'CODE' AND THE SLOW EROSION OF PRIVACY†

*Bert-Jaap Koops**
*Ronald Leenes***

Cite as: Bert-Jaap Koops and Ronald Leenes,
'Code' and the Slow Erosion of Privacy,
12 MICH. TELECOMM. TECH. L. REV. 115 (2005),
available at http://www.mttlr.org/voltwelve/koops&leenes.pdf

† This Article is a revised version of a chapter to appear in CODING REGULATION: ESSAYS ON THE NORMATIVE ROLE OF INFORMATION TECHNOLOGY (L.F. Asscher ed., T.M.C. Asser Press forthcoming 2006). Parts of this Article are based on the work of Dr. Ton Schudelaro and Dr. Anton Vedder, whom the authors thank for their collaboration. They also thank the participants of the "Code as Law" workshop that took place July 1–2, 2004 in Amsterdam, and Michael Froomkin and Joel Reidenberg for their further helpful suggestions.

* Bert-Jaap Koops has an M.Sc. in mathematics and a Ph.D. in law. Professor of Regulation of Technology at the Tilburg Institute of Law, Technology, and Society (TILT), of Tilburg University, the Netherlands.

** Ronald Leenes has an M.A. in Public Administration and a Ph.D. in legal informatics. Associate Professor of Law & Technology at TILT, of Tilburg University, the Netherlands.

The notion of software code replacing legal code as a mechanism to control human behavior—"code as law"—is often illustrated with examples in intellectual property and freedom of speech. This Article examines the neglected issue of the impact of "code as law" on privacy. To what extent is privacy-related "code" being used, either to undermine or to enhance privacy? On the basis of cases in the domains of law enforcement, national security, E-government, and commerce, it is concluded that technology rarely incorporates specific privacy-related norms. At the same time, however, technology very often does have clear effects on privacy, as it affects the "reasonable expectation of privacy." Technology usually makes privacy violations easier. Particularly information technology is much more a technology of control than it is a technology of freedom. Privacy-enhancing technologies (PETs) have yet to be implemented on any serious scale. The consequent eroding effect of technology on privacy is a slow, hardly perceptible process. If one is to stop this almost natural process, a concerted effort is called for, possibly in the form of "privacy impact assessments," enhanced control mechanisms, and awareness-raising.

I. INTRODUCTION

A. *Panoptic Panoramas*

In 1787, Jeremy Bentham, the English utilitarian philosopher, worried over the moral state of his times, devised an architectural design for a prison that he called the Panopticon. This Panopticon has stood as a model 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 cannot 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 to command them individually, day and night. The strength of the Panopticon is not so much that the Inspector can issue commands and monitor the inmate but the *illusion* that he could. As the point of the Panopticon is *discipline* or *training*,[1] the constant illusion of monitoring and inmates' fear of punishment for transgressions means that they 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. Whereas the actual implementation of the Panopticon was not very realistic in Bentham's times, today it is becoming increasingly so. Closed Circuit TV (CCTV) cameras are appearing everywhere, in both private and public places. Although these cameras increasingly 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")[2] and compliance with speed regulations.

1. *See* REGINALD WHITAKER, THE END OF PRIVACY: HOW TOTAL SURVEILLANCE IS BECOMING A REALITY 33 (1999).

2. *Id.* at 141.

Completely in line with panoptic logic, there may not be anyone actually watching the camera shots or the cameras may lack film. It is the possibility of being caught that is part of their effect. The illusion of an omnipresent inspector keeps the subjects in line.

The Internet offers excellent opportunities for even further-reaching forms of surveillance. Boyle,[3] following Foucault's analysis of the Panopticon,[4] concludes that the state is creating an Internet Panopticon: "[T]he state has worked actively to embed or hardwire the legal regime in the technology itself."[5] An interesting aspect of this Internet Panopticon is that the state shifts the responsibility of enforcement to entities in the private sector, such as Internet service providers (ISPs).

"In the meantime private entities are happily creating their own independent Panopticons."[6] 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. "[C]ustomers 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."[7] 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.

B. *Technology, Privacy, and Lessig's Code*

The Panopticon relies heavily on technology. Especially Information and Communication Technologies (ICTs) offer almost unlimited possibilities to facilitate perfect surveillance and monitoring, thereby invading people's privacy. Partly as a result of the rise of the network society, some authors have already proclaimed privacy dead. Book and article titles have included the phrases "the death of privacy"[8] and "the end of

3. James Boyle, *Foucault in Cyberspace: Surveillance, Sovereignty, and Hardwired Censors*, 66 U. CIN. L. REV. 177 (1997).

4. MICHEL FOUCAULT, SURVEILLER ET PUNIR: NAISSANCE DE LA PRISON [DISCIPLINE AND PUNISH: THE BIRTH OF THE PRISON] 197–229 (1975).

5. Boyle, *supra* note 3, at 188.

6. Paul M. Schwartz, *Internet Privacy and the State*, 32 CONN. L. REV. 815, 853 (2000), *available at* http://www.paulschwartz.net/bibliography.html.

7. WHITAKER, *supra* note 1, at 142.

8. A. Michael Froomkin, *The Death of Privacy?*, 52 STAN. L. REV. 1461 (2000); SIMSON GARFINKEL, DATABASE NATION: THE DEATH OF PRIVACY IN THE 21ST CENTURY (1999).

privacy."[9] Or, as Scott McNeally, Sun Microsystems' CEO, proclaimed after Intel acknowledged that they were able to track people through their new Pentium III chip in 1999, "You already have zero privacy . . . . Get over it."[10] Both the influence of technology and the fact that people seem to care less about privacy have been considered factors warranting the statement that privacy is no longer feasible, or relevant, or neither of these.

In this Article, we intend to analyze this impact of technology on privacy. We do so by following Lawrence Lessig's argument in the privacy chapter of his *Code and Other Laws of Cyberspace*.[11] Lessig argues that "the code [technology] has already upset a traditional balance. It has already changed the control that individuals have over facts about their private lives."[12] He illustrates this with several privacy-threatening technologies. After an analysis of different conceptions of privacy and arguments for and against privacy protection, Lessig presents a response to privacy-threatening technology: privacy-enhancing technology (PET). 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 had earlier termed *lex informatica*: software and hardware that regulate themselves, or rather, Internet users and developers who regulate themselves through technology.[13] Although we do not intend to analyze and criticize Lessig's chapter on code and privacy specifically, a rigorous discourse requires a closer look at Lessig's analysis of the impact of code on privacy and the solution he presents 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*,[14] and many authors shared his thoughts, including Jerry Kang,[15]

---

9. CHARLES J. SYKES, THE END OF PRIVACY (1999); *see* WHITAKER, *supra* note 1.

10. Polly Sprenger, *Sun on Privacy: Get Over It*, WIRED.COM, Jan. 26, 1999, http://www.wired.com/news/politics/0,1283,17538,00.html.

11. LAWRENCE LESSIG, CODE: AND OTHER LAWS OF CYBERSPACE 142–63 (1999).

12. *Id.* at 142.

13. Joel R. Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules Through Technology*, 76 TEX. L. REV. 553, 554–55 (1998). Reidenberg had already pointed out this development much earlier, in his seminal 1993 paper, *Rules of the Road for Global Electronic Highways: Merging the Trade and Technical Paradigms*, 6 HARV. J.L. & TECH. 287 (1993).

