

Working paper 'Code' and Privacy

Questions for the workshop

1. Do you agree with the conclusion that privacy-related norms are rarely explicitly built-in in technology?
2. Do you agree with the conclusion that privacy violation is often a side-effect of technological developments?
3. What do you think of the distinction between the 'Death of Privacy' issue and the 'Code & Privacy' issue (see 5.4, 5.5 under 1, and 5.6)?
4. Which cases in 5.3 do you like as particularly illustrative? Which cases are less useful?
5. Are there any other cases you would suggest we describe as particularly relevant?
6. Is privacy slowly eroding through technology?
7. Are Privacy-Enhancing Technologies a sop or the salvation of privacy?
8. Is there any need for action? If so, what kinds of action?

5. 'Code' and Privacy

version 18 June 2004

Ronald Leenes & Bert-Jaap Koops¹

The future of privacy is increasingly linked to the future of technology²

5.1	INTRODUCTION	3
5.1.1	<i>Panoptic Panoramas</i>	3
5.1.2	<i>Technology, Privacy, and Lessig's Code</i>	4
5.1.3	<i>Research Questions and Overview</i>	6
5.2	PRIVACY	6
5.2.1	<i>Concepts of Privacy</i>	6
5.2.2	<i>Privacy Laws</i>	8
5.2.3	<i>The Privacy Balance and Reasonable Expectations</i>	9
5.2.4	<i>An Example: Webcasting</i>	10
5.2.5	<i>A Contextual-Functional Perspective</i>	12
5.3	'CODE' AND PRIVACY IN CONTEXT	15
5.3.1	<i>Law Enforcement</i>	16
	Case 1: Interceptability of Telecommunications	17
	Case 2: Location Data	19
	Case 3: Cryptography.....	20
	Balance.....	24
5.3.2	<i>National Security</i>	25
5.3.3	<i>E-Government</i>	26
	Balance.....	29
5.3.4	<i>Commerce</i>	30
	Case 1: Transaction Monitoring in Mobile Telephony and Banking.....	31
	Case 2: Tag, You're It: RFID Will Get You	32
	Case 3: <i>Facial Recognition in Shops?</i>	35
	Balance.....	35
5.4	THE EFFECTS OF 'CODE' ON PRIVACY	36
5.5	EVALUATION OF 'CODE' AND PRIVACY	37
5.6	OPTIONS FOR ACTION	40
	REFERENCES	42

¹ Dr. Ronald Leenes is assistant professor at the Center for Law, Public Administration, and Informatisation of Tilburg University. Dr. Bert-Jaap Koops is associate professor at the same center. Parts of this chapter are based on the work of dr. Ton Schudelaro and dr. Anton Vedder, whom the authors thank for their collaboration.

² Inspired by Julie Cohen's remark that '*The future of privacy is increasingly linked to the future of copyright enforcement*' (2003).

5.1 Introduction

5.1.1 Panoptic Panoramas

In 1787, Jeremy Bentham, the English utilitarian philosopher, worried over the moral state of his times, and he devised an architectural design for a prison that he called the Panopticon. This Panopticon has stood model for a kind of ultimate surveillance ever since, and is hence connected to the concept of privacy. The Panopticon is a hemispherical building. On the outer perimeter there are a number of levels, each containing cells for the inmates. The individual cells are completely isolated from each other, making it impossible for the inmates to see or hear the other prisoners. In the middle of the Panopticon is the office of the Inspector. The inspector can see and hear every individual prisoner, but the prisoners can not see the Inspector. One can imagine that this requires complicated structures, and one can even doubt whether it could have been constructed in Bentham's times at all.

The principal idea of the Panopticon is that inmates are under potential scrutiny of the Inspector at all times. The Inspector has the capacity to see and hear all inmates and issue commands to them individually, day and night. Not so much that the fact that the Inspector can issue commands and monitor the inmates is the strength of the Panopticon, but the illusion that he could. As the point of the Panopticon is *discipline* or *training* (Whitaker 1999), the constant illusion of monitoring and the fear inmates feel of punishment for transgressions makes that they will learn the rules quickly and behave accordingly. That, at least, is the idea.

In Bentham's view, the idea of the Panopticon could not only be used as a model for prisons, but also for asylums, workplaces, and schools, to name but a few areas. Bentham carried a social mission to improve society, and seeing without being seen plays an important role in accomplishing this goal.

Not surprisingly, the Panopticon has become a metaphor for total surveillance. And whereas the actual implementation of the Panopticon was not very realistic in Bentham's times, it is nowadays becoming increasingly so. Closed Circuit TV (CCTV) cameras are appearing everywhere, in both private and public places. And although increasingly these cameras are operated by private enterprises, many are state-controlled. They are often placed more or less with Benthamite goals in mind, such as the increase of public safety ('Big brother is watching out for you' instead of 'Big brother is watching you' (Whitaker 1999, p. 141)) and increased compliance with speed regulations. And, completely in line with panoptic logic, there may actually not be anyone watching the shots taken by the cameras or they may lack film. It is the possibility of being caught that is part of their effect. The illusion of an omnipresent inspector is there to keep the subjects in line.

The internet offers excellent opportunities for even further-reaching forms of surveillance. Boyle (Boyle 1997), following Foucault's analysis of the Panopticon (Foucault 1978), concludes that the state is creating an Internet Panopticon: '... the state has worked actively to embed or hardwire the legal regime in the technology itself'. An interesting aspect of this Internet Panopticon is that the state shifts the responsibility of enforcement to entities in the private sector, such as ISPs.

In the meantime, as Schwartz writes, private entities are happily creating their own independent Panopticons (2000b, p. 853). Businesses are collecting and processing vast amounts of personal data for different, but not all too different, reasons than the state does. In a sense, private-sector enterprises use monitoring and surveillance to have people behave the way they want. 'Customers are disciplined by consumption itself to obey the rules, to be "good" not because it is morally preferable to being "bad" but because there is no conceivable alternative to being good, other than being put outside the reach of benefits' (Whitaker 1999, p. 142). Coercion in this private Panopticon is replaced by consent, but the prevailing characteristics of panoptic logic remain.

Thus, both the state and the private sector engage in surveillance of people's lives. And while the motives and means vary, both public and private systematic prying into people's privacy raises serious legal and ethical questions.

5.1.2 Technology, Privacy, and Lessig's Code

The Panopticon relies heavily on technology. Especially Information and Communication Technologies (ICTs) offer almost unlimited options to facilitate perfect surveillance and monitoring, and hence invading people's privacy. Partly as a result of the rise of the network society, some authors have already proclaimed privacy dead. Books and articles have been titled 'The Death of Privacy' (Fromkin 2000; Garfinkel 1999) or 'The End of Privacy' (Sykes 1999; Whitaker 1999). Both the influence of technology and the fact that people seemed to care less about privacy have been considered factors that warrant the statement that privacy is no longer feasible, or relevant, or neither of these.

In this chapter, we intend to analyse this impact of technology on privacy. We do so by following the argument of Lawrence Lessig in the privacy chapter of his *Code and Other Laws of Cyberspace* (1999, p. 142-163). Lessig argues that 'the code [*i.e.*, technology] has already upset a traditional balance. It has already changed the control that individuals have over facts about their private lives.' He illustrates this with several privacy-threatening technologies. After an analysis of different conceptions of privacy and arguments pro and con privacy protection, Lessig presents a response to privacy threatening technology: privacy-enhancing technology. That is, in Lessig's view, 'code' that disturbs the traditional balance between privacy and other interests should be checked by 'code' that incorporates privacy values. This latter notion can be seen as an instance of what Reidenberg (1998) has termed Lex Informatica: software and hardware that regulate themselves, or rather, Internet users and developers who regulate themselves through technology.

Although we do not intend to analyze and criticize Lessig's chapter on code and privacy specifically, it is necessary to take a closer look at Lessig's analysis of the impact of code on privacy, and the solution he presents to the problems, in order to get a better understanding of the matter.

Lessig considers privacy from a conventional point of view: privacy equals information privacy - a right to control one's personal data (privacy control). This notion of information privacy is

generally thought to be introduced by Westin in his epoch-making study '*Privacy and Freedom*' (Westin 1967), and is shared by many authors (Kang, Cate, Robert Post). Electronic surveillance and the collection of personal data is problematic in Lessig's view for two reasons: manipulation and loss of equality. The first problem is that the collection of personal data leads to profiling. The profiles constructed on the basis of initial data are used to "normalize the population of which the norm is drawn" (Lessig 1999, p. 154). This is done by presenting the person who fits a particular profile only the options the profiler wants her to see. Obviously, this scheme works best if the profiled is unaware of this selective feed of options. This kind of manipulation affects people's autonomy to make choices.

The second risk Lessig sees in modern data collection is that equality is affected. He argues that people in the private space were relatively equal as a result of the relative anonymity of these spaces and the fact that transactions could take place in relative anonymity as well (Lessig 1999, p. 154). This was the result of the fact that information to discriminate was too costly to acquire. Modern data collection, especially but not only in conjunction with merging multiple data sources, makes it possible to discriminate. Lessig exemplifies this by pointing at frequent-flyer programs, which allow airlines to distinguish between classes of passengers. Whereas people using airlines are aware of the existence of frequent-flyer programs and everyone can join in on such a program, more opaque differentiation in types of customers is done by, for instance, online bookstore Amazon that presents different prices for DVDs on the basis of, for instance, the kind of browser used, whether one is a first-time or a repeat customer, and the ISP used by the customer.³ This is a more convincing example of the pressure on equality posed by profiling. Lessig's solution to these threats is a two-part system: code and property law. Lessig equates privacy with information privacy, and hence restoring people's control over their personal data is the logical approach to address the imbalance caused by technology. Instead of calling for legal measures, such as fair information practices, Lessig seeks the solution in technology: privacy-enhancing technologies. He embraces the idea of software implementing our privacy preferences; an electronic butler, who negotiates privacy protection on our behalf (Lessig 1999, p. 160-161). We will return to this notion, that builds on the World Wide Web Consortium's P3P project, later on in the chapter. The electronic butler implements negotiating power, but what if the other party simply ignores the negotiations and proceeds in collecting and using personal data without a person's consent? Lessig's solution to this problem is to define personal data as property rights and hence introduce property law as the regime to protect people's personal data. Property law facilitates *ex ante* control over personal data; only after consent, personal data may be used. Obviously the consent will only be given at the right price.

This brief summary of Lessig's chapter on code and privacy shows that Lessig claims that:

- privacy equals information privacy;
- code upsets the privacy balance;
- personal data should be considered a property right;
- code and property law should be used to restore the privacy balance.

Lessig's and others' analysis of privacy as control and personal data that should be treated as a property right is not uncontested (e.g. Litman 2000; Schwartz 2000a; Prins 2004). It exemplifies

³ <<http://www.computerworld.com/industrytopics/retail/story/0,10801,49569,00.html>>.

an American way of looking at privacy and privacy threats in the sense that it relies on market principles and self-regulation of private parties. The government is to abstain from interfering. In contrast we can place a European (continental) approach with government regulation for the fair treatment of personal data. In this chapter we will not go in too much detail on the debate over the various privacy conceptions, but we do need a better grasp on the slippery concept of privacy in order to understand the impact of code on privacy. For our purposes in this chapter, Lessig's claims that code upsets the traditional privacy balance, and that code can be used to restore this balance, is the most important.

5.1.3 Research Questions and Overview

In this chapter we try answer the following questions:

- Is privacy-related regulation being implemented in code?
- What (kind of) rules are embedded in this code?
- What could and should be done, by whom and when, to counter potential shifts in privacy balances caused by 'code'?

In answering these questions we will look at both the public and the private sphere, as the panoptic state seems to be emerging in both. Both public and private entities make use of privacy-threatening technologies, for different purposes and by different means. We will argue that different privacy balances exist in the various domains and that the impact and the assessment of this impact of code on privacy should be assessed with respect to the particular context. In other words, privacy and its threats are context-specific, since privacy is not a uniform concept. Apart from the threats, we also try and indicate potential solutions to these threats.

The chapter is organized as follows. In the next section, we briefly discuss a number of relevant notions with respect to privacy. We look at both the European perspective on privacy, which can be said to focus on dignity (Whitman 2004), and the U.S. perspective, which focuses more on liberty. In section three, we discuss developments on privacy and code in four domains, both in the public and the private sphere. Section four sums up the broader issues emerging from this case analysis, and concludes the chapter by answering our questions: does a privacy 'code' exist and, if so, what should be done?

5.2 Privacy

5.2.1 Concepts of Privacy

It has been noted in almost every article or book on privacy: privacy is a slippery notion, often and easily used, but its precise meaning is far from clear. This is not surprising, nor is it problematic: it is the nature of value notions that they are not precisely delineated. In fact, privacy may be a clearer and more concise concept than, for instance, autonomy or liberty (cf. Blok 2002). So, what does privacy amount to? What is it that can be assaulted by 'code'?

Many accounts of privacy take a theoretical approach in the sense that they try to define privacy from a philosophical, ethical, or moral point of view (e.g., Fried 1968; Rachels 1975; Westin

1967). They are not primarily concerned with protecting privacy, or regulating privacy, by means of legal instruments such as legislation. Other accounts focus on the implementation of privacy provisions in legislation and/or the way courts handle privacy issues (e.g. Bygrave 2002). Yet others address both the theoretical and legal-practical aspects of privacy (e.g., Johnson 1989; Blok 2002). And they do this for good reasons. Society is changing, and cases arise all the time that do not adequately fit current legal practice. Such hard cases, as they are called in legal theory, give rise to reflection on the principles on which a particular legal doctrine is founded. Given our field of study, 'code' and privacy, this is especially apparent. We are not particularly interested in the cases that remain within the boundaries of ordinary data-protection law, for instance. We are interested in the cases that make us frown. In other words, the cases that give rise to consider changing current legislation or legal practice. Hence we need to look at both the current legal practice, and the principles and theory surrounding the concept of privacy. We can start our little tour on the concept of privacy by looking at the various discussions that have taken place, and are still taking place, with respect to privacy. Bygrave (2002) distinguishes four major ways in which the concept of privacy is defined.

The first group of definitions takes non-interference as its starting point. This conceptualisation is highly influenced by Samuel Warren and Louis Brandeis' seminal 1890 paper 'The right to privacy. The implicit made explicit'. Warren and Brandeis saw the right to privacy as part and parcel of 'a right to be let alone', and 'the existing law affords a principle which may be invoked to protect the privacy of the individual from invasion [...] by the too enterprising press' (Warren and Brandeis 1890, p. 206). People should, for example, not be photographed by the press just like that, unless they choose to 'go public' themselves.

