure for Issuing Common Opinions on Adequate Safeguards Resulting From "Binding Corporate Rules"', Working Document, 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 B Kahin and E Wilson (eds), *National Information Infrastructure Initiatives: Visions and Policy Design* (Cambridge, MA, MIT Press) at 532–52.

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, JP (1996) *A Declaration of the Independence of Cyberspace*, Davos, Switzerland, 8 February 1996 (http://homes.eff.org/~barlow/Declaration-Final.html).

BBBOnLine (2008) Consumer Privacy Website, (http://www.bbbonline.org/consumer/Privindex.aspx).

Bendrath, R (2001) 'PGP—die ersten zehn Jahre' in *Telepolis*, 19 March (http://www.heise.de/tp/deutsch/inhalt/te/7175/1.html).

Bennett, CJ (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 K Webb (2004) *Voluntary Codes: Private Governance, the Public Interest and Innovation* (Ottawa: Carleton Research Unit for Innovation, Science and Environment), 227–48 (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, CJ and Raab, CD (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.

—— (2006) *The Governance of Privacy. Policy Instruments in Global Perspective*, 2nd (updated) edition (Cambridge, MA, MIT Press).

Berg, T (2000) 'www.wildwest.gov: The Impact of the Internet on State Power to Enforce the Law', 25 *Brigham Young University Law Review* 1305–62.

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

Bijker, WE (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 (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 (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 auf die mündliche Verhandlung vom 18. und 19. Oktober 1983—1 BvR 209, 269, 362, 420, 440, 484/83 in den Verfahren über die Verfassungsbeschwerden, (http://www.datenschutz-berlin.de/gesetze/sonstige/volksz.htm).

CEN (2002) 'Initiative on Privacy Standardization in Europe', Final Report (Brussels: CEN/ISSS).

Charlesworth, A (2000) 'Clash of the Data Titans? US and EU Data Privacy Rules', 6 *European Public Law* 253–74.

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, LF (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* (New York City, Association of Computing Machinery) (http://portal.acm.org/citation.cfm?id=543506).

Cranor, LF and Reidenberg, JR (2002) 'Can user agents accurately represent privacy notices?', Paper for the Telecommunications Policy Regulation Conference (http://tprc.org/papers/2002/65/tprc2002-useragents.PDF).

Drake, WJ (1993) 'Territoriality and Intangibility' in K Nordenstreng and H Schiller (eds) *Beyond National Souvereignty: International Communications in the 1990s* (Norwood/NJ: Ablex) at 259–313.

Ellger, R (1996) 'Vertragslösungen als Ersatz für ein angemessenes Schutzniveau bei Datenübermittlungen in Drittstaaten nach dem neuen Europäischen Datenschutzrecht' 60 *Rabels Zeitschrift für ausländisches und internationales Privatrecht* 738–70.

Engels, F (1978) 'On Authority' in Robert Tucker (ed), *The Marx–Engels Reader* 2nd edtion (New York: W.W. Norton).

EPIC (Electronic Privacy Information Center) (2005a) 'California SB 27 "Shine the Light" Law' (http://www.epic.org/privacy/profiling/sb27.html).

—— (2005b) 'SPAM—Unsolicited Commercial E-Mail' (http://www.epic.org/privacy/junk_mail/spam/).

EPIC and Junkbusters (2000) : *Pretty Poor Privacy: An Assessment of P3P and Internet Privacy* (http://www.epic.org/reports/prettypoorprivacy.html).

EPIC and Privacy International (2004) *Privacy & Human Rights 2004 An International Survey of Privacy Laws and Developments* (Washington, DC: EPIC).

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 (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.

—— (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.

—— (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.

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

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

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

EU JRC (European Union Joint Research Centre) (2003): *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.

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', *ZDNet Tech Update* 19 October (http://techupdate.zdnet.com/Federated_identity_PingID_standards_cartels.html).

Farrell, H (2002) 'Hybrid Institutions and the Law: Outlaw Arrangements or Interface Solutions?' 1 *Zeitschrift für Rechtssoziologie* 25–40.

—— (2003) 'Constructing the International Foundations of E-Commerce: The EU–U.S. Safe Harbor Arrangement', 2 *International Organization* 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', Masters 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 (Federal Trade Commission) (2000) *Online Profiling. A Report to Congress, Part 2: Recommendations*, July 2000 (Washington, DC., Federal Trade Commission) (http://www.ftc.gov/os/2000/07/onlineprofiling.htm).

GBDe (Global Business Dialogue on electronic commerce) (2001) '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, NY, Oxford University Press).

Hansen, E (2004) 'California Senate approves anti-Gmail bill', CNET News.com, 27 May (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 (Independent Centre for Privacy Protection) Schleswig-Holstein and Studio Notarile Genghini (2003) *IMS (Identity Management Systems) Identification and Comparison Study for the EU Joint Research Centre Kiel* (http://www.datenschutzzentrum.de/idmanage/study/ICPP_SNG_IMS-Study.pdf).