14. *See* ALAN F. WESTIN, PRIVACY AND FREEDOM 7 (1967).

15. *See* Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1195–98 (1998).

Fred Cate,[16] and Robert Post.[17] Privacy is undermined by ICTs as they allow for electronic surveillance and the collection of personal data. These activities are problematic to Lessig 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."[18] This is done by presenting only the options the profiler wants the person fitting a particular profile 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 diminished equality. 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.[19] This equality explicitly resulted from the fact that information to discriminate was too costly to acquire. Modern data collection, especially with merging multiple data sources, makes it possible to discriminate. Lessig exemplifies this phenomenon with frequent-flyer programs, which allow airlines to distinguish between classes of passengers. The profiling in this case is not too severe, as airline passengers are aware of the existence of frequent-flyer programs which everyone can join. A more convincing example of the pressure on equality posed by profiling is the opaque differentiation in types of customers that, for instance, was done by the online bookstore, Amazon, who presented different prices for DVDs on the basis of the kind of browser used, whether one was a first-time or a repeat customer, or which ISP the customer used.[20]

Lessig's solution to these threats is a two-tier system: code and property law. Lessig equates privacy with information privacy; hence, restoring people's control over their personal data is the logical approach to address the imbalance technology has caused. Instead of calling for legal measures, such as fair information practices, Lessig seeks the solution in technology: privacy-enhancing technologies (PETs). He embraces the idea of software implementing our privacy preferences: an electronic butler, who negotiates privacy protection on our behalf[21]—a notion that builds on the World Wide Web Consortium's Platform for Privacy Pref-

16. *See* FRED H. CATE, PRIVACY IN THE INFORMATION AGE (1997).

17. *See* Robert Post, *The Social Foundations of Privacy: Community and Self in the Common Law Tort*, 77 CAL. L. REV. 957 (1989).

18. LESSIG, *supra* note 11, at 154.

19. *See id.* at 154–55.

20. Linda Rosencrance, *Amazon Charging Different Prices on Some DVDs*, COMP. WORLD, Sept. 5, 2000, http://www.computerworld.com/industrytopics/retail/story/0,10801,49569,00.html.

21. *See* LESSIG, *supra* note 11, at 160.

erences (P3P) Project.[22] The electronic butler implements negotiating power. But what if the other party simply ignores the negotiations and proceeds to collect and use personal data without a person's consent? Lessig's solution to this problem is to define personal data as property and, hence, introduce property law as the regime to protect people's personal data. The advantage of relying on property law over data protection law lies in the fact that property law facilitates *ex ante* control over personal data: only after consent, may personal data be used. Obviously the consent will only be given at the right price.[23]

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

- privacy equals information privacy;
- code upsets the privacy balance;
- personal data should be considered a property right; and
- code and property law should be used to restore the privacy balance.[24]

Lessig and others' analysis of privacy as control of personal data that should be treated as a property right is contested.[25] Nevertheless, it exemplifies an essentially 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 Article, we will not delve into too much detail on the debate over the various privacy conceptions, but we do need a better grasp on the concept of privacy to understand the impact of code on privacy. To this end, Lessig's most important claims are that code upsets the traditional privacy balance and that "code" can be used to restore this balance.

C. *Research Questions and Overview*

In this Article we try answer the following questions:

- Is privacy-related regulation being implemented in code?
- What (kind of) rules are embedded in this code?

---

22. P3P Public Overview, http://www.w3.org/P3P/ (last visited Nov. 15, 2005).
23. *See* Ronald H. Coase, *Problem of Social Cost*, 3 J.L. & ECON. 1 (1960).
24. *See* LESSIG, *supra* note 11, at 141–63.
25. *See infra* Part VII.

- What are the problems associated with this embedding of rules?
- Does "code" indeed induce shifts in privacy balances?
- What could and should be done, by whom and when, to address these problems?

Here, we make a terminological distinction between code and "code." With code, we denote software and hardware generally.[26] "Code," however, denotes software and hardware that function as a set of normative rules. That is, we use "code" when we refer to an ICT that incorporates certain normative elements, which serve to guide or control (what is perceived as) proper and acceptable behavior. We shall thus distinguish throughout this Article between ICT in general (code) or ICT that embeds certain norms or values ("code").[27]

In answering the research questions we will look at both the public and the private sphere, since 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. Privacy is not an absolute right, and intrusion of the private sphere is sometimes warranted. The interests of all parties involved have to be balanced. We will argue that different privacy balances exist in the various domains and that the impact of code on privacy should be assessed with respect to the particular domain. In other words, whether breaches of privacy are justified is context-specific, since privacy means different things in different contexts. Apart from the threats to privacy, we also try to indicate potential solutions to these threats.

The article is organized as follows. In the next section, we 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, and the U.S. perspective, which can be said to be liberty-oriented.[28] In Part III, we discuss developments on privacy and code in four domains, both in the public and private sphere. Part IV sums up the effects of "code" on privacy that emerge from this case analysis, which we then

---

26. We use code rather than the general term "technology" since we focus on information and communication technologies rather than technology in a broad sense.

27. This is what Lessig generally means when he speaks of "code," as in the title of his book: "The software and hardware that make cyberspace what it is constitute a set of constraints on how you can behave." LESSIG, *supra*, note 11, at 89. However, he also uses "code" in the more neutral sense: for instance, where he writes that code has already upset the traditional privacy balance, he uses the term "code" not to denote software and hardware in a normative sense, but in the neutral sense to mean software code or, more generally, to indicate a vague notion of technology. *See id.* at 142.

28. *See* James Q. Whitman, *The Two Western Cultures of Privacy: Dignity versus Liberty*, 113 YALE L.J. 1151 (2004), *available at* http://ssrn.com/abstract=476041.

analyze in Part V according to basic questions that the notion of "code as law" raises. Next, in Part VI, we try and pinpoint the main problems at stake, and we conclude in Part VII tentatively looking at options for actions to address these problems.

II. PRIVACY

A. *Concepts of Privacy*

Many articles and books on privacy have noted that 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: the nature of value notions is that they are not precisely delineated. In fact, privacy may be a clearer and more concise concept than, for instance, autonomy or liberty.[29] 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.[30] They are not primarily concerned with protecting or regulating privacy by means of legal instruments like legislation. Other accounts focus on the implementation of privacy provisions in legislation or the way courts handle privacy issues.[31] Yet others address both the theoretical and practical legal aspects of privacy.[32] And they do this for good reasons. Society is changing, and cases arise all the time that do not adequately fit the current legal doctrine. Such hard cases, as they are called, give rise to reflection upon the principles on which a particular legal doctrine is founded. In 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—the cases that give rise to consider changing legislation or legal theory. Hence we need to look at both the current legal practice and the principles and theory underlying the concept of privacy. We start our little tour of the concept of privacy reviewing the various discussions that have taken place, and are still taking place, with respect to privacy.

29. *Cf.* PETER BLOK, HET RECHT OP PRIVACY [THE RIGHT TO PRIVACY] (2002).