The second group of definitions centres on the degree of access to a person. An influential popular definition in this category is given by Ruth Gavison (1980), who defines the amount of access to a person on three dimensions: secrecy (the amount of information about a person), solitude (the amount of physical access to a person), and anonymity (the amount of attention given to a person). Privacy in Gavison's perception is a normatively neutral, instrumental concept.

A third group sees privacy in terms of information control. Westin (1967), Fried (1968), Rachels (1975) and also Lessig belong to this group. Some quotes can illustrate their position. Westin considers privacy to be 'an instrument for achieving individual goals of self realization' and defines it as 'being in a position to determine for oneself, when, how, and to what extent information about oneself is communicated to others' (Westin 1967); 'the control we have over information about ourselves' (Fried 1968); 'the ability to control who has access to us' (Rachels 1975).

The fourth groups of definitions relates privacy closely to intimate or sensitive information. Julie Inness promotes this privacy concept when she writes: 'the state of possessing control over a realm of intimate decisions, which includes decisions about intimate access, intimate information, and intimate actions' (Inness 1992). This may also enhance personal expression and choice (Schoeman 1992).

5.2.2 Privacy Laws

As privacy has found its way in all sorts of statutes, and is the subject of much case law, there is also a large body of knowledge on how society and the courts should cope with privacy. The way privacy is incorporated in positive law depends on legal traditions, however. In the U.S. common-law system, privacy provisions are scattered over many statutes and acts. The Constitution and the Bill of Rights are of course important, as they establish constitutional rights and privacy might qualify as such a right. Privacy as such, however, is not explicitly mentioned in either the Constitution or the Amendments. But this is precisely one of the reasons why Warren and Brandeis could argue that a right to privacy exists. A combination of Amendments is generally seen to cover the basic aspects of privacy.⁴ Relevant are the Third, Fourth, Fifth, Tenth and Fourteenth Amendments, and perhaps the First.

Apart from the constitutional provisions, privacy law in the U.S. is sectoral. Many sectoral acts contain privacy provisions. Examples can be found at the federal level in, for instance, Title III of the Omnibus Crime Control and Safe Streets Act of 1968 on wiretapping, the Privacy Act of 1974 that established a legal framework for the records collected by the federal government, the Cable Act of 1984 (cable television), the Video Privacy Protection Act (video rental records), the Electronic Communications Privacy Act of 1986 (electronic mail), the Polygraph Protection Act of 1998 (lie detectors), and the Telephone Consumer Protection Act of 1991 (auto-dialers and junk faxes) (Rotenberg 2001). At the state level, there are many more. Rotenberg (2001) argues that these sectoral laws, and the privacy provisions therein, are the result of new technologies entering the market and the need to regulate intrusive monitoring by these new technologies.

In the European Continental tradition, there is a history of privacy protection, both in the various constitutions, as well as in various national laws as a result of, for instance, the implementation of European Community Directives, for instance the EC Data Protection Directive.⁵ The cornerstone of European privacy protection is Article 8 of the European Convention on Human Rights and Fundamental Freedoms, which states:

1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

This provision establishes the core of privacy protection by protecting private life, and by specifying three particular spheres: home, family, and correspondence. This core and these spheres are associated with three types of privacy-protection measures.

1. *Physical Privacy*: the protection of people's physical bodies against invasive procedures, such as genetic tests, drug testing, and body searches (bodily privacy), as well as the setting of limits

⁴ Justice Douglas, for instance upheld this idea in his famous 'penumbra' argument in *Griswold v. Connecticut*, 381 U.S. 479 (1965).

⁵ Directive 95/46/EC.

on intrusion into the home and other physical environments, such as the workplace⁶ (territorial privacy). This covers searches, video surveillance, and other forms of monitoring.

2. *Relational Privacy*: both the security and privacy of communications, such as mail, telephones, e-mail, and direct communication, and the privacy of personal or intimate relationships, such as family life.

3. *Informational Privacy*: included in the private life, and developed in especially the EC Data Protection Directive, is the protection of informational privacy. This involves the establishment of rules governing the collection and handling of personal data, such as credit information, and medical and government records.

5.2.3 The Privacy Balance and Reasonable Expectations

Is privacy an absolute right? Although some claim it is, or at least go a long way in this direction, no-one effectively claims that privacy is completely inviolable. Breaches of privacy can be justified by considerations of the common good. A balance is required between privacy and other interests, and particularly with sensitive interests such as law enforcement and national security, this balance has always been a precarious one that seems to be continually contested. Etzioni (1999), for instance, claims that privacy is overvalued and that a new balance has to be found between privacy and other values. 'We need to treat privacy as an individual right that is to be balanced with concerns for the common good – or as one good among others, without a priori privileging any of them' (p. 4). Bearing in mind that he wrote this before 9/11, the view that privacy should not be 'privileged' has since gained wider acclaim.

In the European context, the privacy balance is essentially struck through the second paragraph of article 8 ECHR. Breaches of privacy are allowed if they are necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others. This necessity requirement covers proportionality and subsidiarity, that is, the privacy violation has to be proportional to the goal to be reached, and the goal should not be attainable by another, less infringing measure. Moreover, the breach of privacy has to be 'in accordance with the law', and hence has to be sufficiently clear and foreseeable for citizens, so that they are able to know in what circumstances their privacy can be violated. These criteria of legality, legitimacy, subsidiarity, and proportionality are also embedded in the fair information-processing standards set by EC Directives and implemented in national data-protection legislation in the EU member states. As such, balancing the various interests is inherent to the European data-protection regime (*cf.* De Hert 1998).

In the U.S. context, an important concept in assessing the right to privacy is that of 'reasonable expectation'. This concept was introduced in U.S. case law in the light of the Fourth

⁶ The workplace can also be protected by article 8 ECHR. See, e.g., *Niemitz v. Germany* (1992), *Halford v. UK* (1997).

Amendment's prohibition of unreasonable searches and seizures. In 1968, the Supreme Court in *Katz v. United States*⁷ decided the placement by federal authorities of an electronic listening device in a public phone booth to be unconstitutional. Justice Harlan wrote that the protected zone under the Fourth Amendment is defined by the individual's 'actual', subjective expectation of privacy, to the extent to which that expectation is 'one that society [was] prepared to recognize as reasonable'. In a large number of cases, the reasonable expectation of privacy has been the test to decide whether the (federal) state has unconstitutionally breached someone's privacy. Thus, for example, reasonable expectations of privacy can exist in homes, businesses, sealed luggage and packages, but no reasonable expectations of privacy were found in bank records, voice or writing samples, phone numbers, and automobile passenger compartments, trunks and glove boxes (Cate 1997).

Although reasonable expectations of privacy as such do not play a role in the continental concept of privacy, as justified breaches of privacy are covered in article 8 para. 2 ECHR, the concept nevertheless plays a role in the European outlook on privacy. The balancing test of deciding when a privacy violation is necessary in a democratic society, after all, depends on the seriousness of the privacy violation, and this in turn relies to a certain extent on the way or amount of privacy that people experience in that particular context. Privacy breaches by technology are in many cases troublesome simply because people expect their privacy to be respected in those cases; if people are unfamiliar with new, privacy-invasive technologies, the use of such technologies will be considered a greater violation of privacy, and hence, the counter-balancing interest will have to be more serious if such a use is to be allowed under the balancing test of article 8 para. 2 ECHR.

5.2.4 An Example: Webcasting

To illustrate how new technologies affect privacy adversely and how a loss in actual privacy may lead to shifts in reasonable privacy expectations or in the balance of privacy and other interests, we shall describe a prototypical case: webcasting or webradio.

One of the problems with technology and privacy is that in some instances breaches of privacy, potentially at least, occur in situations where the users of the technology are unaware of the possible breaches as they expect to have privacy. Radio, and later television, were originally broadcast over the air as a practical way to reach people in geographically diverse locations. Anyone with the proper equipment could tune in to a show and listen to, or view, the audio(visual) content provided by the broadcaster. As there is no way to monitor who listens to what on ether broadcast radio, the technology does not affect people's privacy. The introduction of cable networks in the 1970s and advances in content encryption provided content providers more control over their audience, as they opened the way to subscription-based broadcasting and pay-per-view models. Whereas a subscription model generally only gives information on the channels a subscriber subscribes to, a pay-per-view model implies insight in the programs listened to or watched by a subscriber. These data, since they are, or can be, connected to subscriber data, do impact people's privacy.

⁷ *Katz v. United States*, 389 U.S. 347 (1967).

The Internet is becoming an important channel for the delivery of audiovisual content in ways that resemble the traditional radio and television broadcast. Streaming-media protocols, such as the Real Time Streaming Protocol (RTSP)⁸ and Real-Time Protocol (RTP), enable anyone with a broadband Internet connection to set up on-demand delivery of real-time data, such as audio and video, in live data feeds or stored clips. Delivery can take place either unicast, in which the client chooses what and when to receive, or multicast, in which case every client receives the same data at the same time.

Listeners or viewers use audio and video players, such as RealPlayer, Windows Media Player, or iTunes to connect to a streaming server. The player requests the server to open a session in which particular data is streamed to the client. Client and server exchange information about the location (server and client IP) and the content to be broadcast.

Webradio has become quite popular and is used by traditional radio stations as a supplementary service or as a means to reach larger audiences. But also, thousands of non-professional providers have set up webradio stations. The popularity of webradio is due to the unprecedented number of 'radio' stations a listener can access with simple means: an ordinary PC with a broadband connection (cable, DSL).

The fact that client and server exchange data for the proper functioning of the service does not necessarily affect the privacy of the listeners. As long as no logs are kept, there are no privacy issues per se. The catch in this case comes from the content provided. Since most material broadcast is copyrighted material, webradio or webcasting touches upon copyright law. Although it is being debated whether webcasters are to pay license fees and to whom – the artists and/or the record industry –, the case has been settled in many countries.⁹ Webcasters generally need a license agreement with the copyright holder or the representatives of the copyright holders (neighbouring rights), the SENA in the Netherlands, for instance. The webcaster has to pay remuneration for each track (song) streamed for each listener.¹⁰

This royalty-payment scheme, made possible by the technology, differs from that of traditional over-the-air radio. Traditional radio-broadcast license fees are based on estimates of the number of listeners of a particular radio station. Webradio allows for a much more precise scheme, because the listener's media player, iTunes for instance, requests a particular webradio station to start streaming content to the client. The webcaster therefore knows exactly which clients are tuned in to its broadcast. This facilitates the production of exact data on the number of clients tuned in on each track streamed by the webcaster. Webcasters are obliged to produce these data in their quarterly reports to (representatives of) rights-holders, such as SENA, and as such they keep detailed listener logs, containing the date and time a particular client has tuned in and out of particular stations, as well as the client's IP. IP's can in some instances be traced back to individuals, and hence can be identifiers.¹¹ This means that data maintained by webcasters, and made available to organizations such as the SENA, can be used for monitoring and profiling of listeners. An individual webcaster of, say, Lowlands Jazz, may be able to infer information from the patterns Ronald's computer leaves in their listeners' log. It may tell something about

⁸ <<ftp://ftp.ietf.org/rfc/rfc2326.txt>>.

⁹ See for instance *Bonneville International Corp. v. US Copyright Office*, 01-3720, 17-10-2003 (3rd Circ. 2003).

¹⁰ In the Netherlands, the fee in 2004 was 0.00084 € per track per listener. In the U.S., it was 0.0007 \$ in 2002.

¹¹ According to the Dutch Data Protection Authority, <http://www.cbpweb.nl/documenten/uit_z2000-0340.htm>.

Ronald's taste as he tends to tune in to another station (unknown to the LowLands Jazz station) at moments that suggest his taste to be the motivator (after a couple of notes or the start of a new program). Or, it may tell something about his living habits, if patterns occur in the times he tunes in to the station (usually in weekends rather than working days, and on Tuesdays). The impact on the privacy of the listener increases if various listener logs are merged, especially if they are combined with other online traces, such as website logs, which also contain IPs. Most people are aware of the fact that IPs are logged when they surf the internet. But are they aware that webcasters also collect data on their use of the service? Of old, one could listen to over-the-air radio anonymously, and many people will expect webcasting not to depart from this idea. Yet it does. The webradio listener is monitored and the data collected can in principle be used for other purposes than remuneration.

How should we assess this example? Webcasting as a species of 'radio' introduces a shift in the privacy balance. Listening to broadcast radio is no longer completely anonymous if done through webradio. What can justify this diminishing of privacy? If we apply Etzioni's (communitarian) test,¹² then clearly there is no well-documented and macroscopic threat to the common good; the listeners log is just a convenient way to meet financial or economic needs. As IPs are unique, they provide convenient metering units. Is this enough to warrant the diminishing of the privacy protection? Not necessarily, especially if there are (even) less intrusive ways to measure the number of 'eyeballs' in a particular timeslot.

Nevertheless, it may well be that the new privacy infringement goes unnoticed or unheeded by the public and government at large, thus *de facto* establishing a new – lower – privacy standard. And perhaps as people get used to being 'watched' by webradio, they no longer mind that this affects their personal lives, and it will not be regarded as reasonable anymore to expect privacy when listening to the radio.

5.2.5 A Contextual-Functional Perspective

We have discussed some ways of looking at privacy, both from a theoretical and from a legal point of view. One of its central characteristics, also emerging from the example of webcasting, is the notion of reasonable expectations or the balancing test. This indicates that privacy is a living, continually changing thing, a fluid concept, dependent on socio-cultural factors. With respect to these socio-cultural factors, Whitman (2004) writes 'What must be hidden before the eyes of others, seems to differ from society to society'. In a recent paper, he discusses two western cultures of privacy. He describes the European culture on the one hand, which has the protection of a right to respect and personal dignity at its core. The continental European privacy rights are rights to one's image, name and reputation, and what the Germans call the right to

¹² Etzioni (1999, p. 12) proposes a test for determining whether privacy and the common good are out of balance. Privacy should only be limited if society is threatened by a well-documented and macroscopic threat. If this test is passed, one should consider if these threats can be countered without first resorting to measures that might restrict privacy. The measures introduced should be minimally intrusive, and measures that treat undesirable side-effects of needed privacy-diminishing measures are to be preferred over those that ignore these effects. Privacy-diminishing measures in Etzioni's view should therefore be *necessary*, which resembles the European continental notion of finality, they should be in accordance with the subsidiarity principle (as a last resort), and proportional (minimally intrusive).

informational self-determination (Whitman 2004). At the other hand he places the U.S. tradition, which is oriented toward 'values of liberty, and especially liberty over against the state'. This is in line with the traditional American pre-occupation with fear for intrusions by the state, especially in one's own home.