ICPP (Independent Centre for Privacy Protection) Schleswig-Holstein (2008) *EuroPriSe—Europäische Datenschutz-Pilotzertifzierungen beginnen*, Press Release, 30 January (https://www.datenschutzzentrum.de/presse/20080130-europrise-pilotzertifizierung.htm)

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

ISO/IEC (2006), 'New Work Item Proposal on A privacy framework', ISO Joint Technical Committee 1, Document ISO JTC N8172, 22 June.

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

Johnson DR, Crawford, SP, and Palfrey, JG 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, DR and Post, DG (1997) 'The Rise of Law on the Global Network' in B Kahin and C Nesson (eds) *Borders in Cyberspace. Information Policy and the Global Information Infrastructure* (Cambridge, MA, MIT Press), at 3–7.

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, NY, 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, MA, Open University Press).

Mayer-Schönberger, V (1998) 'Generational Development of Data Protection in Europe' in PE Agre and M Rotenberg (eds), *Technology and Privacy: The New Landscape* (Cambridge, MA, MIT Press) at 219–41.

—— (2003): 'The Shape of Governance: Analyzing the World of Internet Regulation', 43 *Virginia Journal of International Law* at 605–73.

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.

—— (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.

—— (1998b) Directorate for Science, Technology, and Industry, Committee for Information, Computer and Communications Policy 'Dismantling the Barriers to Global Electronic Commerce', An International Conference organised 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.

—— (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 at the Conference 'Realising the Potential of Global Electronic Commerce', Ottawa, 7–9 October, OECD Doc No DSTI/ICCP/REG(98)10/FINAL, published 18 December 1998.

Perritt, HH (1997) 'Jurisdiction in Cyberspace: The Role of Intermediaries' in B Kahin and C Nesson (eds), *Borders in Cyberspace. Information Policy and the Global Information Infrastructure* (Cambridge, MA, MIT Press) 164–202.

Post, DG (1998) 'The "Unsettled Paradox": The Internet, the State, and the Consent of the Governed', 5 *Indiana Journal of Global Legal Studies* 521–39.

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

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

Reidenberg, JR (1998) 'Lex Informatica: the Formulation of Information Policy Rules Through Technology', 76 *Texas Law Review* at 553–84.

—— (1999) 'The Globalization of Privacy Solutions. The Movement towards Obligatory Standards for Fair Information Practices' in CJ Bennett and R Grant (eds), *Visions of Privacy. Policy Choices for the Digital Age* (Toronto, University of Toronto Press).

—— (2000) 'Resolving Conflicting International Data Privacy Rules in Cyberspace', 52 *Stanford Law Review* 1315–71.

Richardson, L (2000) 'History of Self-Regulation Cast Doubt on its Effectiveness', *Privacy Times*, 12 July, 7–11.

Rosecrance, R (1996) 'The Rise of the Virtual State', 4 *Foreign Affairs* 45–61.

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

Rössler, B (2001) *Der Wert des Privaten* (Frankfurt am Main, Suhrkamp).

Schwarz, PM and Reidenberg, JR (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', 68 *Social Research* at 481–513.

Shaffer, G (1999) 'The Power of Collective Action: The Impact of EU Data Privacy Regulation on US Business Practice', 5 *European Law Journal* 419–37.

Shaffer, G (2000) 'Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting up of U.S. Data Privacy Standards' 25 *Yale Journal of International Law* at 1–88.

Sietmann, R (2004) 'Bundestag will Datenschutzreform anmahnen' in *Heise News* 1 December (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, MS (2006) *Internet Privacy: Overview and Legislation in the 109th Congress, 1st Session*, CRS Report to Congress RL31408 (Washington DC, Congressional Research Service).

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

Swire, PP and Litan, RE (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', 63 *Zeitschrift für ausländisches öffentliches Recht und Völkerrecht* 1–28.

TRUSTe (2008) TRUSTe Fact Sheet, (http://www.truste.org/about/fact_sheet.php).

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

—— (2005) 'Safe Harbor Overview' (http://www.export.gov/safeharbor/sh_overview.htm).

—— (2007) '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, DC., United States 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 4 *Harvard Law Review* 193–220.

Weichert, T (2000) 'Zur Ökonomisierung des Rechts auf informationelle Selbstbestimmung' in H Bäumler (ed), *E-Privacy. Datenschutz im Internet* (Braunschweig and Wiesbaden, Vieweg) 158–84.

White House (1997) A Framework for Global Electronic Commerce, 1 July.

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

Winner, L (1986b) 'Do artifacts have politics?' in L Winner, *The Whale and the Reactor. A Search for Limits in an Age of High Technology* (Chicago, IL: University of Chicago Press) 19–39.

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

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