30. *See* Charles Fried, *Privacy*, 77 YALE L.J. 475, 477 (1968) (arguing "privacy is not just one possible means among others to insure some other value, but . . . it is necessarily related to ends and relations of the most fundamental sort: respect, love, friendship and trust."); WESTIN, *supra* note 14; James Rachels, *Why Privacy Is Important*, 4 PHIL. & PUB. AFF. 323 (1975).

31. *See, e.g.,* LEE A. BYGRAVE, DATA PROTECTION LAW: APPROACHING ITS RATIONALE, LOGIC AND LIMITS (2002).

32. *See, e.g.,* BLOK, *supra* note 29.

Bygrave offers a distinction in four major ways in which the concept of privacy is defined that is useful for our analysis.[33] The first group of definitions takes non-interference as its starting point, a conceptualization highly influenced by Samuel Warren and Louis Brandeis' seminal 1890 paper, *The Right to Privacy: The Implicit Made Explicit*.[34] 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."[35] People, for example, should not be photographed by the press at its whim, unless they choose to "go public" themselves.

The second group of definitions centers on the degree of access to a person. Ruth Gavison gave an influential and popular definition in this category,[36] which defined 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.[37]

A third group sees privacy in terms of information control. Westin,[38] Fried,[39] Rachels,[40] and also Lessig[41] 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."[42] Fried and Rachels echoed his definition of privacy: "the *control* we have over information about ourselves";[43] "our ability to control who has access to us."[44]

The fourth definition group relates privacy closely to intimate or sensitive information. Julie Inness promotes this privacy concept: "privacy is the state of possessing control over a realm of intimate decisions, which includes decisions about intimate access, intimate information,

33. BYGRAVE, *supra* note 31, at 128–29.
34. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy: The Implicit Made Explicit*, 4 HARV. L. REV. 193 (1890).
35. *Id.* at 206.
36. Ruth Gavison, *Privacy and the Limits of Law*, 89 YALE L.J. 421 (1980).
37. *See id.* at 423.
38. *See* WESTIN, *supra* note 14.
39. *See* Fried, *supra* note 30.
40. *See* Rachels, *supra* note 30.
41. *See* LESSIG, *supra* note 11.
42. WESTIN, *supra* note 14, at 7.
43. Fried, *supra* note 30, at 482.
44. Rachels, *supra* note 30, at 326.

and intimate actions."[45] This may also enhance personal expression and choice.

B. *Privacy Laws*

As privacy has found its way into 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. 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. Though not explicitly mentioned, Warren and Brandeis could argue that a right to privacy exists.[46] A combination of Amendments, including the Third,[47] Fourth,[48] Fifth,[49] Tenth[50] and Fourteenth Amendments,[51] and possibly the First,[52] is generally seen to cover the basic aspects of privacy.[53]

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, for instance,[54] in Title III of the Omnibus Crime Control and Safe Streets Act of 1968 on wiretapping,[55] the Privacy Act of 1974,[56] the Cable Communications Policy Act of 1984,[57] the Electronic Communications Privacy Act of 1986,[58] the Video Privacy Protection Act of 1988,[59] the Employee Polygraph Protection Act of 1998,[60] and the Telephone Consumer Protection Act of 1991.[61] At the

45. JULIE C. INNESS, PRIVACY, INTIMACY, AND ISOLATION 140 (1992).
46. *See* Warren & Brandeis, *supra* note 34.
47. *See* U.S. CONST. amend. III.
48. *See* U.S. CONST. amend. IV.
49. *See* U.S. CONST. amend. V.
50. *See* U.S. CONST. amend. X.
51. *See* U.S. CONST. amend. XIV.
52. *See* U.S. CONST. amend. I.
53. Justice Douglas, for instance, upheld this idea in his famous "penumbra" argument in *Griswold v. Connecticut*, 381 U.S. 479, 482–85 (1965).
54. *See* Marc Rotenberg, *Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get)*, 2001 STAN. TECH. L. REV. 1, ¶ 26, http://stlr.stanford.edu/STLR/Articles/01_STLR_1/index.htm.
55. 18 U.S.C. §§ 2510–2520 (2000).
56. *See* 5 U.S.C. § 552a (2000) (establishing a legal framework for the records collected by the federal government).
57. 47 U.S.C. §§ 521–611 (2000) (cable television).
58. 18 U.S.C. §§ 2510–2522, 2701–2711 (2000) (amended 1988) (electronic mail).
59. 18 U.S.C. § 2710 (2000) (video rental records).
60. 29 U.S.C. §§ 2001–2009 (2000) (lie detectors).
61. 47 U.S.C. § 227 (2000) (auto-dialers and junk faxes).

state level, there are many more. Rotenberg argues that these sectoral laws, and the privacy provisions therein, are the result of new technologies entering the market and the need to regulate new technologies' intrusive monitoring.[62]

In the European Continental tradition, there is a history of privacy protection, both in the various constitutions, as well as in various national laws resulting from their implementation of European Community Directives.[63] The cornerstone of European privacy protection is Article 8 of the European Convention on Human Rights and Fundamental Freedoms (ECHR), 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.[64]

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

1. *Physical Privacy* is 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 on intrusion into the home and other physical environments—such as the workplace[65] (territorial privacy). This covers searches, video surveillance, and other forms of monitoring.

2. *Relational Privacy* is both the security and privacy of communications—such as mail, telephones, e-mail, and direct

62. Rotenberg, *supra* note 54, ¶¶ 27–28.

63. See, *for example, the EC Data Protection Directive.* Council Directive No. 95/46, 1990 O.J. (L 281) 31, *available at* http://www.dataprotection.ie/viewdoc.asp?DocID=93.

64. Council of Europe, European Convention on Human Rights and Fundamental Freedoms [ECHR], art. 8, Nov. 4, 1950, 213 U.N.T.S. 222.

65. The workplace can also be protected by Article 8 of the ECHR. *See id.*; *see, e.g.*, Niemitz v. Germany, 16 Eur. Ct. H.R. (ser. A) at 97 (1992); Halford v. United Kingdom, 24 Eur. Ct. H.R. 523 (1997).

communication—and the privacy of personal or intimate relationships—such as family life.

3. *Informational Privacy*, included in the private life and especially developed in the EC Data Protection Directive,[66] is the protection of informational privacy. This protection involves the establishment of rules governing the collection and handling of personal data—such as credit information and medical and government records.

C. *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. Considerations of the common good can justify breaches of privacy. 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 contested continually.

Etzioni,[67] 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."[68] 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 of the ECHR.[69] 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 and 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 means that a privacy violation has to be proportional to its goals, and the goal cannot 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 so that citizens are able to know in what circumstances their privacy may 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

66. *See* 1990 O.J. (L 281) 31.
67. ARMITAI ETZIONI, THE LIMITS OF PRIVACY (1999).
68. *Id.* at 4.
69. *See* ECHR, *supra* note 64, art. 8(2).

member states. As such, balancing the various interests is inherent to the European data-protection regime.[70]

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 Amendment's prohibition of "unreasonable searches and seizures."[71] In 1968, the Supreme Court, in *Katz v. United States*,[72] held unconstitutional the federal authorities' unwarranted placement of an electronic listening device on the outside of a public phone booth to record a phone conversation.[73] 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."[74] In a large number of cases, the reasonable expectation of privacy has been the test to decide whether the government has unconstitutionally breached someone's privacy. Thus, 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."[75]

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(2) of the ECHR.[76] The concept, nevertheless, plays a role in the European outlook on privacy. The balancing test to determine when a privacy violation is necessary in a democratic society, after all, depends on the seriousness of the privacy violation, which in turn relies, to a certain extent, on the way or amount of privacy people experience in the particular context. This is one of the reasons why a closer look at the relation between technology and privacy is warranted. People will generally base their online expectations on offline experiences and will expect to have the same level of protection online as they have offline. In the case of new, privacy-invasive technologies, the user will have a false expectation of privacy. Hence, the use of such technologies will be considered a greater violation of privacy. This requires the interest served by

70. *See* PAUL DE HERT, PRIVACY EN HET GEBRUIK VAN VISUELE TECHNIEKEN DOOR BURGER EN POLITIE [PRIVACY AND THE USE OF VISUAL TECHNOLOGIES BY CITIZENS AND POLICE] (1998).