Not only between societies is there a difference in what is deemed suitable for protection under the guise of privacy, but the concept also changes over time (for an extensive overview see Moore 1984). Societal changes such as changing attitudes with respect to moral standards with respect to clothing and behaviour are well described (e.g. Westin 1967). Also, the impact of ICT on the concept of privacy is given ample consideration in research.

The past decades have shown tempestuous developments in the fields of ICT. It has almost become commonplace to assert that these developments have had a tremendous influence on policymaking, regulation and legislation with regard to privacy. But other factors have been important as well. First of all, the exponential growth of ICT applications was situated in an eventful socio-economic context. In many countries, a new demarcation of the private and public sectors of society has taken place, a process that is still going on. The privatization and semi-privatization of formerly public or semi-public institutions have changed ideas about the permissibility of all kinds of ways in which personal data are used. Second, the past decades have witnessed a growing internationalisation, not to say globalisation, of what were formerly merely local or national activities. This has sharpened the exchange of different views on and usages of privacy, for instance, between Europe and the United States. All of these factors – technological developments, socio-economic changes, the fading importance of national boundaries – have influenced the regulation of privacy, and they have contributed to changes in the meaning and significance that are assigned to privacy, both by ordinary citizens and by legislatures and policy makers.

In turn, this increasing attention of legislatures and policy makers for privacy itself has led to structural changes in the meaning of privacy. Law and regulation, through their authoritative status, have had a steering and enshrining effect on the meaning of privacy and the privacy discourse.

Hence, '[p]rivacy is a conventional concept. What is considered private is socially or culturally defined. It varies from context to context, it is dynamic, and it is quite possible that no single example can be found of something which is considered private in every culture' (Johnson 1989).

This raises the question how it is possible to evaluate the possible influence of 'code' on this fluid notion of privacy. Some authors, such as Johnson (1989) and Vedder (2000), have proposed to use a contextual-functional framework that does justice to the influence of contextual factors and – at the same time – enables us to understand how the notion of privacy can retain a certain unity in spite of all the changes and extensions that it displays. Vedder, building on Johnson, uses 'privacy as immunity from judgements of others' as the descriptive frame for the concept of privacy, with the exception of decisional privacy. This concept is a common denominator of many privacy conceptions.

With respect to the normative point of privacy and the normative evaluation of privacy, the situation is more complex. One might say that privacy is not an end, but merely a means to achieving other goals (Bygrave 2002; Cate 1997). It is debated in literature as to which goals

qualify in this respect. For instance, Johnson (1989) proposes 'personal freedom'; Benn (1988) puts forward a limited set of subdimensions of freedom: the freedom of self presentation and moral autonomy.

Vedder (2000) rejects these monistic underlying values and instead proposes that we look at particular contexts to denote the functions and values of privacy in these contexts. In his view, privacy is an instrumental value that can serve the fulfilment of various other values, and it depends on the context just which value privacy enhances. In other words, privacy serves multiple functions, one or more of which are relevant in a particular situation.

We agree with Vedder that it is most fruitful to look at specific contexts in order to show just what privacy means in that context. We will therefore look at various fields in which privacy-related 'code' is at work, in order to analyse how 'code' affects the balance between privacy and other interests.

In order to be able to denote what underlying values and functions privacy in those particular contexts may serve, we shall outline some potential candidates.

There is much literature on the values and interests served by privacy. For our purpose we do not need an extensive overview, but instead start with the set that Westin (1967) provides, as this covers a broad area and is still seen as an important basis (Bygrave 2002). The values served by privacy can be distinguished in values for the individual and values for society. Core individual values are: individuality, autonomy, dignity, integrity, emotional release, self-evaluation, and inter-personal relationships. *Individuality* reflects the fact that we want to see ourselves as individual persons and the protection of individuality means a protection against flattening out, or becoming one-dimensional. Profiling is a technology that touches upon this sense of individuality. *Autonomy* is related to individuality; it is a person's ability to make his own choices. *Dignity* is a third important value, relating to the right to be shielded against unwanted public exposure – to be spared embarrassment or humiliation. Whitman (2004) even calls dignity the core of privacy in the continental tradition. Associated with both dignity and the other previously discussed values is *integrity*, or the right to be taken as a whole.

Emotional release, or the release from public roles, provides an individual with an opportunity to be out of the public eye, to retreat from public role-playing and be 'herself'. *Self-evaluation* relates to the time and space an individual needs to process the information she constantly gets into a meaningful whole and to reflect on herself and her position in the world. The final value of individual privacy according to Westin is the opportunity it provides for limited and *protected communication*. Westin calls this set the values concerned more or less with 'achieving individual goals of self-realization' (Westin 1967, p. 39).

As for society, privacy protection also has a significant relevance for society as a whole. Here, civility, stability, pluralism, and democracy are the values that benefit from privacy protection.

The protection of one's private sphere has individual and societal benefits. Giving up (part of) one's private sphere can also have benefits for the individual and society. Walker (2000) discusses some of the advantages of sharing personal information. He mentions cost, access, convenience, collaboration, community, security, responsibility, and trust. Some of these factors relate to the fact that private enterprises aim at profiling customers and value direct marketing as

it may lower their cost of doing business. In return, they offer discounts and special services to loyal customers. Convenience is a benefit, as services can be tailored to particular users or clients and the interaction can be made more personal, which obviously is valued by some people. Collaboration is important in Walker's view, in the sense that some services can only be offered if sufficient numbers of collaborators exist. Telephone books only have value if a sufficient number of telephone subscribers are listed. By community, Walker refers to a need for people to engage in public discussions, and he argues that people have a need to know the others, referring to the Cheers opening song, "You want to go where everybody knows your name". The last benefit of sharing personal information seems to stem from an idea that anonymous interaction in cyberspace (and in meatspace), facilitates 'wrongs', and that these can be prevented if people do not interact anonymously.

Now, with these numerous potential values and functions of privacy in mind, we proceed to analyse how 'code' affects privacy in various contexts.

5.3 'Code' and Privacy in Context

What do we mean by 'code' & privacy? The relationship between 'code' & intellectual property is relatively clear.¹³ For instance, code embedded in media players makes people conform to the rules put forward by the designer of the media player, who no doubt has implemented these in accordance with the wishes of the rights-holders of the media to be played by the player. 'Code' in this context precludes violations and automates the enforcement of public decisions (Reidenberg 2004).

The relationship between 'code' and privacy, however, is less clear. Obviously, technology may affect privacy. Technology facilitates monitoring and surveillance, and enormous amounts of personal data can be collected and processed, thus affecting information privacy. But can 'code' with respect to privacy play a role similar to that in the context of intellectual property, as in Digital Rights Management (DRM) systems? It can. But there is a discrepancy. Whereas one might see 'code' as a threat to privacy, the opposite is the case if we take the 'code & intellectual property' situation as a guide. 'Code' can be used to prevent actors and organizations to breach privacy, just as 'code' precludes violations of copyright law through DRM systems. Privacy protecting rules can be hardwired within the infrastructure of the Internet and applications. An example of this kind of embedding policy in code can be seen in the changes Microsoft made to their ".Net Passport" service as a result of the objections raised to the original design by the Article 29 Working Party.¹⁴ Microsoft built the European data privacy protections directly into the company's technology (Reidenberg 2004).¹⁵

But this notion of 'code' & privacy runs counter to what we actually perceive. Technology in many ways threatens privacy. If we take 'code' to indicate technology in a broad sense, then 'code' by itself is often privacy-threatening in the sense that it can usually be used to invade

¹³ See the chapter on 'code' and intellectual property by Natali Helberger.

¹⁴ The Article 29 Working Party is the consortium of the European data-protection supervisory authorities that monitors compliance with EU data-protection regulation.

¹⁵ See, for instance, <http://www.informationweek.com/showArticle.jhtml?articleID=6512119>.

people's privacy. Taken specifically, however, as rules built into technology, 'code' can be seen as providing at least as much privacy enhancement as privacy threats.

In fact, Lessig, in our view, appears to mix 'code' and code in his chapter on privacy. Were he writes that code has already upset the traditional privacy balance (Lessig 1999, p. 142), he uses the term 'code' not to denote code in a normative sense, but in the neutral sense as software code, or more generally to indicate a vague notion of technology. But when he states that code could re-create something of the traditional balance, he means 'code' in the normative sense of 'code' as regulation. Taken more loosely together, as Lessig seems to be doing (see e.g. Lessig 1999, p. 6), 'code' embeds certain values, and the central questions are: what, and whose, values are embedded?

In our view, it is useful to distinguish between these two uses of the term 'code'. For the purposes of this chapter, both are relevant. In fact, the obvious starting point seems to be the first meaning: code as technology in general, which is usually – if not always – more privacy-threatening than privacy-friendly by its nature (see section 5.4). But since privacy is all about balance, the other meaning of built-in rules comes in usefully: privacy-enhancing technologies (PETs) can be a solution to re-establishing disturbed balances. In the analysis of various domains in which the privacy balance may be shifting, we shall therefore start with a general notion of technology influencing privacy, and then specifically indicate whether and how privacy-protecting norms could be built-in in technology as a possible part of addressing potential shifts in protection.

5.3.1 Law Enforcement

As of old, law enforcement is one of the prime contenders in privacy debates. By its nature, law enforcement should uncover what is hidden and what people like to keep hidden. The natural tendency to safeguard the interest of law enforcement therefore is to create investigation powers that uncover hidden things, if necessary by force. Constitutional protection against (over)intrusive searches and other kinds of prying into people's lives is one of the most important areas in which we see privacy at work. And although people may easily say they 'have nothing to hide', thus suggesting that the police should be given ample room for crime investigation, most of these would still protest when the police installs a camera in their bedroom to monitor marital murders. Privacy in the sense of protection from government intrusion into the private sphere of its citizens is still very much an issue.

The context of law enforcement is also one of the prime areas in which 'code' affects privacy. Two major developments in technology have swayed the traditional balance of law enforcement and privacy over the past decades.

The first is the advent of new surveillance technologies. Technologies like transaction monitoring and location monitoring through tiny beacons or mobile telephony, directional microphones, hacking, and merging public and forensic databases are already sufficiently developed to be used to great advantage for law enforcement. In the near future, advanced video surveillance with face recognition, aerial photography, automated speech recognition and voice recognition, and spyware may add to law-enforcement's intrusion potential. Still somewhat further ahead looms the use of technologies like RFID, ambient intelligence, and 'smart dust' that may enable

systematic, covert, and perfect tracking and observing of people into the most detailed aspects of their personal lives. Most of these technologies enable not only reactive searching, but also proactive monitoring to detect criminals on the verge of committing a crime.

The second development is equally important, but less obvious. More and more areas of people's lives are being digitised, and on-line methods replace off-line methods of doing things, in communication, banking, shopping, education, photography, archiving, et cetera. This means that an ever-increasing amount of data about personal life is digitised and stored somewhere. In turn, this enables law enforcement to gather many more data with 'on-line' powers than used to be available to them with the matching 'off-line' powers.

In order to illustrate how these developments work in practice, we will sketch three examples that show various ways in which 'code' functions in the law-enforcement context.

Case 1: Interceptability of Telecommunications

The interception of telecommunications has always been an important tool for law enforcement. With the growth of telecommunications, this importance has only increased – interception is one of the most vital tools for investigating and prosecuting crime nowadays.

With the developments in telecommunications that took place in the 1990s, however, it increasingly seemed that the police could no longer rely on the plain old telephone system for its interception. New technologies, infrastructures and services, such as mobile telephony, packet-switched communications, and call-forwarding, were not necessarily as easy to intercept technically. Therefore, governments decided to establish regulations that demanded the telecoms industry to build into their technology a wiretap capability, thus making sure that it was at least technically feasible for law enforcement to continue to intercept, regardless of further technological developments.

In the United States, the Communications Assistance for Law Enforcement Act of 1994 (CALEA) was passed in October 1994.¹⁶ The purpose of CALEA is “to preserve the ability of law enforcement to conduct electronic surveillance in the face of rapid advances in telecommunications technology”.¹⁷ It requires telecommunications carriers to ensure that their equipment, facilities, and services are capable of, among other things, enabling the government to intercept communications content and to access call-identifying information (47 U.S.C. § 1002 (a)). Moreover, the law also demands a certain number of simultaneously interceptable lines (47 U.S.C. § 1003) – a provision that led to fierce debates when the Federal Communications Commission made proposals to implement this. The law provides a 'safe harbour' for telecom carriers if they comply with publicly available technical requirements or standards adopted by an industry association or standard-setting organisation (47 U.S.C. § 1006).¹⁸ And, in turn, manufacturers of telecommunications equipment and providers of support services are required to make available to telecom carriers equipment and services that comply with the interceptability requirements (47 U.S.C. § 1005(b)).

¹⁶ Pub. L. No. 103-414, 108 Stat. 4279, available at <<http://www.askcalea.net/>>.

¹⁷ <<http://www.askcalea.net/faqs.html#05>>.

¹⁸ See <<http://www.askcalea.net/standards.html>> for an overview of available standards. Although “publicly available”, the standards are not cheap: e.g., it costs USD352 to download standard J-STD-025-B-2003, <https://www.atis.org/atis/docstore/doc_display.asp?ID=2570>.

Pursuant to CALEA, the telecom industry has developed and is still developing technical standards for interceptability. For instance, a subcommittee of the Telecommunications Industry Association (TIA), together with a committee of the Alliance for Telecommunications Industry Solutions, has developed an interim standard, J-STD-025, that should meet the CALEA requirements. Since the FCC found the standard deficient in some respects, it added more requirements (a ‘punch list’), e.g., to identify the active parties of a multiparty call, and to provide all signals, such as the use of feature keys, available from the subject.

Telecom manufacturers have also been active: the “FBI has signed agreements with AG Communications Systems, Lucent Technologies, Motorola, Nortel Networks, and Siemens AG for technical solutions developed to meet the assistance capability requirements of CALEA.”¹⁹

The United States has not been the only country to pass legislation on interceptability. Indeed, the European Union quickly followed the U.S. with a Council Resolution of 17 January 1995, which outlined quite similar requirements for interceptability.²⁰ Arguing that “interception may only be effected insofar as the necessary technical provisions have been made”, the resolution listed the a summary of the needs of law enforcement “for the technical implementation of legally authorized interception in modern telecommunications systems”. Subsequently, the member states carried out the resolution by passing laws similar to CALEA.

The relationship with industry and standard-setting bodies was less direct – or more covert – in Europe than in the U.S. An EU body did send a letter to international standardisation organisations (IEC, ISO, and ITU) in December 1995, pointing out the resolution and “inviting” to take account of the requirements,²¹ but the EU resolution nor the national implementation laws do not explicitly refer to standard-setting bodies, nor do they require telecom manufacturers to develop interceptable equipment. Apparently, it was left more to industry itself – both telecom providers and manufacturers – to develop and incorporate interceptable equipment and services.

Although several industry and standardisation bodies, such as the U.S. TIA and ATI and the European ETSI, have been working on incorporating interception norms in the technology, other bodies have consciously refrained from doing so. It is instructive to read the statement of the Internet Engineering Task Force (IETF) on their wiretap policy, which explains why the IETF decided not to consider interception requirements as part of their standard-developing work.²² Apart from considering that building-in interception capability will make the network considerably more complex and hence more vulnerable, it also argues that IETF standards relate to cross-border communications that pass numerous jurisdictions with numerous, and diverging, requirements for privacy. Building-in a uniform privacy-infringing option would therefore not be a Good Thing; rather, national bodies should develop the standards according to their own jurisdiction regime. This is a rather odd argument for a body like the IETF, since the Internet by

¹⁹ <<http://www.askcalea.net/faqs.html#14>>.

²⁰ Council Resolution of 17 January 1995 on the lawful interception of telecommunications (96/C 329/01), OJ 4 November 1996.

²¹ Statewatch, *European Union and FBI launch global surveillance system*, February 1997, <http://www.privacyinternational.org/issues/tapping/statewatch_tap_297.html>.

²² RFC 2804, May 2000, endorsed by the Internet Architecture Board and Internet Engineering Steering Group, <<http://www.ietf.org/rfc/rfc2804.txt>>.

its nature can hardly cope with diverging national technical standards. Perhaps the real reason why the IETF did not want to develop interceptability is their fear for abuse: “Experience shows that tools designed for one purpose that are effective for another tend to be used for that other purpose too, no matter what its designers intended. (...) What this boils down to is that if effective tools for wiretapping exist, it is likely that they will be used as designed, for purposes legal in their jurisdiction, and also in ways they were not intended for, in ways that are not legal in that jurisdiction. When weighing the development or deployment of such tools, this should be borne in mind.” In other words, the IETF has refrained from building-in a specific option for interceptability, partly because such ‘code’ may not meet the privacy laws of certain countries and also because the technology can be abused to infringe privacy in ways unintended by the designers.

The case of interceptability of telecommunications shows that governments have passed legislation that requires technology providers to build in certain features related to legal norms, in this case, the feasibility of the investigation power of interception. Industry has – naturally – complied with these legal requirements, and hence, telecommunications infrastructures have a built-in capacity for interception, and they have included more detailed interception features according to the requirements set by governments. This is not to say that telecom technology is inherently privacy-infringing, but it is thus at least capable of being privacy-infringing. Perhaps because of the IETF’s concern with resulting vulnerabilities and privacy risks, the privacy-threatening ‘code’ has not been incorporated in the lower levels of the Internet architecture – telecom providers use software and hardware add-ons to ensure interceptability. This allows for national differentiation. At the same time, however, this has also created less transparency, since – as opposed to Internet standards – interceptability technologies and their use are kept rather obscure. The U.S. debates over the Carnivore system, which allows interception of packet-switched communications, illustrate the tendency of governments not to publish details about law-enforcement-related technologies.²³

Case 2: Location Data

-mobile telephony: cell data and detailed location techniques

-9-1-1 emergencies: mandatory location data

-location-based services

-briefly refer to GPS in cars

-briefly refer to RFID

-conclusion: technology enables increasing, systematic and covert localisation of individuals; law enforcement joins in and profits from this; not unlikely that this will be reinforced by legal requirements for investigation purposes; privacy shift is significant, since localisation is possible on a much wider scale, and post ipso facto (particularly with mandatory data retention)

²³ See, e.g., EPIC’s FOIA activities at <<http://www.epic.org/privacy/carnivore/>>.

Case 3: Cryptography

'Cryptography' indicates systems that alter data so that unauthorized people cannot access them. It is, essentially, a privacy-enhancing technology, since it can protect the secrecy of communications and of stored data. In the 1970s, cryptography saw two developments that were to be of great significance to the development of the information age. First, the U.S. developed the Data Encryption Standard (DES), an automated crypto system. This was based on traditional cryptographic methods, but DES was so well designed that it proved to be uncrackable even by supercomputers until the mid-1990s. After DES, several similar systems were devised that proved to be equally strong, or stronger still through the use of longer keys.

Second, and even more important, public-key cryptography was invented, a system in which people no longer share a single key to encode and decode a message; instead, each person has a key pair with a public and a private key. Through public-key cryptography, people can communicate without having to exchange a key through a secure channel. You can send someone your public key in an e-mail message, with which she can send you a message that only you can read, and even if someone eavesdropped and knows the *encoding* key, he is none the wiser because he does not know the *decoding* key.

Until the 1970s, most crypto systems could be cracked. Of course, some were stronger than others, such as the coding machines used in the Second World War, but all turned out to be crackable in the end, if enough effort was put into it. But the new generation of crypto systems that emerged in the 1970s has turned out to be virtually uncrackable, no matter how much effort you take. (This is in theory, at least; in practice, implementations and use of secure crypto systems often turn out to have flaws.) It is a matter of computing power: to crack a message, you have to try every possible key, and it takes literally ages before you are likely to find the right one. Naturally computers get stronger every day, but it is easy to encode with a slightly longer key to more than compensate for this. Compared with traditional codes, then, modern automated codes are more or less uncrackable. It is a difference of degree, not a fundamental difference, but the difference of degree is so big that it has indeed altered the field.

The difference between the old and new cryptographic 'code' has created a controversy that only recently seems to have calmed down into a status quo. Governments traditionally have not worried much that people could use cryptography; only the government knew the most sophisticated coding schemes, and what people encoded, the government could usually decode. With modern cryptography, that is no longer the case. People can use robust cryptography and the police – in theory – stands empty-handed: wiretaps and computer searches are useless if all they find is code.

The controversy this has created is twofold, related to two different roles of government: protecting national security and enforcing the law.²⁴ The first – cryptography hampering national security – is mainly concerned with crypto use by *foreigners*, and this has given rise to export controls in many countries. During the Cold War, agreements were made within the Coordinating Committee for Multilateral Export Controls (COCOM) to curb the export of cryptography. In 1995,

²⁴ See Koops (2004) for an overview of states' initiatives in crypto legislation. The examples that follow can be found, with references, on this website.

this was followed up by the Wassenaar Arrangement, an international (non-binding) instrument of 33 countries that regulates the export of weapons and dual-use goods (that is, goods that have both a military and a civil application); cryptography is such a dual-use good. The thrust of the arrangement is to allow only export of weak (easily crackable) cryptography and to require licenses for export of strong cryptography. As the 1990s evolved, the controls were increasingly controversial, especially in the U.S., since they hampered electronic commerce and were practically unenforceable, given that strong crypto programs could be downloaded from many places on the Internet. After several relaxations, in the U.S. and in the Wassenaar regulations, the controversy seems to have calmed down in the new millennium; apparently, the licensing procedures are sufficiently smooth nowadays not to really obstruct international (e-)commerce anymore. Of course, the effectiveness of remaining export controls is low: if foreign crooks and criminals want to obtain strong cryptography, they can download reliable and free programs from various countries through the Internet.

The second part of the controversy, related to *domestic* crypto use, is more complex. It was only in the early 1990s that governments realized that law enforcement could be seriously hampered by cryptography.²⁵ Conceptually, there are two possible solutions to address this. You can either create mechanisms that ensure that the government has access to decoding keys *beforehand*, e.g., by having people deposit keys somewhere when they want to use cryptography, or by mechanisms that ensure access to keys *afterwards*, e.g., by a legal power that enables the police to force someone to give a decryption key in case of a crime.

The U.S. government was one of the first to try the first approach. In 1993, they launched the Clipper chip, a chip for telephone encryption with a built-in backdoor for government access.²⁶ They hoped that if enough people would voluntarily use this chip, the crypto problem would remain manageable (the police would simply notice when someone used non-Clipper encryption, and this would be interesting information in itself).

The U.S. were not the only country to try to curb cryptography's progress. In the Netherlands, in 1994, a draft law was considered to virtually ban crypto use, except for those who would be lucky enough to get a license; after large public outcry, the idea was hastily abandoned. Still, the Dutch government for a long time afterwards thought of schemes that resembled the Clipper chip. If Trusted Third Parties (TTPs) offer confidentiality services (e.g., to provide customers with crypto keys for encoding data), they might be forced to facilitate "legal access". In a "partnership approach" of government and industry, a project on Legal Access (*Rechtmatige toegang*) was established, which was to make sure the government could have access to crypto keys without

²⁵ It must be remarked here that this still appears to be a mainly theoretical problem. There still is not really a law-enforcement problem with cryptography (yet), even though it has been predicted ever since 1993 that law enforcement would soon become a joke because of cryptography. So far, few criminal cases appear to have been blocked by cryptography. Few public data are available; Denning & Baugh have researched numerous crypto cases related to searches, the majority of which were not stopped by encryption. The *2002 Wiretap Report* of the U.S. Courts mentions that 'Encryption was reported to have been encountered in 16 wiretaps terminated in 2002 (...); however, in none of these cases was encryption reported to have prevented law enforcement officials from obtaining the plain text of communications intercepted', <<http://www.uscourts.gov/wiretap02/2002wt.txt>>. Our impression is that only since one or two years, at least in the Netherlands, does the police really encounter encryption that cannot easily be cracked in any significant number of cases. Perhaps, in the future, crypto use by criminals may therefore indeed become a real-life problem.

²⁶ Many documents concerning Clipper and its aftermath can be found in Hoffman (1995) and Schneier & Banisar (1997).

obstructing industry too much. The outcome of the project, however, was that an economic-effect analysis showed that mandatory “legal access” is not economically feasible, since in that case, TTPs will move abroad; hence, the government refrained from further steps in this direction.

Similar developments took place in the UK, where the government launched one consultation document after the other with proposals for government backdoor access to encoded data. First, such systems were proposed to be mandatory, but later, the government said they could be voluntary.²⁷ In Germany, part of the government also favoured an approach of mandatory backdoor-access schemes, but other government parts opposed this.²⁸ France, which was the only country in the Western world that had had strong domestic controls on cryptography at all, actually enacted a law in 1996 to regulate backdoor access: if people deposited their crypto keys with a government agency, they could get a license for strong cryptography.²⁹

Interestingly enough, governments were not the only ones to think about and devise backdoor schemes. Cryptographers themselves were active in the field, researching ways to build into the technology backdoor government access, or, alternatively, ways to circumvent backdoor access in schemes devised by others. For example, a study group from Royal Holloway University, London, developed a key-escrow scheme for international communications that would allow national government authorities to decrypt without having to resort to mutual assistance by the foreign country. They also included options for sophisticating their scheme: splitting keys to distribute among several TTPs, and changing keys regularly, so that, e.g., time limits on wiretap warrants might be technically enforced.³⁰

The extent to which cryptographers went to try and incorporate norms into technology, can be illustrated by a paper by Bellare and Rivest. They apparently considered it a problem that there is no middle way between wiretapping (which overhears all conversations) and not wiretapping (which overhears none). To provide such a middle way, Bellare and Rivest proposed ‘translucent cryptography’.³¹ This is not opaque, in that encrypted communications are entirely unreadable for law enforcement, nor is it transparent, which means that law enforcement cannot read everything they intercept either. Rather, the system allows law enforcement to read a fraction p of encrypted intercepts – where p is a number between 0 and 1. The amount of translucency, in their proposal, is to be established by parliament. This fraction p could vary with applications; for instance, whereas for domestic communications, parliament might set p equal to 0.2 (allowing a relatively high level of privacy), they might require p to be 1 for international communications, or at least for communications with rogue states. Parliament could decide to change the fraction if the situation changes significantly, either because some terrible crimes involving cryptography have happened, or because elections were held and parties have promised their voters to set p to a particular value. This, at least, is the world view emerging from the technical paper. The point of this example is not that it is a realistic proposal, but that it shows the extent to which

²⁷ Department of Trade and Industry, *Paper on regulatory intent concerning use of encryption on public networks*, June 1996; *Licensing of Trusted Third Parties for the Provision of Encryption Services*, March 1997; *Building Confidence in Electronic Commerce*, March 1999.

²⁸ See a summary on Koops (2004) and several documents on <<http://www.kuner.com/data/crypto/crypto.html>>.

²⁹ *Loi no 96-659 du 26 juillet 1996 de réglementation des télécommunications*, *Journal Officiel* 27 July 1996.

³⁰ Jefferies et al. 1996.

³¹ Bellare and Rivest 1996.

some code developers go to devise code that can incorporate norms – in this case, norms to be set by parliament.

Nevertheless, however much governments and cryptographers may have thought they could solve the problem of criminal crypto use with this approach, it all came to nothing. By the late 1990s, backdoor-access schemes were out: Clipper had died a silent death,³² the Dutch, UK, and German governments thought better of it, and France abandoned the 1996 law and liberalised crypto use in 1999³³. There were several reasons for this. U.S. citizens did not trust the government with backdoor access, and even the U.S. government itself failed to use the Clipper chip. Technically, the backdoor schemes were tricky, not having proved themselves secure enough to be considered reliable. Most importantly, the schemes would not serve their purpose of preventing criminals to use encryption: serious and organized criminals would always have easy access to non-backdoor cryptography, and if necessary, they could use superencryption (first encrypt with a private, uncrackable system, then encrypt with the government backdoor system) to escape notice. And even if non-backdoor crypto were outlawed, few criminals would mind; they would just break another law (and one that was hardly enforceable anyway). With corporate and non-habitual criminals, the backdoor schemes might have had some effect, but for the kinds of criminals that the governments really wanted to target, the backdoor schemes were ineffective.

Then what? In recent years, many governments have chosen the second approach. They have enacted laws that allow the police to command people to decrypt or to hand over their crypto keys. The Netherlands was the first to do so, in 1993.³⁴ More recently, the UK, Belgium, France, and a host of other countries have followed.³⁵ Thus, instead of relying on ‘code’ to incorporate law-enforcement access, they have settled for a merely legal solution in the form of an investigation power: if the police encounter encoded data, they can command decryption. The upshot is that cryptography is and remains a privacy-enhancing technology, which citizens can use to protect themselves against governments. It does not appear to be in very wide use, however: it is built-in in numerous software and infrastructure elements, but end users rarely use encryption themselves. The lack of use may be explained partly by the – perceived – difficulty of the technology, but also partly by the government campaigns of the 1990s against cryptography, not least by the export controls that effectively hampered law-abiding citizens and businesses to adopt strong cryptography on a large scale. Regulation in this case seems to have had an impact, not – as in the case of interceptability – on technology itself, but on the *use* of a privacy-enhancing ‘code’.