71. U.S. CONST. amend. IV.

72. 389 U.S. 347 (1967).

73. *See id.* at 348, 359.

74. *Id.* at 361 (Harlan, J. concurring).

75. See CATE, *supra* note 16, at 57 (internal quotes omitted) (footnote omitted).

76. ECHR, *supra* note 64, art. 8(2).

infringing the privacy of the user to have more weight if such a use is to be allowed under the balancing test of Article 8(2) of the ECHR.[77]

D. *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.[78]

One of the problems with technology and privacy is that in some instances breaches of privacy occur in situations where the users of the technology are unaware of the possible breaches because they expect to have privacy. Radio, and later television, was 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 broadcast radio, the technology does not affect people's privacy. This changed with the introduction of cable networks in the 1970s and advances in content encryption. These means provided content providers with more control over their audience, and it opened the way to subscription-based broadcasting and pay-per-view models. The different types of subscription models have different effects on the privacy of the users. Whereas a subscription model generally provides information only on the channels to which a subscriber subscribes, a pay-per-view model implies insight into the programs to which a subscriber listened. This data, by virtue of being relatable to subscriber data, does impact people's privacy.

The Internet has become an important channel for the delivery of audiovisual content in ways that resemble the traditional radio and television broadcasting. Streaming-media protocols, such as the Real Time Streaming Protocol (RTSP)[79] and Real-Time Protocol (RTP),[80] enable anyone with a broadband Internet connection to set up on-demand delivery of real-time data, both audio and video, in live data feeds or stored clips. Delivery can take place either unicast, in which the client chooses

---

77. In the European Union, that is. *See id.*

78. Recently, one form of webcasting has been popularly dubbed "podcasting" in reference to the recipient's ability to download the media to a portable player (like an iPod) so she can enjoy the media at the most convenient time. *See* Podcasting, WIKIPEDIA, http://en.wikipedia.org/wiki/podcasting (last visited Nov. 15, 2005).

79. *See* HENNING SCHULZRINNE ET AL., INTERNET ENGINEERING TASK FORCE (IETF), REAL TIME STRAMING PROTOCAL (RTSP) (1998), ftp://ftp.ietf.org/rfc/rfc2326.txt.

80. *See* HENNING SCHULZRINNE ET AL., IETF, RTP: A TRANSPORT PROTOCAL FOR REAL-TIME APPLICATIONS (1996), ftp://ftp.ietf.org/rfc/rfc1889.txt.

what and when to receive, or multicast, in which 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 internet protocol (IP) address) and the content to be broadcast.

Webradio has become quite popular, and many traditional radio stations use it 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 or DSL).

The fact that a 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 relates to the content provided. Most material broadcast is copyrighted material, and, hence, webradio or webcasting touches upon copyright law. Although it is being debated whether webcasters are to pay license fees and to whom—the artists or the record industry, the case has been settled in many countries.[81] Webcasters generally need a license agreement with the copyright holder or the representatives of the copyright holders, such as the SENA in the Netherlands, for instance. The webcaster has to pay remuneration for each track (song) streamed for each listener.[82]

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 mediaplayer, iTunes for instance, requests a particular webradio station to start streaming content to the client. The webcaster therefore knows exactly which clients tune in to its broadcast, when, and for how long. 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 this data in their quarterly reports to rights-holders. Accordingly, the webcasters 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 address. IP addresses can be

81. *See, e.g.*, Bonneville Int'l Corp. v. Peters, 347 F.3d 485 (3d Cir. 2003).

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

traced back to individuals in some instances and, thus, can be identifiers.[83] Consequently, data maintained by webcasters can be used for monitoring and profiling listeners.

For a hypothetical user, Ronald, his privacy could be impacted by listening to a webcast of music. An individual webcaster of, say, Lowlands Jazz, may be able to infer information from the patterns Ronald's computer leaves in the webcaster's listeners log. It may tell something about Ronald's taste because he tends to tune in to another station (unknown to the LowLands Jazz station) at moments that suggest his taste to be the motivator (for instance, after a couple of notes or the start of a new program). Or, it may reveal something about his living habits if patterns occur in the times he tunes in to the station (such as, usually on weekends rather than working days, except Tuesdays, which turns out to be his day off). The impact on the listener's privacy increases if various listener logs are merged, especially if they are combined with other online traces, like website logs, which also contain IP addresses.

Most people are aware of the fact that IP addresses 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, in principle, can 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 diminishment of privacy? If we apply Etzioni's (communitarian) test,[84] 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. Because IP addresses are unique, they provide convenient metering units. Is this enough to warrant the diminishing of the privacy protection? Not necessarily, especially if

83. *See* Dutch Data Protection Authority, Een IP-adres is niet altijd een persoonsgegeven [An IP-Address Is Not Always a Real Person], http://www.cbpweb.nl/documenten/uit_z2000-0340.htm (last visited Oct. 22, 2004).

84. ETZIONI, *supra* note 67, at 183–215, proposes a test for determining whether privacy and the common good are out of balance. Privacy should be limited only 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 accord with the subsidiarity principle (as a last resort) and be proportional (minimally intrusive). *Id.*

there are less intrusive ways to measure the number of listeners at any give time.

Nevertheless, it may well be that the new privacy infringement goes unnoticed or unheeded by the public and government at large, thereby *de facto* establishing a new—*lower*—privacy standard. Perhaps as people get used to being "watched" by webradio, they will no longer mind that this affects their personal lives, and they will not regard as reasonable an expectation of privacy when listening to webradio.

E. *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 wrote: "What must be hidden before the eyes of others, seems to differ from society to society."[85] In a recent paper, he discusses two western cultures of privacy.[86] The European culture on the one hand, 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 Germans call the *right to informational self-determination* . . . ."[87] On the other hand, the U.S. tradition is oriented toward "values of liberty, and especially liberty against the state."[88] This emphasis on liberty is in line with the traditional American, fearful pre-occupation with state intrusions, especially in one's own home.[89] These differences in core values have consequences as to what should be protected against intrusion. In continental Europe, credit-card reporting, for instance is seen as a "dangerous exposure of private life to most Europeans"[90] and is governed by strict regulation; whereas in the U.S., it is common practice. Dignity in the continental mind is no less important than market efficiency.[91] Also, workplace e-mail and consumer data are deemed much more wor-

85. Whitman, *supra* note 28, at 1161.

86. *See id.*; Joel R. Reidenberg, *Resolving Conflicting International Data Privacy Rules in Cyberspace*, 52 STAN. L. REV. 1315 (2000), *available at* http://reidenberg.home.sprynet.com/international_rules.pdf (comparing the U.S. and European approaches to privacy).