³² O’Hara and Harreld 1997.

³³ *Décret no 99-200 du 17 mars 1999 définissant les catégories de moyens et de prestations de cryptologie dispensées de toute formalité préalable; Décret no 99-199 du 17 mars 1999 définissant les catégories de moyens et de prestations de cryptologie pour lesquelles la procédure de déclaration préalable est substituée à celle d’autorisation.*

³⁴ Article 125k para. 2 Dutch Code of Criminal Procedure, inserted by the *Wet computercriminaliteit*, *Staatsblad* 1993, 33.

³⁵ Part III of the UK *Regulation of Investigatory Powers Act 2000*; article 88quater Belgian Code of Criminal Procedure (*Wet van 28 november 2000 inzake informaticacriminaliteit / Loi du 28 Novembre relative à la criminalité informatique*, *Staatsblad / Moniteur Belge* 2001 – 298); title IV French Code of Criminal Procedure (*Loi no 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne*). See further, e.g., the entries on Australia, Ireland, Trinidad & Tobago, India, Malaysia, and Singapore in Koops 2004; the latter three have only limited scope.

Balance

Technology appears to be a key driver in enabling law enforcement to pry deeper into the personal sphere, often invisibly from a safe distance. The balance with privacy of new investigation powers is supposedly made time and again by the legislature and the courts, but because technology is developing, so does the reasonable expectation of privacy surrounding this technology. After all, there is less expectation of privacy when surfing the Internet than when watching television in your home, or when walking streets that have clearly visible 24-hour camera surveillance. The case of location data suggests that somewhere in the perhaps not too far-away future, people's movements may also lose the reasonableness of privacy expectations, since localisation is becoming an increasingly common side-effect of technology.

It may therefore be argued that 'code' is changing the traditional balance of privacy and law enforcement. This regards all kinds of domains: in the physical sphere, privacy is threatened as the home becomes intelligent and connected to the Internet through domotics, and as electronic monitoring allows the police to see through walls and curtains. Relational privacy is put under pressure as personal relationships depend vitally on telecommunications that may be wiretapped but that may also be sweepingly monitored with speech and voice recognition, and that are increasingly being subjected to data retention. And informational privacy is disappearing when the police can request all electronically processed data on any subject from any data processor, and can merge databases to find hidden patterns and connections.

However, it should be observed that this development is not caused so much by 'code', i.e., technology with explicit privacy-infringing features built-in, as by technology in general. Privacy infringement happens to be a side-effect of technology development per se. The case of interceptability is an exception in this respect; it seems the only example in the list of developments sketched above that consciously built-in 'privacy infringement'. Still, conscious or not, the effect on privacy is practically the same: slow erosion.

Does 'code' do something about this shifting balance itself? That is, are privacy-enhancing technologies somehow counterbalancing the privacy-threatening technologies in this field? To some extent, that may be the case. Cryptography is a prime example of a technology that enables people to keep communications and written thoughts hidden from government surveillance. Steganography may also hide the fact of communication itself: post a picture of a red Toyota to a newsgroup with a message hidden in it that only your partner in crime will recognise. Anonymisers enable Internet activities with less chance of being traced. Sunglasses will help to thwart face recognition, and a Faraday cage will make your home an impenetrable castle for electronic spies. Many examples like these can be given of technologies that help to counteract invasive technologies.

Nevertheless, our impression is that the privacy-threatening code is more developed and in wider use than the privacy-enhancing code. One of the reasons for this is that citizens are responsible themselves to use protective technologies, and they usually have no reason – and often not the knowledge and awareness – to put themselves to considerable costs and effort to build a technological shield against government intrusion. Law enforcement, on the other hand, has a major incentive to use the intrusive technologies, and this may explain why privacy-

threatening technologies are developed sooner and used more widely than privacy-enhancing technologies.

Of the examples given, only cryptography seems a PET that has really gained a definite foothold, if not with the general public, than at least with technology-aware citizens and criminals. But as the case of cryptography shows, governments have not been really happy with privacy technologies, precisely for the reason that they hamper law enforcement. And although crypto-curbing laws and proposals seem to have died a slow death, as soon as a high-profile child murder or terrorist case emerges in which cryptography blocks finding the culprit, legislatures may be quick to yield to the pressure of law enforcement and pass a law that intends to restrict the use of cryptography. This is not to say that legislatures will not consider the balance between privacy and law enforcement in such a case, but it suggests that the interest of law enforcement is often considered so important that privacy-friendly technologies will not be readily supported by governments, even if they do not outlaw them in a single sweep of legislative zeal prompted by a high-profile incident. The bottom-line seems to be that law enforcement always trumps privacy.

5.3.2 National Security

The interest of national security is closely related to that of law enforcement, and we therefore refrain from giving specific cases here. Nevertheless, there is one significant difference worth mentioning. Protecting national security is by its nature closely intertwined with secrecy and stealth. Investigation by security agencies is never as overt as law enforcement may be; it thrives only on covert intrusion techniques. This makes privacy-threatening 'code' all the more relevant to the field of national security: it is precisely covert surveillance that has received a boost through the technology development over the past decades. Global eavesdropping on an unprecedented scale through Echelon, satellite photography that – in military applications – will soon become sophisticated enough to notice intimate details of individuals on earth (e.g., sunbathers on a deserted stretch of beach), thermal imagers, and 'smart dust'³⁶ are but a few examples of the increased potential for covert intelligence.

And there is more. In the case of cryptography discussed in the previous section, we asserted that cryptography has retained its foothold as a privacy-enhancing technology. But even this is not entirely true. Even here, a suspicion cannot be altogether discarded that backdoors are built in. It is true that the idea of building-in mandatory backdoors for government access has utterly failed, but this regards the protocols and standards. We can be fairly sure that crypto systems, such as the Advanced Encryption Standard, are reliable and do only what they are supposed to do, because the protocols have been published and scrutinised extensively. However, for *implementations* and concrete products, this may differ. The story of Crypto AG is disillusioning:

'For decades, the US has routinely intercepted and deciphered top secret encrypted messages of 120 countries. These nations had bought the world's most sophisticated and supposedly secure commercial encryption technology from Crypto AG, a Swiss company that staked its reputation and the security concerns of its clients on its neutrality. (...) All the while, because of a secret

³⁶ 'Smart dust' are sensor systems implemented in objects of 1 cubic millimetre, see <<http://www-bsac.eecs.berkeley.edu/~mattlast/research/index.html>>.

agreement between the National Security Agency (NSA) and Crypto AG, they might as well have been hand delivering the message to Washington. Their Crypto AG machines had been rigged so that when customers used them, the random encryption key could be automatically and clandestinely transmitted with the enciphered message. NSA analysts could read the message traffic as easily as they could the morning newspaper.³⁷

This is not to suggest that every crypto product is bugged, but the story should make us wary of trusting privacy-enhancing products at first sight.

Therefore, even more than is the case with law enforcement, 'code' is threatening the existing balance between privacy and national security interests. And since the activities and technologies of security agencies are much less published than those from law enforcement, there is even less incentive for people to protect themselves with privacy-enhancing technologies. Thus, particularly in the area of national security, 'code' favours a significant shift of the balance to the detriment of privacy, a push that can only be checked by legislatures and courts in a conscious attempt to retain privacy at a certain level. Since 9/11, however, such a conscious attempt is anathema, and national-security interests ride along with technology to diminish citizens' reasonable expectations of privacy.

5.3.3 E-Government

We started this chapter with a discussion of Bentham's Panopticon, the ultimate way of government to spy on and control their citizens. Whereas this image may be an appropriate one in the light of developments with respect to national security as described in the previous section, e-government shows us a different face of government. Here it is not so much Big Brother who monitors his citizens, but instead we are guarded and looked after by Soft Sister (Frissen 1998), although Soft Sister may turn out not to be so soft after all, as we shall see. Since the mid-1990s, governments have adopted the notion of electronic government, following the advances of e-commerce. In U.S. vice-president Al Gore's re-engineering government through IT programme (President 1993), the two hitherto deemed opposing forces, efficiency and consumerism, were connected, and they have since dominated the development of e-government. An important result of the e-government venture seems to be that improving service delivery for citizens and improving efficiency in the public sector prevail over information privacy protection (Raab 2001).

In the rise of e-government, citizens are more and more seen as customers (Seidle 1995) who deserve levels of service delivery comparable to those in the private sector. Service delivery should be simpler, more efficient, and more customer-friendly. IT, and especially the Internet, is a means to accomplish these goals. Central concepts in the e-government development are online service delivery and integrated service delivery through one-stop shops. The former allows citizens to apply for services, such as permits or grants through the internet. The latter means that problems are addressed in a holistic manner: instead of having to go from agency to agency a citizen can apply for several related services at a single location, both offline and online.

³⁷ Madsen 1999.

Government agencies, of course, keep records of their clients, as these are necessary for their daily operation. For instance, citizens on welfare receive their benefit every month and the welfare agency has to keep track of who is entitled to what amount of benefit. In fact, government as such does not exist in most countries, but instead is made up of a multitude of government agencies. Each of these has their own tasks and responsibilities, and their own records. It is safe to say that almost all records in public offices are computer databases nowadays. Information in these databases can easily be shared, and hence, information from different records may be exchanged between agencies and combined into new information. Goals of improving government efficiency and improving service delivery to citizens introduce pressure to do just that: combine information sources across agencies.

Both government and citizens benefit from this scheme at first. Citizens do so even in a double sense: efficiency gains may lead to lower taxes, and better service delivery may lead to more satisfied customers. Efficiency gains for government derive from the fact that information is entered once and reused at multiple locations. The cost of obtaining data decreases and the overall accuracy of the data can be higher than in the case of each agency collecting their own data.

The benefits for the citizen derive from the fact that once the identity of this citizen is known to the wired government, the various databases can be used to determine their legal position with respect to rights and obligations, at least to some extent. For instance, the entitlement to a rental benefit can be established by combining income data (available to the tax authorities) with data on rent paid by the applicant (available to the housing corporation, which in some cases is a public agency, at least in the Netherlands). Information from the various government databases can therefore be used to pre-populate (online) forms or even to make decisions on the basis of this information without intervention of the citizen altogether. This latter type of service delivery is called pro-active service delivery (BZK 2000) and shows precisely what is meant by the softer sister concept mentioned earlier: government taking active care of their citizens by combining the available information on citizens and to determine their rights (and obligations) and taking action on these without waiting for the citizens to call for these actions. This paternalistic notion may appeal to some and is part of government policy in at least some countries, such as the Netherlands.

Although citizens may benefit from the fact that they only have to provide a limited amount of information, or no information at all, to receive particular services, there is a downside to this, related to informational privacy. The threats are caused by the fact that access to information in the various government databases becomes easier as a result of the e-government developments. Access to information in databases can be provided on the basis of many attributes associated to a person (e.g., name or address). In practice, however, identification numbers are frequently used for this purpose. A reason for using identification numbers instead of, for instance, one's name, is that they are concise and do not have variants. Names and addresses can be written in many different ways; this is not only the case with 'foreign' names containing diacritics, but also ordinary names give rise to different spellings: omission of middle initials, additions to names, maiden names, et cetera. The advantage of using identification numbers is even bigger when data sources have to be combined. Here the process of matching

of records in the various tables on the basis of names and/or addresses produces many mismatches and non-matches due to the variations.

A consequence is that there is a tendency to use a single unique identification number for a large variety, if not all government databases. This tendency can be illustrated by recent developments in the Dutch medical sector. In 2002, the Dutch Data Protection Authority (College Bescherming Persoonsgegevens) issued a policy paper arguing for the use of sectoral unique identification numbers instead of a single identification number for all government databases (Vermissen and De Heij 2002). This scheme allows for inherently better data protection than the use of a single identification number, since it prevents unnecessary merging of data bases. The policy has in principle been embraced by the Dutch government (Koninkrijksrelaties 2002), and the medical sector advised to adopt a sectoral Care Identification Number (Zorg Identificatie Nummer, ZIN) for each citizen. However, a study on the costs this would create for health-care insurance companies and health-care providers (Brenda 2004) now seems to tilt the balance towards adopting instead the generic Citizen Service Number (BurgerServiceNummer, BSN) that is currently being developed as an overarching government ID number.³⁸ Efficiency is therefore a primary reason not to diversify identification systems. This leads to mergeability of data bases, which in turn enables 'cross-fertilisation' of services. For example, data bases on hospitalisation might be merged with other data bases in order to make profiles of people that have a high 'hospital risk'; insurance companies might subsequently use such profiles to diversify insurance costs.

Likewise, the traditional compartmenting of citizen data in government, which occurred for a large part because paper and face-to-face relationships lead to decentralised storage, is giving way to centralised (or distributed) on-line accessible data warehouses. These data collections make the naïve notion that 'the government already knows everything about its citizens', which was in fact not true in the fragmented off-line world, more and more of a reality. Interrelated government data bases allow, for instance, social-security providing agencies to see whether someone has yet to pay a speed-driving ticket, or the tax authorities to check how often someone has entered a prison to visit an inmate. This is not only a theoretical threat. At present police officers already consult vehicle registration information for personal use and social welfare employees are known to have used data for other purposes than social welfare. These malpractices relate to individual databases, but there is no reason to assume it will not happen when the data sources become even richer by cross-linking; on the contrary, the enlargement of both the data bases' scope and the people who have access to them increase the risk of 'interesting excursions' and misuse.

Although currently serious forms of 'cross-fertilising' of government services does not occur, software enables the merging of data and thus at least in theory allows the creation of new policy instruments: you receive a rental allowance only if you have paid all your fines; your monthly social-security benefit is decreased if you drive a car and have taken a plane twice in a year (thus polluting the environment more than the average citizen); and your request for a building permit is processed with priority if you have submitted your tax income in time over the past five years. There may be some citizens who appreciate such schemes, but others will feel

³⁸ <<http://www.automatiseringsgids.nl/news/default.asp?nwsId=26437>>.

threatened by government agencies knowing details of their lives that they do not need to know to do their proper job.

Undermining Privacy Through Ignorance

The privacy-threatening use of code in e-government is to a large extent the result of (perhaps too much) efficiency thinking and also of laziness. It is too easily assumed that giving access to citizen data within the government is essential to improve service delivery. The applications could be constructed in such a way that only the necessary minimum of information is revealed; for instance, for offering a housing benefit, the responsible agency need not know the income of a citizen, they only need to request the tax department to report whether or not the citizen's income is below the relevant threshold. In fact, this is one of the essential applications of the notion of PET, as it was introduced by the Dutch and Ontarian Data Protection Authorities (IPC & Registratiekamer 1995): construct technology in such a way that the minimum amount of data necessary for the specific goal is used, and shield-off all other information.

Moreover, it is usually taken for granted that the government should know the identity of the citizen to perform any task or service. Again, this is not always necessary. For example, if a neighbourhood planning committee collects comments from citizens through a website, it need not ask for identification, when a verification of residency of the respondent within the particular neighbourhood suffices. Technology can facilitate such privacy-friendly verification in numerous ways, depending on the desired level of security, from anonymous or pseudonymous smart cards with biometrics handed out by a municipality to each citizen, to merely publishing a generic access code in the local newspaper.

Indeed, biometrics is a technology that may be used in a non-identifying way, by allowing compartmented access to relevant characteristics of a person stored on a smart card. In practice, however, biometrics is usually viewed only as a technology for identification, and it is used in a privacy-threatening rather than a privacy-enhancing way.

Case 1: Merging Databases to Combat Fraud

Balance

In the public sector, there seem to be different worlds. In one world, we have policy makers concerned with modernizing government and improving service delivery. They have a difficult task of envisioning how government in the information age should look like. They have to cope with organizational inertia and uninterested citizens. They have to convince an unwilling audience that changes are necessary.

Then there are the systems designers. They cope with the complexity of realising the seemingly simple notions of one-stop shops, interrelated government, a holistic approach to public-service delivery. This has to be accomplished by connecting a multitude of systems, databases, protocols, and what have you.

In yet another world, we have the privacy protectionists, for instance the data protection authorities. Their concern is privacy protection, but not at all costs. They produce whitepapers and reports that address the relationship between public-service delivery and the need for keeping a balance between privacy-protection interests and efficiency and service-delivery

improvements (e.g., Raab 2001; Radwansky 2002; Vermissen and de Heij 2002). What they propose is maintaining a balance by implementing 'privacy by design', implementing privacy protection in code by adopting PETs and by maintaining data walls between sectors. These proposals are not unrealistic, yet they rarely seem to get through to the other worlds. How do these different worlds relate to the privacy balance? The modernisation of government, embodied in the aims to improve efficiency and service delivery, seem to prevail over privacy interests (Raab 2001). This is not so much due to the fact that these other interests necessarily prevail over, or inhibit, privacy concerns, but rather because there is little awareness or appreciation of the privacy-enhancing possibilities of technology, and the cost of implementing proper privacy-protecting 'code' is deemed too high. Policy makers and systems developers are hardly aware of the alternatives to personalised access to services.

5.3.4 Commerce

Electronic commerce is somewhat similar to e-government, in that the central idea is doing traditional things in new, electronic ways, with kindred interests of efficiency and serviceability. Added, however, are commercial interests: businesses have a significant interest in collecting data about customers, their habits, and their interests, since these can be used to target current or potential customers in a more effective, personalised way. Moreover, email addresses and profiles are increasingly being treated as commodities in themselves, leading to multiple and largely invisible streams of personal-data traffic across the world. Numerous 'code' developments facilitate this collection, use, and spread of personal data in the context of e-commerce, from having people fill in web forms with personal data, to more covert techniques such as cookies and spyware, and from merging databases with profiles to transaction monitoring to create new information.

Although the nature of such activities is nothing new compared to what happened in traditional brick-and-mortar business, the scale and ease of processing personal data have increased significantly enough to warrant the statement that the balance is tipping in the direction of commercial interests to the detriment of informational privacy. This entails various risks, such as the denying of goods or services to consumers with a 'wrong' profile, or showing higher prices on a website based on a 'high-risk' profile, or allowing only customers with a 'right' profile to pay afterwards; and this happens regardless of whether the individual in the zip-code area indeed has a low income. Moreover, personalised commercial communications may give the consumer the eerie feeling that 'this company knows everything about me'. Or consumers may feel offended when they search for something and the website shows them related goods or services (when you look for Hiroshige prints, the web page says: 'persons who bought this book also enjoy reading 'Erotic Japanese Woodcuts', showing an image of the eroticising cover). Although the privacy-related harm in such cases does not seem very great, in certain circumstances, the effects of businesses knowing more about the consumers than is necessary for particular, solicited transactions, can be grave, particularly when someone has many characteristics of uninteresting or high-risk groups and when no alternative ways are left to conduct business in a more privacy-friendly way.

In the following cases we illustrate the ways in which technology nibbles at data protection of citizens, and how sometimes, commercial uses of data are also adopted by the government.

Case 1: Transaction Monitoring in Mobile Telephony and Banking³⁹

Carrying out transactions, and especially electronic transactions, generates data. This is also true for the mobile telephony and banking industries. Mobile telephone operators, for instance, obviously need to know which number is calling which other number and for how long. They need these data in order to make the proper connections and they need these data for billing purposes. Similarly, banks need to know the account numbers of payers and payees as well as the amounts of transfers when money is transferred between accounts or when money is deposited or withdrawn. So, the main reason for collecting transaction data is the proper functioning of transaction systems themselves.

However, transaction data may also be used for purposes other than those for which they were originally collected. Suspects in a Dutch high-profile child murder case were, for instance, located in Spain following a cash withdrawal from a cash dispenser.⁴⁰

Transaction data generated during mobile phone calls or financial transactions may also be used to build profiles of the behaviour of individual customers. Since about 2000, monitoring systems have been available to do just that. Some mobile phone system operators use this type of electronic monitoring to detect theft, payment fraud, and identity fraud. The monitoring software builds and constantly updates individual customer profiles and spots when there is a marked change in someone's behavioural pattern or when someone is in default of payment. In the first situation, the change in a customer's behaviour may be an indication that the customer's mobile phone has been stolen and that the thief, or the receiver, has started using it for himself, thus creating his own individual usage pattern, which differs from the victim's pattern. In the second case, a customer will be disconnected from the service if he fails to pay in time. If however, the defaulter were to reapply and be accepted, for instance, because of the use of a false name, the monitoring system would then detect that the behavioural patterns of the 'new' customer is the same as that of a known defaulter, because the customer will ring the same phone numbers as before. Consequently, the service could then be discontinued again.

Applications of behavioural monitoring, such as fraud detection but also the detection of commercial opportunities, are also important in the financial world. Electronic monitoring is used, for instance, during customer acceptance and credit-scoring procedures. By analysing various types of data, providers of financial services can, on the one hand, assess the commercial potential of a future customer. On the other hand, data analyses can also be used to assess whether acceptance of a potential customer is likely to result in a bad debt or whether there are other grounds to reject an applicant. Additionally, behavioural monitoring is also used after applicants have been accepted. Once transactions have begun, behavioural monitoring can be used to detect behaviour that exceeds certain predefined limits, or to make profiles of the behaviour of individual customers based on the type, number, and frequency of the transactions they make, when, where, how, and with whom they make them, the sums of money involved, et

³⁹ This section is based on Schudelaro 2003, p. 228-229.

⁴⁰ <[http://rtl.nl/\(/actueel/rtlnieuws\)/components/actueel/rtlnieuws/12_december/19/buitenland/rowena.xml](http://rtl.nl/(/actueel/rtlnieuws)/components/actueel/rtlnieuws/12_december/19/buitenland/rowena.xml)>.

cetera. All of these data can be linked to names and account numbers. The data obtained through this kind of transaction monitoring is not only valuable from a risk-assessment, fraud-detection, or commercial-opportunity point of view, but it can also be valuable for law-enforcement purposes: behavioural monitoring may be used, for instance, to detect and investigate money laundering.

Thus, we see in the mobile-phone and banking sectors the emergence of monitoring as an effect of technology developing in such a way that consumer data can be merged and analysed; this enables close scrutiny of communications patterns and transaction behaviour, which is used not only for fraud-prevention and fraud-detection purposes, but also for commercial purposes. As a side-effect, the government may step in and use the monitoring capability that has emerged in the private sector; they may even make data collection and monitoring mandatory for law-enforcement purposes, to combat telecoms fraud and money laundering.

Case 2: Tag, You're It: RFID Will Get You⁴¹

There has always been a need to be able to identify and trace products. For this reason, products carry manufacturer and product codes, and since the 1970s many products also carry the UPC (universal product code) or bar code number. Barcodes have to be read by optical scanners and hence have to be visible to the scanner. This limits the use of the technology. Using radio signals instead of optical scanning alleviates the line-of-sight problem and also opens up new possibilities and uses for product tags. Recent advances in technology have made possible the production of Radio-Frequency Identification (RFID) tags with very small footprints and low cost. Soon, they will appear in ever more products.

An RFID system consists of a tag capable of transmitting, and sometimes receiving, information by means of radio signals. The reader consists of a radio receiver that processes the data sent by the RFID tag. Radio tags can be read at 7 items a second, and they can be read even if they are covered by fog, snow, paint, or cardboard.

RFID tags come in various flavours (see Cavoukian 2004 for an overview). Some tags carry chips that can hold a larger amount of data and process information (encryption, verification); they may even contain sensors (to measure temperature, for instance). Chipless tags can store a more limited amount of data (typically 24 bits), but they are cheaper to produce than chip-carrying tags. There are passive tags, which are activated and powered by the reader, with a limited range to about 10 meters; active tags contain a power source and an active transmitter capable of sending the signal over a larger distance (up to several kilometres). Passive tags are smaller and cheaper to produce; they are usually read-only tags that can not be changed after production time. More expensive tags can be changed, or written to, after production.

The price of passive tags at present is in the order of € 0,15-0,50 for quantities of 100,000, which means that they are not suitable for cheap mass consumer products at present. Prices are expected to drop to less than \$ 0.05 a piece (MIT 2002). This would make them suitable to replace barcodes on most products, which means that they can be used as price tags in supermarkets.

⁴¹ Subtitle inspired by the title of a report by the Ontario privacy commissioner Cavoukian (Cavoukian 2004)

RFID tags are generally used as a means of identification of objects, animals, or persons for security or payment reasons, or to be able to provide specialized services. They can be used to provide location information in, for instance, supply chains or buildings. They can also be used to provide specific data about the tagged item, such as colour, size, and production date. This may be used, for example, by washing machines ('Are you sure you want to wash this purple sock together with your white laundry?') or fridges ('You had better finish your milk, which is nearing its best-before date').

So far, current applications are relatively limited in scale due to the cost of present tags. But there are also many plans to implement tags in large numbers. Esso (SpeedPass) and Shell (EasyPay), for instance, use RFID tags in payment systems. SpeedPass users have a key tag incorporating an RFID tag that allows them to pay for their gas without using cash or credit card (WOLFF 2001). Many organizations, such as Tilburg University, have personal RFID cards that provide access to the office buildings. Household pets and cattle are tagged with RFID tags embedded in glass tubes for identification purposes. For cattle, they could replace the yellow ear-tags currently used for cattle in the Netherlands. A number of large seaport operators are installing tags on the containers they process.⁴² Employees in the harbours are also equipped with tags, allowing a detailed log of who has been involved with particular containers. In Alexandria Hospital in Singapore, every patient, visitor and staff member was issued an RFID card after the SARS outbreak in the spring of 2003.⁴³ This allowed all movements of people within the hospital to be traced. In the event of a new SARS victim, this information could be used to quickly establish with whom the victim has had contact. Delta airlines is testing RFID tags attached to baggage to make tracking and tracing of luggage easier.

Large supermarket and retail chains are interested in using RFID tags on their goods because it will allow them to streamline the supply chain. Boxes with items can be inspected without a need to open them, and 'smart shelves' are envisioned to signal staff they need replenishing. The American Wal-Mart chain, who was also a main driving force in introducing the barcode in 1984, intends to introduce RFID tags in conjunction with its top-100 suppliers in 2005. In the UK, the Tesco chain started a pilot project in a store in Cambridge. Gillette, Wal-Mart and Tesco co-operate in the RFID experiments. Prada shoes has plans to implement RFID tags, and Bennetton and Marks & Spencer in the UK have announced plans to incorporate tags in clothing. Moreover, the European Central Bank considers embedding hair-thin RFID tags in euro notes, in order to combat counterfeiting, black-market transactions and money laundering. A final application of radiofrequency identification chips is for labelling people. The American company Applied Digital Solutions is marketing chips (VeriChip) which can be implanted into humans. These chips were at first coined as a means to keep track of children. If a person carrying such a chip goes missing or is abducted, chip-reading devices can be placed in the search area in an effort to track it down. But other uses are soon found. The Barcelona Baja Beach Club offers their members the option to have a VeriChip implanted for € 25 to replace the traditional membership card. The embedded chip offers their carrier the guarantee that they do not have to queue, get reserved tables, and, most importantly, it allows them to order drinks to

⁴² <<http://www.rfidjournal.com/article/articleview/26/1/1/>>.

⁴³ <<http://www.rfidjournal.com/article/articleview/446/1/1/>>.

be put on their tab. 'The bartender simply pings you with a handheld scanner'.⁴⁴ What the chip carriers probably do not realize is that they can also be 'pinged' outside of the Baja Beach Club, perhaps by a local pub owner who dislikes Baja Beach braggards and refuses them entry, or by the local police officer interested in how much the Club member has drunk.

The present applications are fairly straightforward and their use is proportional. Objects can be identified by reading their tag and hence their location can be established, or action can be undertaken on the basis of the identity. But looking further in the future uses can be foreseen that at one time cross the border of proportional use.

An obvious use of RFID tags is personalization of services. Objects and information displays may offer personalised responses and information, depending on the tag that is in its vicinity. Razors and electric toothbrushes could trigger intelligent mirrors, that is, mirrors equipped with a display, to provide specific training or use instructions. Shopping windows can have displays that show personalised information and discounts on the basis of tags worn by a passer-by. In museums, audio and visual information provided by the various objects can be tailored to the person watching the object. The RFID tags in euro notes to counter forgery, black-market transactions, and blackmailing may also be read by law-enforcement agencies to search for fraudulent or stolen money – but also by criminals interested in scanning wallets to find the right wallet to pickpocket.