87. Whitman, *supra* note 28, at 1161 ("the right to control the sorts of information disclosed about oneself") (footnote omitted).

88. *Id.*

89. *See id.* at 1161–62.

90. *Id.* at 1192.

91. *Id.* at 1192–94.

thy of protection in continental Europe than in the U.S.[92] Whitman also notes examples where U.S. privacy protection is much stronger than continental protection. Phone wiretapping by the police in many European countries occurs much more frequently than in the U.S., and is perfectly legal.[93] Another continental interference with private affairs that may strike Americans as odd is the fact that judges can intervene with respect to the name parent's give their newborn baby.[94]

Not only is there a difference in what is deemed suitable for protection under the guise of privacy between societies, but each society's concept also changes over time.[95] Societal changes such as changing attitudes with respect to moral standards, to clothing, and to behavior are well described.[96] Most dramatic may be the impact of recent terrorist attacks on privacy notions.

The impact of ICT on the concept of privacy is given ample consideration in research.[97] It has almost become commonplace to assert that developments in the fields of ICT have had a tremendous influence on policymaking, regulation, and legislation with regard to privacy. But other factors have been important as well. First, 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 going on still. 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 is used. Second, past decades witnessed growing internationalization, not to say globalization, 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, and the fading importance of national boundaries—have influenced the regulation of privacy, and they have

92. *See id.* at 1194–95.

93. *See id.* at 1158–59.

94. Such a case arose when French parents decided to call their daughter "Mégane Renaud," pronounced the same as Renault Mégane, a popular French car at the time. Although the courts ultimately decided not to overrule the parents, they could have done so. *See id.* at 1217 (citing CA Rennes, 6e ch., May 4, 2000, J.C.P. 2001, IV, 2655, note Pierre & Boizard). "The court's opinion emphasized that the parents had not any 'arrières-pensées'—that is, any unacknowledged or ulterior intentions, and that the car model in question would likely go out of production by the time the child reached school age." *Id.* at 1195 n.324.

95. *See, e.g.*, BARRINGTON MOORE, PRIVACY: STUDIES IN SOCIAL AND CULTURAL HISTORY (1984).

96. *See* WESTIN, *supra* note 14.

97. *See, e.g.*, CATE *supra*, note 16; Julie E. Cohen, *DRM and Privacy*, 18 BERKELEY TECH. L.J. 575 (2003); Froomkin, *supra* note 8; Schwartz, *supra* note 6.

contributed to changes in the meaning and significance assigned to privacy, both by ordinary citizens and by legislatures and policy makers.

In turn, this increasing attention of legislatures and policy makers towards privacy 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.

Johnson nicely summarizes the image we have described so far: "[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."[98]

This raises the question of how to evaluate the possible influence of "code" on this fluid notion of privacy without resorting to abstract truisms. Some authors, such as Vedder,[99] have proposed a contextual-functional framework that does justice to the influence of contextual factors, and—at the same time—enables us to understand how and why the notion of privacy works in that context. This means that we should depart the normative point of privacy and instead take an instrumental view: privacy is not an end in itself, but merely a means to achieving other goals.[100] The goals promoted by privacy are abundantly discussed in literature. For instance, Johnson proposes "personal freedom";[101] Benn puts forward a limited set of subdimensions of freedom: the freedom of self-presentation and moral autonomy.[102] Such monistic values do not help us accomplish our goal to make more specific statements and to transcend the level of abstract truisms. To accomplish this goal, we can join Vedder,[103] who rejects monistic underlying values and instead proposes that we look at particular contexts to denote the functions and values of privacy in these contexts. In this view, privacy is an instrumental value that can serve the fulfillment 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 can be relevant depending on the particular situation.

---

98. Jeffrey L. Johnson, *Privacy and the Judgment of Others*, 23 J. VALUE INQUIRY 157, 157 (1989).

99. *See* A.H. Vedder, *Medical Data, New Information Technologies, and the Need for Normative Principles Other than Privacy Rules*, *in* LAW AND MEDICINE, 441, 447–53 (Michael Freeman & Andrew Lewis eds., 2000). *But cf.* Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119 (2004), *available at* http://crypto.stanford.edu/portia/papers/RevnissenbaumDTP31.pdf.

100. *See* BYGRAVE, *supra* note 31, at 125; CATE, *supra* note 16, at 101–02.

101. Johnson, *supra* note 98.

102. STANLEY I. BENN, A THEORY OF FREEDOM 311–12 (1988).

103. Vedder, *supra* note 99, at 447–53.

Therefore, in order to analyze how "code" affects the balance between privacy and other interests, we look at various fields in which privacy-related "code" is at work, and try to assess what privacy means in that specific context. To be able to denote what underlying values and functions privacy may serve in those particular contexts, we shall outline some candidates. For our present purposes, a list provided by Bygrave suffices.[104] This list contains a number of values that recur in the extensive literature on values and interests served by privacy. Bygrave distinguishes individual and societal values privacy protection serves. The core individual values follow:

- *Individuality*: Individuality reflects the fact that we want to see ourselves as individual persons. The protection of individuality means a protection against flattening out, becoming one-dimensional. Profiling is a technology that touches upon this sense of individuality, as it assigns characteristics to individuals based on characteristics of others.
- *Autonomy*: This value is related to individuality; it is a person's ability to make his own choices.
- *Dignity*: Dignity is the right to be shielded against unwanted public exposure—to be spared embarrassment or humiliation. Whitman even calls dignity the core of privacy in the continental tradition.[105]
- *Integrity*: This is the right to be taken as a whole. This value is closely associated with dignity, autonomy, and individuality.
- *Emotional release*: 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 to be "herself."
- *Self-evaluation:* 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.
- *Protected communication*: This relates to the notion of being able to communicate with others confidentially, without running the risk of being overheard. This value is closely related to the core U.S. value of freedom (of expression).[106]

104. *See* BYGRAVE, *supra* note 31, at 133–35.
105. Whitman, *supra* note 28, at 1161.
106. *See* U.S. CONST. amend. I.

For society as a whole, privacy serves important values. Civility, stability, pluralism, and democracy are central values in this respect. On the other hand, giving up one's private sphere and disclosing personal data also has values which are important for society. Walker provided a comprehensive list of values of foregoing privacy.[107]

- *Cost*: 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.[108]
- *Access*: Personalization (with preferences derived from a user's conduct), customization (with preferences derived from a user's expressed desires), and interactivity (interaction with a website to obtain a user's tailored content) add value to online experience and result in repeated access of sites offering these facilities.[109]
- *Convenience*: Convenience results from the fact that services can be tailored to particular users or clients thereby focusing the interaction, for instance, by offering purchase recommendations.[110]
- *Collaboration*: Collaboration is important, as some services can only be offered if sufficient numbers of collaborators exist. Telephone directories, for instance, only have value if a sufficient number of telephone subscribers are listed.[111]
- *Community*: Community refers to a social need to know the people one engages with; compare the Cheers opening song, "You want to go where everybody knows your name."[112]
- *Security*: Security of online transactions can be improved by means of identification and authentication. Credit-card fraud can be traced and noticed when credit-card companies have access to the cardholder's spending history.[113]

107. Kent Walker, *Where Everybody Knows Your Name: A Pragmatic Look at the Costs of Privacy and the Benefits of Information Exchange*, 2000 STAN. TECH. L. REV. 2, http://stlr.stanford.edu/stlr/articles/00_stlr_2/index.htm.
108. *See id.* ¶¶ 28–33.
109. *See id.* ¶¶ 34–39.
110. *See id.* ¶¶ 40–43.
111. *See id.* ¶¶ 44–50.
112. *See id.* ¶¶ 51–61.
113. *See id.* ¶¶ 62–68.