Radio tags can have a long lifespan, as passive tags can be read long after they have served their intended purpose. Price tags on products, for instance, can be read after the client leaves a shop. The widespread use of RFID tags can therefore easily lead to profiling and monitoring. Corporations, but also governments, can keep track of people by following the tags they wear or carry. Since tags can have an individual identification code, tracing a particular person is possible. This is even easier if they possess items that contain personalized tags, such as the EasyPay card. Moreover, combining data on the various tags carried by a person allows for sophisticated monitoring of lifestyles and habits. For instance, someone entering a Shell station with a car equipped with Michelin tyres, wearing Prada shoes and paying with her EasyPay card, leaves a trace by both her shoes and her car tires. If this information is combined with purchases in shops, she runs the risk of becoming completely transparent. And this may occur without her being aware of it: for one thing, people will rarely notice tags, and if they do, they will tend to regard them as just another barcode, not realising the tracking potential that RFID tags have.

Thus, the use of RFID tags may seriously impact informational privacy. Data from the tags can be collected without the carriers' explicit consent, and even possibly without their being aware of the tag's existence. Invasion into people's personal lives is even greater if identity papers such as passports and driver's licenses are tagged, or if RFID tags like the VeriChip are implanted. This allows for constant tracking of people. A news item in CNet, gave a preview of people tracking: 'Delegates to the recent Communist Party Congress were required to wear an RFID badge equipped with the tiny tag, which permitted their movements around the conference to be constantly tracked and recorded.'⁴⁵

⁴⁴ <<http://www.thefeature.com/article?articleid=100662&ref=1208370>>.

⁴⁵ <http://news.com.com/2009-1088-984352.html?tag=fd_rndm#38>.

Opposition to the use of radio tags is rising from both privacy watchdogs, such as the Electronic Privacy Information Centre (EPIC), the Electronic Frontier Foundation, and European Digital Rights (EDRI), and from consumer organizations, individual consumers, and recently also politicians⁴⁶. As a result of the fierce opposition, many forerunners of RFID use – Bennetton, Wal-Mart, Prada, and Gillette among them – have retracted, or at least changed, their plans. Nevertheless, we think it is inescapable that tags are increasingly used in products, because the benefits for commerce will be simply too great. The real issue is *how* they will be used, for how long, and who will be able to read them under what conditions.

Blocking RFID

RFID tags can, as we have seen, pose serious threats to a person's informational privacy, and also allow a person or object's location to be traced. But resistance is not futile. There are various ways in which RFID tags can be disabled. First of all, the tags can be destroyed physically, for instance by smashing the tag or by 'cooking' them in a microwave oven, which destroys the chip by overloading the circuitry with high-energy radio waves. Since RFID tags use radio signals to communicate with tag readers, traditional radio jamming can be used to disrupt data communication between tag and reader, or the tags can be shielded by metal foil to prevent radio waves from entering or leaving the tag. RSA Security is experimenting with 'Blocker Tags'. These tags can selectively (e.g., only the range of tag id's assigned to Prada shoes) or universally block RFID tags from being read by sending out fabricated data. The blocker tags, if embedded in, for instance, a shopping bag, provide a designated privacy zone: if the item is inside the bag, it cannot be read, but if it is removed, it can be read (JUELS *et al.* 2003). Another way to disable RFID tags is by deactivating the tags when they have served their purpose. The MIT Auto-ID Center has proposed to include a 'kill switch' into the RFID specifications (CAVOUKIAN 2004). A number of RFID manufacturers, such as Philips Semiconductors have announced they will do so.⁴⁷ Chips that implement the kill switch can be disabled on checkout by the reader if the customer requests so. A requirement in that scenario, of course, is that the customer is aware of the tag and its risks; and even then, he may not be fully assured that the tag is actually disabled or may not be switched on again.

Case 3: Facial Recognition in Shops?

Balance

As in e-government, technology facilitates large-scale information collection as well as information shielding, but tends by itself to favour only the former.

Privacy-enhancing technologies can be used to curb data collection, such as anonymisers, cookie crunchers, RFID blockers, and anti-spyware tools, but consumers have to make an effort

⁴⁶ Californian senator Debra Brown has proposed legislation to require persons or entities that use RFID tags to comply with certain conditions, such as an obligation to get an individual's written consent before collecting RFID data and the obligation to destroy or incapacitate the tags once a customer leaves a shop (California sb 834 bill 20040220).

⁴⁷ <<http://blog.digitalidworld.com/archives/000433.html>>.

(and certain costs) to protect their privacy with these. Moreover, often they are not aware of the covert data collection that is taking place in (e-)commerce, and they do not bother to use PETs. And although it is conceivable that privacy-enhancing 'code' is built-in more in infrastructures and services, so far, little progress seems to be made in that area. The interests at stake simply seem to favour privacy-threatening technology much more than privacy-friendly 'code'.

5.4 The Effects of 'Code' on Privacy

What picture emerges from the *tour d'horizon* of 'code'-influenced privacy? There is a clear common thread in all of the domains that we analysed. Privacy-related norms are rarely explicitly built-in in technology. As such, a Lessigish privacy 'code' or a Reidenbergian *Lex Informatica Vitae Privatae* does not exist. Technology, in particular software and the Internet architecture, rarely incorporates specific privacy-related norms. The few existing exceptions concern building-in an option of privacy violation, such as interceptability of telecommunications.

At the same time, however, technology very often does have clear effects on privacy.

Technology affects the 'reasonable expectation of privacy', it partly shapes what can be deemed 'necessary in a democratic society' when it comes to deciding what privacy violations are acceptable. In the vast majority of technologies that are developed and used in real life, this influence is to the detriment of privacy. That is, technology often has the side-effect of making privacy violations easier. Particularly information technology turns out to be a technology of control. Although at a theoretical level, it also is a technology of freedom, in practice, it rarely functions as such. Privacy-enhancing technologies (PETs) have been devised and propagated, but they have not been implemented on any serious scale.

This conclusion holds both for the public and for the private domain. As the examples in law enforcement and e-government show, technology offers increasing opportunities for large-scale monitoring – from intercepting all telecommunications (and there is a *lot* of telecommunications nowadays) to monitoring the movements of people. Also in the private sector, technology enables more and more control of people, from workplace and transaction monitoring to personalisation of consumer relationships, with new applications such as facial recognition and RFID monitoring looming ahead.

This is understandable. One of the prime attributes of information and communications technology is that it enables sharing of information rather than shielding or compartmentalising information. And the people who usually decide on how technology is applied are precisely the people on the strong side of power relations – governments, businesses, employers –, who have an interest in gathering information about the people on the other side, so that they can maintain or expand their power basis.

This is not to say that people in power always consciously exploit technology for control purposes, but it does mean that there is little incentive to look deep into the effects of new technologies for privacy. If some more control is possible by a new application, well, that is not what the application was made for, but it is fine nonetheless. They gladly adopt the new possibilities. In fact, after a lapse of time, people get so used to this new control mechanism, that it may be no longer perceived as a side-effect, but as an intrinsic – and perhaps intended – characteristic of the technology. This is when the 'reasonableness' of a privacy expectation is

shifting: once the new technology is accepted as being inherently control-friendly, there no longer is a reasonable expectation that this control is not exerted. At that point, since control is also a primary interest to governments in their law-and-order role, the control characteristic may also be mandated by law. Non-interceptable telecommunications is forbidden, because the police have got so used to intercepting telecommunications that a large part of their work is based on this method. Identification is made obligatory, because government employees feel they simply have to know the identity of citizens in order to be able to do their job.

The eroding effect of technology on privacy is thus a slow, hardly perceptible process. There is no precise stage at which one can stab a finger at technology to accuse it of unreasonably tilting the balance of privacy. Exactly because of the flexible, fluid nature of what is deemed privacy, society gradually adapts to new technologies and the privacy expectations that go with it.

If one is to stop this almost natural process, a conscious effort and considerable resources are called for.

5.5 Evaluation of ‘Code’ and Privacy

We now return to the initial question that triggered this research: how does ‘code’ relate to privacy? How should we perceive the notion of ‘code as law’ when it comes to privacy regulation? We turn to the questions Lodewijk Asscher formulated in Chapter 3.

1. Can *rules* be distinguished in the code?

Only rarely does code include specific privacy-related rules. One example is interceptability of telecommunications, in which the ‘rule’ is built-in that the government must have an option of intercepting telecommunications if it wants to. Other examples are PETs, such as anonymisers and RFID blockers; here, the ‘rule’ is that one must be able to use technology in an anonymous, unsupervised way. Even though such norms are not legal rules in the sense of ‘Thou shalt not kill’, one can see them as expressing rights: everyone has the right to anonymity; the government has the right to intercept. It is stretching things a bit to see them as constituting these rights themselves, though – rather, they are enforcement mechanisms of such rights. In the vast majority of technologies, however, there are no privacy-related ‘rules’. The technology just often happens to facilitate control, but this is not a consciously built-in characteristic that could count as a rule. Since this majority of cases does not count as ‘code’ in the strict sense, we shall restrict answering the remainder of the question for the minority cases, where ‘code’ consciously incorporates a rule.

2. Can the rules be *trusted*, is there any guarantee that rules are not changed during the game?

3. Can they be *understood*, i.e. is it understandable how ‘code’ works and what it does? If so, are those rules transparent, are they accessible to the general public?

5. Are ‘code’ rules *reliable* in the sense that they are predictable? Is there a difference between what the ‘code’ maker says ‘code’ does and its *actual* working?

This cluster of questions into the transparency of ‘code’ is hard to answer, given the scarcity of examples. We will nevertheless give a tentative answer.

Government-mandated ‘code’ that enforces control, such as interceptability, tends to be obscure; this might invite changing the rules along the way, in the development process or afterwards in ‘updating’ technology. The debates in the U.S. over CALEA and the wide interpretation the government gave to the interceptability requirement, might be seen as an example of a fear that what would actually be built-in in the telecommunications infrastructure was more than mere interceptability. The culture of secrecy triggers the fear that the built-in rule – interceptability – functions differently, that is, in an even more privacy-threatening way. One might say that ‘code’ in its guise of government-mandated control rules is inherently unreliable: unless law enforcement and national security replace secrecy with openness and open source, there will always remain a hint of suspicion, justified or not, that technology does more than what the government says it does.

With PETs, this is not the case. Precisely because it is developed to protect privacy by people who are usually ardent defenders of privacy, there is less risk that the built-in rule – you can be anonymous, you can do this without being monitored – is actually changed. Yet this is not absolute, as the story of NSA-induced backdoors in Crypto AG’s cryptography products suggests. We do not believe developers of privacy-enhancing technologies are being routinely infiltrated or convinced by security agents to build in backdoors. However, given the covert nature and the large interests of national security, particularly in the current post-9/11 climate, one cannot altogether dismiss a fear that even PET products produced by privacy-minded people, particularly robust ones that thwart any kind of control, are being covertly altered.

4. Are ‘code’ rules contradictory? Do they pose a logical or at least *consistent* system of regulation? Do ‘code’ rules require the impossible?

In a way, one might view government-mandated privacy-infringing ‘code’ as contradictory with PET ‘code’. After all, they have opposing goals, and a technology with a built-in option for privacy infringement clashes with a technology that has privacy protection built-in. They function more or less as an arms race, with PETs reacting to overintrusive surveillance technologies, and privacy-infringeable ‘code’ being developed to counteract the threat to governments of uncrackable PETs. This neatly mirrors the precarious balancing act of privacy, which is continuously being tugged at by the interests on both sides of the balance.

Still, this does not need to be the definitive answer. PETs are interesting precisely because they can incorporate shades of privacy protection. The concept of PET is not so much that it protects privacy absolutely, but that it *enhances* the protection of privacy, and usually so that it does not unreasonably restrict other interests at stake. Often, one can develop technology in such a way that privacy is not unnecessarily threatened while still achieving its primary goal. Particularly the domains of e-government and commerce lend themselves well to such PETs: one can easily do business with the government and with enterprises without offering the most intimate details of one’s private life. The privacy-threatening side-effect of technology can be curbed to a considerable extent by such PETs. And so, ‘code’ can offer – in theory, at least – a consistent system of regulation by allowing degrees of privacy protection: privacy when possible, infringement when necessary.

6. Is there a sovereign? An *authority* that makes the ‘code’ rules?

With government-mandated enforcement 'code', there is a clear sovereign: the government. If the built-in privacy infringeability is mandated by the legitimate legislator – parliaments and the like –, there is no specific 'code' problem of legitimacy. If parliament decides that all telecoms should be interceptable, then so be it. But if the 'code' should be built-in – hush-hush – at the urge of government in its guise of national-security protector, there may be more cause for concern, given the intransparency and uncontrollability of such actions.

For PETs, the relevant authority is the technology developer, operating perhaps at the urge of Data Protection Authorities and privacy lobbies, and sometimes at the urge of government (as in the case of Microsoft's .Net passport).

7. Is there a *choice*? Can consumers/citizens choose not to obey the rules? Can citizens/consumers freely choose another system of law/code?

The choice issue is related to the question of consistency. Citizens cannot choose between interceptable and non-interceptable telecommunications, simply because the built-in interceptability has been made obligatory by law. But they can choose to use PETs when telecommunicating, counteracting the risk of interception. (Of course, they could also choose not to use telecommunications anymore – or can they?) In principle, they can choose any array of technologies that fit their own privacy desires (supposing the PET does not secretly leak). In practice, however, the choice is more difficult. Choice implies awareness, and particularly with privacy, there is considerable lack of awareness among the general public of the potential uses to which technologies can and will be used against you. Choice also implies affordability, and although anonymisers or RFID blockers do not cost millions of euros, they are not free either. More importantly, they are time-consuming and require a conscious effort to apply, as opposed to the one-click-does-it-all interface that people have gotten used to. There is yet another constraint. In doing business, be it with enterprises or the government, the technology is not consciously privacy-threatening but facilitates privacy infringements nonetheless. Hardly ever can one choose to use a PET in such situations. It is the provider of goods and service – business, government – that should implement a PET; if they do not, the citizen/consumer cannot herself decide to use PET: the system simply refuses anonymous communications, or requires you to fill in fields with personal data that, in principle, have nothing to do with the good or service at issue (why do they have to know you are female and the date you were born if you want to e-mail a question to a government through a web form?). In the commerce domain, one might look at the market to ensure choice nevertheless, some companies offering consumers privacy-friendly services; in the public domain, one can – so far – not choose between governments to conduct business with.

8. Do 'code' rules conflict with or alter *traditional* legal norms?

The 'code' rules seem at first sight in line with traditional legal norms. After all, they are developed precisely to enforce existing norms: interceptability and PETs are both examples of enforcement-enhancing technologies that safeguard accepted legal values: law enforcement and privacy protection.

At second sight, one may be more critical, however. Enforcement may be built-in not only because it enforces a traditional legal norm, but also because it *reinforces* this norm. In other

words, there is a mutual influence between legal norms and technology, particularly technologies of control. As noted above, if technological development facilitates more control, and once society gets used to this new technology, the step of mandating the control element in the technology may appear merely applying the law, but at the same time, it makes the law stronger than it ever was. This is because the element of rule-breaking is eliminated. Where formerly, people could, if they wanted to, circumvent control, even if the control was consistent with the law, with built-in enforcement there is no escaping control. In this way, 'code' that 'applies' existing legal norms at the same time makes the legal norm itself absolute.

Now, how does the notion of 'code as law' work overall when it comes to privacy regulation? The main answer is that 'code' as such does not function as law in the privacy context. That is, by and large, no norms are built-in in technology that relate directly to privacy, except for a handful of enforcement-enhancing technologies.

The subsidiary answer is that, where technology does function as Lessigish 'code', i.e., in these enforcement tools of interceptable telecoms and PETs, one can voice concern over some elements. Notably, the transparency of the 'code' and the non-circumventability can be perceived as problematic. But this should not be exaggerated: we are talking about a very minor part of the gamut of technology as we use it today, making the fact that one has no choice but to use it less pregnant. And the 'codes' mentioned may be intransparent, because we cannot exclude national-security-urged backdoors being built-in, but then again, we can also not exclude the possibility that the world is teeming with Martians we just happen never to see because they are smart enough to stay invisible. And any lawyer specialised in telecommunications law can tell that many legal norms are not particularly transparent either. In short, in the relatively few cases in which privacy-related norms are built-in explicitly in technology, there are concerns of transparency and mandatory compliance, but these concerns may not differ radically from non-'code' forms of regulation.

5.6 Options for Action

Now we can go into the second part of our question: if 'code' causes potential shifts in privacy balances, what should be done about this?

It turns out that there are in fact two distinct issues at stake, which require separate treatment. The larger issue emerging from our analysis concerns the slow but gradual erosion of privacy that is a side-effect of much technological development (see 5.4). The privacy balance clearly seems at stake here, and so, we should look into options for action. However, this does not belong to the 'code' debate as triggered by Reidenberg and Lessig. Rather, it fits in the 'death of privacy' issue that ought to be but does not really, Froomkin (2000) notwithstanding, seem to be a serious academic and societal debate.⁴⁸

The second, but much smaller, issue is 'code' as a privacy-related regulation or enforcement tool (see 5.5). This affects privacy regulation to a minor extent. Some things can be done to address

⁴⁸ 'Erosion of privacy' has been debated in the 9/11 context and before, centering on the U.S. Patriot Act, the U.K. Regulation of Investigatory Powers Act, and similar privacy-diminishing laws. However, the erosion of privacy as inherently facilitated by technology – the issue we are concerned with here – is not the topic of that debate.

flaws in the functioning of this 'code' as privacy law, notably to enhance transparency and to counter the uncircumventability, but this seems to us less urgent than the first issue. We therefore take the liberty of concentrating our options for action on an issue that is not really part of the 'code' topic of this book. How can the gradual erosion of privacy be addressed?

Lessig suggests two pillars of tilting the balance of privacy back again. One is commodification of personal data, that is, treating personal data as a commodity that the data subject owns, comparable to, e.g., portrait rights marketed by celebrities.⁴⁹ Such an approach might give people enough power over their personal data that the risks of data merging, profiling, exclusion, and the like can be countered. However, as Prins argues, this approach ultimately fails, because it is ineffective: 'Given that, to a large extent, individuals depend on the use of their data and that personal data are the motor of our information society, a move towards a legally recognized property right in personal data will in effect not change the free public availability and exchange of these data.' Instead, she argues that data protection should be safeguarded by instruments to enhance visibility (awareness and knowledge) and control.⁵⁰

Could Lessig's second pillar, Privacy-Enhancing Technologies, provide such an instrument? PETs, after all, are an instrument of control. As we have argued in the cases in the various domains, PETs by and large seem a pet of data protection commissioners and privacy lobbyists, but so far, they do not seem to get through to other sides. They remain mainly a theoretical solution that has yet to prove its effect in practice. We discern several reasons for this: technology by itself tends to combine and connect rather than to compartmentalise, information wants to be free rather than be shielded, and governments dislike technologies they cannot break to get information. Moreover, the people who need PETs are usually not the ones who can decide whether they are used. And even if they can, they are often not aware of the consequences that on-line (trans)actions have for their privacy, or they are not willing to invest extra effort and money in using PETs.

Therefore, if PETs are to do the trick of keeping privacy alive, a conscious and concerted effort is needed. The market will not stimulate and use PETs by itself; in our view, it is clear the government intervention is needed if privacy-enhancing 'code' is really to carry weight in stopping the gradual erosion of privacy. Sometimes, we get a glimpse of what such intervention may achieve, such as when Microsoft adapted its .Net passport system under European pressure.

What could a government PET action plan look like? First, governments should consistently evaluate, or have others evaluate, technology developments for their effects on privacy. Just as Dutch legislation requires an 'environment impact report' to be made for, e.g., major construction activities, extraction of oil, and waste dumps, legislatures could impose an obligation to make a 'privacy impact analysis' in cases of new technologies being developed and marketed.

Second, there should be more binding mechanisms to respect privacy when possible and to only infringe privacy when necessary. Although the principles of subsidiarity and proportionality are enshrined in many privacy and data-protection laws, they do not appear to have much effect on

⁴⁹ Lessig (1999), p. xxx.

⁵⁰ Prins (2004), p. 26.

the privacy risks of technology. As a corollary of a privacy impact analysis, a control mechanism should be established that checks whether technologies are constructed in the most privacy-friendly way compatible with other requirements (such as information needs and security). We are not sure that this is entirely feasible, but it should be at least possible to uncover excesses and overintrusive technologies. The control mechanism should then also have some sanctioning power, e.g., a prohibition for the government to buy privacy-unfriendly technologies, or a power to fine companies that fail to make a privacy impact analysis or that market clearly privacy-unfriendly products.

Third, and perhaps most importantly, a PET action plan should raise awareness, both of citizens/consumers and of enterprises, of government agencies as well as of technology developers. Raising awareness of privacy risks with citizens and consumers is in fact a crucial first step to stopping the downward spiral of privacy erosion. Only if they are aware that there is 'death of privacy' development and what this may mean for their future, can – perhaps – a sufficient amount of leverage be established that can start to check the natural privacy-eroding tendency of technology and its promoters.

References

- Bellare, M., and R.L. Rivest. *Translucent Cryptography. An Alternative to Key Escrow, and its Implementation via Fractional Oblivious Transfer*, 996.
<http://theory.lcs.mit.edu/~rivest/BellareRivest-translucent.ps>.
- Benn, S. I. *A theory of freedom*. Cambridge: Cambridge University Press. 1988.
- Blok, Peter. *Het recht op privacy*. Den Haag: Boom Juridische uitgevers. 2002.
- Boyle, James. Foucault in Cyberspace: surveillance, sovereignty, and hardwired censors. *U. Cin. L. Rev* 66: 177-. 1997.
- Brenda, M.A. *Zorg Identificatie Nummer. Onderzoek consequenties invoering ZIN voor zorgverzekeraars en zorgaanbieders*, Utrecht: Cap Gemini Ernst & Young (voor NICTIZ), 2004.
- Bygrave, Lee A. *Data Protection Law: Approaching its Rationale, Logic and Limits*. The Hague, London, New York: Kluwer Law International. 2002.
- BZK. *Contract met de toekomst*. Den Haag: Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. 2000.
- Cate, Fred. *Privacy in the Information Age*. Washington DC: Brookings Institution Press. 1997.
- Cavoukian, Ann. *Tag, You're It: Privacy implications of Radio Frequency Identification (RFID) Technology*, Ontario: Information and Privacy Commissioner/Ontario, 2004.
- De Hert, Paul. *Privacy en het gebruik van visuele technieken door burger en politie*. Brussel: Politeia. 1998.
- Denning, Dorothy, and William Baugh. *Hiding Crimes in Cyberspace*, <<http://www.cs.georgetown.edu/~denning/crypto/hiding1.doc>>.
- Etzioni, A. *The Limits of Privacy*. New York: Basic Books. 1999.
- Foucault, Michel. *Surveiller et punir: naissance de la prison (Discipline and punish: The birth of the prison)*. Paris: Gallimard. 1978.
- Fried, C. Privacy. *Yale Law Journal* 1968: 475-493. 1968.
- Frissen, P. *Public Administration in Cyberspace*. in *Public administration in an information age*, edited by I.Th.M. Snellen and W.B.H.J. van der Donk. Amsterdam etc.: IOS Press. Pp. 33-46. 1998.
- Froomkin, A. Michael. The Death of Privacy? *Stanford Law Review* 52: 1461-1543. 2000.

- Garfinkel, S. *Database Nation. The death of privacy in the 21st century*. Cambridge: O'Reilly. 1999.
- Gavison, Ruth. Privacy and the limits of law. *Yale Law Journal*: 421-471. 1980.
- Hoffman, Lance J. (ed.). *Building in Big Brother. The Cryptographic Policy Debate*. New York: Springer. 1995.
- Information and Privacy Commissioner & Registratiekamer, Privacy-Enhancing Technologies: The Path to Anonymity, August 1995, <<http://www.ipc.on.ca/docs/anoni-v2.pdf>>.
- Jefferies, N., C. Mitchell, and C. Walker. "A Proposed Architecture for Trusted Third Party Services." Pp. 98-104 in *Cryptography: Policy and Algorithms, Proceedings of the conference*: Springer-Verlag (LNCS 1029). 1996.
- Johnson, J.L. Privacy and the judgment of others. *The Journal of Value Inquiry*: 157-168. 1989.
- Juels, A, R. L. Rivest, and M. Szydlo. "The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy." Pp. 103-111 in *8th ACM Conference on Computer and Communications Security*, edited by V Atluri: ACM Press. 2003.
- Koninkrijksrelaties, Ministerie van Binnenlandse Zaken en. *Advies van de Tafel 'Persoonsnummerbeleid in het kader van identiteitsmanagement'*. Den Haag: Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. 2002.
- Koops, Bert-Jaap. "Crypto Law Survey, version 22.1." 2004. <<http://law.uvt.nl/koops/cryptolaw/>>.
- Lessig, Lawrence. *Code and other laws of cyberspace*. New York: Basic Books. 1999.
- Litman, Jessica. Information Privacy/Information Property. *Stanford Law Review* 52: 1283- 1313. 2000.
- Madsen, Wayne, Crypto AG: The NSA's Trojan Whore?, *Covert Action Quarterly* 63, January 1999, <<http://www.100megsfree4.com/farshores/crypto.htm>>.
- MIT. *The New Network: Identify Any Object Anywhere Automatically*, Cambridge: Mass: MIT Auto-ID Center, 2002.
- Moore, B. *Privacy: Studies in social and cultural history*. Armonk: ME Sharpe. 1984.
- O'Hara, Colleen, and Heather Harreld. DOD sinks the Clipper. *Federal Computer Week* 17 February. 1997.
- President, Office of the Vice. *Reengineering government through IT, Washington DC*: Government Printing Office, 1993.
- Prins, J.E.J., Property and Privacy: European Perspectives and the Commodification of our Identity, working paper, 2004.
- Raab, C. *Electronic service delivery in the UK. Proaction and privacy protection*. in *Designing E-Government*, edited by J.E.J. Prins. Dordrecht: Kluwer Law International. Pp. 41-62. 2001.
- Rachels, J. Why privacy is important. *Philosophy and Public Affairs*: 323-333. 1975.
- Radwansky, George. "The privacy challenge - Connecting citizens with all levels of Government." in *Conference Board of Canada's 2002 eGovernment Conference Crossing Bridges to Success*. Ottawa, Ontario, May 9, 2002. 2002. <http://www.privcom.gc.ca/speech/02_05_a_020509_e.asp>.
- Reidenberg, Joel R., 'Lex Informatica: The Formulation of Information Policy Rules Through Technology', *Texas Law Review* 76 (February 1998), p. 553-84, <http://reidenberg.home.sprynet.com/lex_informatica.pdf>.
- Reidenberg, Joel R. States and Internet Enforcement. Jan 2004. 2004.
- Rotenberg, Marc. Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get). *Stanford Technology Law Review* 2001. 2001. <http://stlr.stanford.edu/STLR/Articles/01_STLR_1>.
- Schneier, Bruce , and David Banisar. *The Electronic Privacy Papers*,. New York etc.: John Wiley & Sons. 1997.

- Schudelaro, Antonius Adrianus Petrus. *Electronic payment systems and money laundering risks and countermeasures in the post-internet hype era*. Nijmegen: Wolf Legal Publishers. 2003.
- Schwartz, Paul M. Beyond Lessig's Code for Internet Privacy: Cyberspace Filters, Privacy-Control, and Fair Information Practices. *Wisconsin Law Review*: 743-788. 2000a.
- Schwartz, Paul M. Internet Privacy and the State. *Connecticut Law Review* 32: 815-. 2000b. <http://www.paulschwartz.net/bibliography.htm>.
- Seidle, F.L. *Rethinking the delivery of public services to citizens*, Montreal: Institute for research on Public Policy (IRPP), 1995.
- Sykes, C.J. *The End of Privacy*. New York: St. Martin's Press. 1999.
- Vedder, A.H. *Medical Data, New Information Technologies, and the Need for Normative Principles other than Privacy Rules*. in *Law and Medicine : Current Legal Issues*, edited by M. Freeman and A. Lewis. Oxford: Oxford University Press. Pp. 441-459. 2000.
- Vermissen, J.A.G., and A.C.M. de Heij. *Elektronische overheid en privacy. Bescherming van persoonsgegevens in de informatie-infrastructuur van de overheid*, Den Haag: College bescherming persoonsgegevens, 2002.
- Walker, Kent. Where Everybody Knows Your Name: A Pragmatic Look at the Costs of Privacy and the Benefits of Information Exchange. *Stanford Technology Law Review*. 2000. HTTP://STLR.STANFORD.EDU/STLR/ARTICLES/00_STLR_2.
- Warren, Samuel D., and Louis D. Brandeis. The right to privacy. The implicit made explicit. *Harvard Law Review*: 193-220. 1890.
- Westin, A. *Privacy and Freedom*. New York: Atheneum Press. 1967.
- Whitaker, Reginald. *The end of privacy : how total surveillance is becoming a reality*. New York: New Press : Distributed by W.W. Norton. 1999.
- Whitman, James Q. The Two Western Cultures of Privacy: Dignity versus Liberty. *Yale Law Journal* Vol. 113. 2004.
- Wolff, John. *RFID Tags - An intelligent Bar Code Replacement*: IBM Global Services, 2001.