- *Accountability/responsibility*: Anonymous interaction in cyberspace is thought to facilitate "wrongs"; it is sometimes presumed that these wrongs can be prevented if people do not interact anonymously.[114]
- *Trust*: Trust in online relationships can often not be based on the parties' knowing each other. Sharing personal data makes it possible to find out more about whether a party is trustworthy.[115]

III. "CODE" AND PRIVACY IN CONTEXT

What do we mean by "code" and privacy? The relationship between "code" and intellectual property is relatively clear.[116] For instance, code embedded in media players in the form of Digital Rights Management (DRM) systems makes people conform to the rules the designer of the media player put forward, who, no doubt, has implemented these in accordance with the wishes of the rights-holders of the media. "Code" in this context precludes violations and automates the enforcement of public decisions.[117]

The relationship between "code" and privacy is less clear. Obviously, technology may affect privacy. Technology facilitates monitoring and surveillance as vaster amounts of personal data can be collected and processed, thus affecting informational privacy. But can "code" with respect to privacy play a role similar to that in the context of intellectual property, as exemplified by DRM systems? It can, but there is a discrepancy. Whereas one might see "code" as a threat to privacy, the opposite, actually, is more likely to be the case. "Code" can be used to prevent actors and organizations from breaching privacy, just as "code" precludes violations of copyright law via DRM systems. In the context of "code" and privacy, "code" has the potential to protect the rights of the users, whereas in the context of IPR, and also of "code" and speech, it has the potential to limit the individual's rights.

Privacy–protecting rules can be hardwired within the infrastructure of the Internet and applications. Two prominent examples are the World

114. *See id.* ¶¶ 69–77.

115. *See id.* ¶¶ 78–82.

116. *See* Natali Helberger, *Fence on Fence Can: Intellectual Property and Electronic Self-Regulation*, in CODING REGULATION, *supra* note †, *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=817769.

117. *See* Joel R. Reidenberg, *States and Internet Enforcement*, 1 U. OTTAWA L. & TECH. J. 213, 225–29 (2004), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=487965.

Wide Web Consortium's (W3C) projects Platform for Internet Content Selection (PICS)[118] and Platform for Privacy Preferences Project (P3P).[119] PICS allows content providers to add metadata describing the nature of the content. PICS also allows for filters to be designed that filter content on the basis of the user's preferences. It was originally intended to help parents and teachers to determine what children can access on the Internet. But also, privacy-protecting metadata and filters can be assigned.[120] In this case content providers are required to label their content with metadata describing their use of data provided by the user. The user's application (a web browser, for instance) can then decide on the basis of these labels whether a particular website acts in accordance with her wishes.

The Platform for Privacy Preferences Project (P3P) provides an automated way for users to gain more control over the use of their personal information on web sites they visit. Web sites store information about the way they handle personal information in machine-readable form (XML). The user stores her own privacy preferences in her browser, which then compares the website's privacy characteristics with the user's preferences and decides whether to enter the website or not.

Another 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.[121] Microsoft built the European data privacy protections directly into the company's technology.[122]

This notion of "code" and privacy, where "code" appears to protect privacy, rather than to infringe upon it, runs counter to what we actually perceive. This discrepancy exists if we do not separate the different kinds, or uses, of "code" or technology in general. Technology in many ways threatens privacy. If we take "code" to indicate technology or code in a broad sense, it then, by itself, is often privacy-threatening in the sense that it can be used to invade 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.

---

118. Platform for Internet Content Selection, http://w3.org/PICS (last visited Nov. 15, 2005).

119. P3P Public Overview, *supra* note 22.

120. *See, e.g.*, Jean-Marc Dinant, Using PICS as an Enhanced Privacy Protection Technology?, http://www.droit.fundp.ac.be/crid/eclip/pics.html (last visited Nov. 15, 2005) (draft).

121. The Article 29 Working Party is the consortium of the European data-protection supervisory authorities that monitors compliance with EU data-protection regulation. *See* Justice & Home Affairs, Art. 29 Data Protection Working Party, http://europa.eu.int/comm/justice_home/fsj/privacy/workinggroup/index_en.htm (last visited Nov. 15, 2005).

122. *See* Reidenberg, *supra* note 117, at 218–19; Helen Jung, *Microsoft Agrees to Changes in Passport*, INFORMATION WEEK, Jan. 30, 2003, available at http://www.informationweek.com/showArticle.jhtml?articleID=6512119.

For the purposes of this Article, 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.[123] But since privacy is all about balance, the other meaning of built-in rules is useful: 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 start with a general notion of privacy-influencing technology and then indicate whether and how privacy-protecting norms could be built into technology as a possible part of addressing potential shifts in protection.

A. *Law Enforcement*

As of old, law enforcement is one of the prime contenders in privacy debates. By nature, law enforcement should uncover what is hidden and what people would 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 privacy is clearly 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 still would protest if the police installed a camera in their bedroom to prevent marital murders. Privacy in the context of protection from government intrusion into its citizens' private sphere remains 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, surveillance and digitalization, 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. Further ahead looms the use of technologies like Radio Frequency Identification (RFID),[124] ambient

123. *See infra* Part VI.

124. ANN CAVOUKIAN, ONTARIO INFORMATION AND PRIVACY COMMISSIONER, TAG, YOU'RE IT: PRIVACY IMPLICATIONS OF RADIO FREQUENCY IDENTIFICATION (RFID) TECHNOLOGY (2004), http://www.ipc.on.ca/docs/rfid.pdf.

intelligence,[125] and "smart dust"[126] that may enable systematic, covert, and perfect tracking and observation of people in 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 digitized, and online methods replace offline methods of doing things in communication, banking, shopping, education, photography, archiving, and a myriad of other things. This means that an ever-increasing amount of data about one's personal life is digitized and stored somewhere. In turn, this enables law enforcement to gather much more data with online powers than was available to them with matching offline powers. To illustrate how these developments work in practice, we will sketch two examples that show various ways in which "code" functions in the law-enforcement context.

1. 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 now one of the most vital tools for investigating and prosecuting crime.

With the telecommunications developments 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 as easy to intercept technically. Therefore, governments decided to establish regulations that demanded the telecommunications industry build a wiretapping capability into their technology, thus guaranteeing it was at least technically feasible for law enforcement to continue to intercept, regardless of further technological developments.

---

125. Ambient intelligence is "a pervasive and unobtrusive intelligence in the surrounding environment supporting the activities and interactions of the users." Giuseppe Riva et al., *Presence 2010: The Emergence of Ambient Intelligence*, *in* BEING THERE: AMBIENT INTELLIGENCE 61 (G. Riva, Fabrizio Davide & Wijnand A. IJsselsteijn eds., 2003), *available at* http://www.vepsy.com/communication/book4/4_04riva.pdf; *see* Ambient Intelligence Research Group, http://www.ambientintelligence.net/ (last visited Nov. 15, 2005).

126. "Smart dust" is a sensor system implemented via objects of 1 cubic millimeter. *See, e.g.*, Matthew Last, Optical Communications Project Overview, http://www-bsac.eecs.berkeley.edu/~mattlast/research/index.html (last visited Nov. 15, 2005); Kris Pister et al., Smart Dust: Autonomous Sensing and Communication in a Cubic Millimeter, http://robotics.eecs.berkeley.edu/~pister/SmartDust/ (last visited Nov. 15, 2005).

In the United States, the Communications Assistance for Law Enforcement Act of 1994 (CALEA) was passed in October of 1994.[127] 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."[128] 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.[129] Moreover, the law also demands a certain number of simultaneously interceptable lines[130]—a provision that led to fierce debates when the Federal Communications Commission made proposals to implement it.[131] The law provides a "safe harbor" for telecommunications carriers if they comply with publicly available technical requirements or adopted standards of an industry association or standard-setting organization.[132] In turn, manufacturers of telecommunications equipment and providers of support services are required to supply telecommunications carriers with equipment and services that comply with the interceptability requirements.[133]

Pursuant to CALEA, the telecommunications 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, for example, 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.[134]

---

127. Pub. L. No. 103-414, 108 Stat. 4279 (1994) (codified in scattered sections of 18 U.S.C. and 47 U.S.C.), *available at* http://www.askcalea.net/calea.html.

128. AskCALEA, Frequently Asked Questions, http://www.askcalea.net/faqs.html#04 (last visited Nov. 15, 2005).

129. *See* 47 U.S.C. § 1002(a) (2000).

130. *See* 47 U.S.C. § 1003 (2000).

131. *See* U.S. Telecom. Ass'n v. FCC, 227 F.3d 450, 465 (D.C. Cir. 2000) ("Although the Commission appears to have interpreted the J-standard as expanding the authority of law enforcement agencies to obtain the contents of communications, . . . the Commission was simply mistaken."); Further Notice & Proposed Rule, 13 F.C.C.R. 22632 (1998); Public Notice, 13 F.C.C.R. 13786 (1998).

132. *See* 47 U.S.C. § 1006 (2000); AskCALEA, Standards, http://www.askcalea.net/standards.html (last visited Nov. 15, 2005). Although "publicly available," the standards are not cheap: for instance, it costs $352 to download standard J-STD-025-B-2003. Alliance for Telecommunication Industry Solutions, Doc. No. J-STD-025-B-2003, https://www.atis.org/atis/docstore/doc_display.asp?ID=2570 (last visited Nov. 15, 2005).

133. *See* 47 U.S.C. § 1005(b) (2000).

134. *See* Communications Assistance for Law Enforcement Act, 14 F.C.C.R. 16794, 16825–33, 16842–46 (1999); U.S. Telcom. Ass'n, 227 F.3d at 465.

Telecommunications 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."[135]

The United States has not been the only country to pass legislation on interceptability. Indeed, the European Union quickly followed the U.S. with the Council Resolution of January 17, 1995,[136] which outlined quite similar requirements for interceptability. Arguing that "interception may only be effected insofar as the necessary technical provisions have been made," the resolution listed a summary of the law–enforcement needs "for the technical implementation of legally authorized interception in modern telecommunications systems."[137] 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 standardization organizations (IEC, ISO, and ITU)[138] in December 1995, pointing out the resolution and "inviting" the organizations to take account of the requirements,[139] but neither the EU resolution nor the national implementation laws explicitly refer to standard-setting bodies or require telecommunications manufacturers to develop interceptable equipment. Apparently, the task was left more to industry itself—both telecommunication providers and manufacturers—to develop and to incorporate interceptable equipment and services.

Although several industry and standardization bodies, such as the U.S. TIA[140] and ATI[141] and the European ETSI,[142] have been working on incorporating interception norms in the technology, other bodies have consciously refrained from doing so. It is instructive to read the state-

135. AskCALEA, Frequently Asked Questions, http://www.askcalea.net/faqs.html#12 (last visited Nov. 15, 2005).

136. Council Resolution of 17 January 1995, 1996 J.O. (C 329) 1 (Resolution on the Lawful Interception of Telecommunications).

137. *Id.*

138. *See* International Engineering Consortium, http://www.iec.org (last visited Nov. 15, 2005); International Organization for Standardization, Homepage, http://www.iso.org (last visited Nov. 15, 2005); International Telecommunication Union, http://www.itu.int/home (last visited Nov. 15, 2005).

139. *See European Union and FBI Launch Global Surveillance System*, STATEWATCH BULL., Jan.–Feb. 1997, *available at* http://www.statewatch.org/eufbi/eufbi01.htm.

140. *See* Telecommunications Industry Association Online, http://www.tiaonline.org (last visited Nov. 15, 2005).

141. *See* Advanced Technology Institute, Advancing Technology Through Collaboration, http://www.aticorp.org/ (last visited Nov. 15, 2005).

142. *See* European Telecommunications Standards Institute, http://www.etsi.org (last visited Nov. 15, 2005).

ment 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.[143] 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 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 of 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.[144]

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 its designers did not intend.

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 investigative power of interception. Industry has, naturally, complied with these legal requirements, and hence, telecommunications infrastructures have a built-in capacity for interception, including more detailed interception features according to the government requirements. This is not to say that telecommunications technology is inherently privacy-infringing, but it is, thus, at least, capable of being privacy-infringing.

---

143. IETF POLICY ON WIRETAPPING, THE INTERNET GROUP (2000), http://www.ietf.org/rfc/rfc2804.txt (last visited Nov. 15, 2005) (endorsed by the Internet Architecture Board and Internet Engineering Steering Group).

144. *Id.* at 4–5.

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—telecommunications 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.[145]

2. Case 2: Cryptography

"Cryptography" indicates systems that alter data so that unauthorized people cannot understand the data. 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 cryptography 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 *en*coding key, he is none the wiser because he does not know the *de*coding key.[146]

Until the 1970s, most cryptography systems could be cracked. But the new generation of cryptography systems that emerged in the 1970s has turned out to be virtually uncrackable, no matter the effort taken. (This is in theory, at least; in practice, implementations and use of secure

145. *See, e.g.*, Electronic Privacy Information Center (EPIC), Carnivore Page, http://www.epic.org/privacy/carnivore/ (last visited Nov. 15, 2005) (listing EPIC's Freedom of Information Act, 5 U.S.C. § 552 (2000), activities concerning the FBI's Carnivore project).

146. For a more technical review of these cryptography developments, see Gary C. Kessler, An Overview of Cryptography, § 5.3–.4, May 1998, http://www.garykessler.net/library/crypto.html.

cryptography systems often turn out to have flaws.) It is a matter of computing power: to crack a message, one must try every possible key, and it takes literally ages before the right one is found. 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—stand empty-handed: wiretaps and computer searches are useless if all they find is garbled code.

The controversy this has created is twofold, relating to two different roles of government: protecting national security[147] and enforcing the law.[148] The latter part of the controversy, related to *domestic* cryptography use, is more complex than the first, which primarily deals with export controls. It was only in the early 1990s that governments realized cryptography could seriously hamper law enforcement.[149] Conceptually, there are two possible solutions to address this: either create mechanisms that ensure government access to decoding keys

147. *See infra* Part III.B.

148. *See* Bert-Jaap Koops, Crypto Law Survey (v. 23.0), Jan. 2006, http://rechten.uvt.nl/koops/cryptolaw/, for an overview of states' initiatives in cryptography legislation. The examples that follow can be found, with references, on Koops's website.

149. It must be remarked here that this still appears to be mainly a theoretical problem. There still is not really a law-enforcement problem with cryptography, even though it has been predicted ever since 1993 that law enforcement would soon become a joke because of cryptography. So far, cryptography appears to have blocked few criminal cases. Little public data is available. The *2002 Wiretap Report* for the Office the United States Courts mentions that "[e]ncryption 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." 2002 WIRETAP REPORT, ADMIN. OFFICE OF U.S. COURTS 5, http://www.uscourts.gov/wiretap02/2002wttxt.pdf. *See* Dorothy Denning & William Baugh, *Hiding Crimes in Cyberspace*, 2 INFO. COMM. & SOC'Y 251 (1999), *available at* http://www.cs.georgetown.edu/~denning/crypto/hiding1.doc (researching numerous cryptography cases related to searches, the majority of which encryption did not stop).

Our impression is that only in last few years, at least in the Netherlands, have police really encountered encryption that could not be cracked easily in any significant number of cases. Perhaps, in the future, criminal cryptography may indeed, therefore, become a real-life problem.

beforehand—for example, by having people deposit keys somewhere when they want to use cryptography—or mechanisms that ensure access to keys *afterwards*—by providing legal power that enables the police to force someone to give them a decryption key in case of a crime.

The U.S. government was one of the first to try the first, *ex ante* approach. In 1993, they launched the Clipper chip, a chip for telephone encryption with a built-in backdoor for government access.[150] They hoped that if enough people would voluntarily use this chip, the cryptography 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. was not the only country to try to curb cryptography's progress. In the Netherlands in 1994, a draft law was considered that virtually would have banned cryptography 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 deliberated schemes that resembled the Clipper chip. If Trusted Third Parties (TTPs) offer confidentiality services (for example, to provide customers with cryptography 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 to make sure the government could have access to cryptography keys without 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 TTPs would move abroad in that case; hence, the government refrained from further steps in this direction.

Similar developments took place in the U.K., where the government launched one consultation document after another with proposals for government backdoor access to encoded data. At first, such systems proposed to be mandatory, but later, the government said they could be voluntary.[151] In Germany, part of the government also favored mandatory

150. Many documents concerning Clipper and its aftermath can be found in BUILDING IN BIG BROTHER: THE CRYPTOGRAPHIC POLICY DEBATE (Lance J. Hoffman ed., 1995), and BRUCE SCHNEIER & DAVID BANISAR, THE ELECTRONIC PRIVACY PAPERS (1997).

151. *Compare* DTI, LICENSING OF TRUSTED THIRD PARTIES FOR THE PROVISION OF ENCRYPTION SERVICES: PUBLIC CONSULTATION PAPER ON DETAILED PROPOSALS FOR LEGISLATION ¶ 57 (1997), http://www.fipr.org/polarch/ttp.html ("The legislation will provide that bodies wishing to *offer* or *provide* encryption services to the *public* in the U.K. will be required to obtain a licence.") *with* DTI, BUILDING CONFIDENCE IN ELECTRONIC COMMERCE, CONSULTATION DOCUMENT ¶ 33 (1999), http://www.dti.gov.uk/cii/elec/elec_com_1.html ("[T]he Government has opted for a voluntary but statutory regime.").

backdoor-access schemes, but other government bodies opposed this.[152] 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 cryptography keys with a government agency, they could get a license for strong cryptography.[153]

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 others devised. For example, a study group from Royal Holloway University in 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, for example, time limits on wiretap warrants might be enforced technically.[154]

The extent to which cryptographers attempted to incorporate norms into technology is illustrated in Bellare and Rivest's article.[155] They 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."[156] This is not opaque, whereby 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 ρ of encrypted intercepts—where ρ is a number between 0 and 1. The amount of translucency, in their proposal, is to be established by parliament. This fraction ρ could vary with applications; for instance, whereas for domestic communications parliament might set ρ equal to 0.2 (allowing a relatively high level of privacy), they might require ρ to

152. See a summary in Koops, *supra* note 148 (select the "Germany" link), and links at Christopher Kuner, Cryptography Regulation, http://www.kuner.com/data/crypto/crypto.html (last visited Nov. 15, 2005).

153. Law No. 96-659 of July 26, 1996, Journal Officiel de la République Française [J.O.] [Official Gazette of France], July 27, 1996, p. 11384.

154. Nigel Jefferies, Chris Mitchell & Michael Walker, *A Proposed Architecture for Trusted Third Party Services*, *in* CRYPTOGRAPHY: POLICY AND ALGORITHMS, 1029 LECTURE NOTES IN COMPUTER SCIENCE 98, 99–100 (Ed Dawson & Jovan Golić eds., 1996).

155. Mihir Bellare & Ronald L. Rivest, *Translucent Cryptography: An Alternative to Key Escrow, and Its Implementation via Fractional Oblivious Transfer*, 12 J. CRYPTOLOGY 117 (1999), *available at* http://theory.lcs.mit.edu/~rivest/BellareRivest-translucent.ps.

156. *See id.* at 118–20.

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, because either some terrible crimes involving cryptography have occurred or elections were held recently and parties promised their voters to set ρ to a particular value. This, at least, is the world view emerging from the technical paper.[157] The point of this example is not that it is a realistic proposal, but that it shows the extent to which 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 cryptography use with this approach, it all came to nothing. By the late 1990s, backdoor-access schemes were out: Clipper had died a silent death;[158] the Dutch, U.K., and German governments thought better of it; and France abandoned the 1996 law and liberalized cryptography use in 1999.[159] There were several reasons for the failure of this backdoor approach. 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 from using 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. Even if non-backdoor cryptography 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, *ex post* approach. They have enacted laws that allow police to command people to decrypt or to hand over their cryptography keys. The Netherlands was the first to do so, in 1993.[160] More recently, the U.K.,

157. *See id.* at 129.

158. Colleen O'Hara & Heather Harreld, *DOD Sinks the Clipper*, FED. COMP. WEEK, Feb. 17, 1997.

159. *See* Decree No. 99-200 of Mar. 17, 1999, J.O., Mar. 19, 1999, p. 4951 (Fr); Decree No. 99-199 of Mar. 17, 1999, J.O., Mar. 19, 1999, p. 4050 (Fr).

160. *See Wetboek van Strafvordering* [Sv] [*Code of Criminal Procedure*], art. 125k, ¶ 2 (2003) (Neth.), *codified by* Wet computercriminaliteit [the Computer Crime Act], *Staatsblad van het Koninkrijk der Nederlanden* [Stb.] [*Official Gazette of of the Kingdom of the Netherlands*], 1993, p. 33.

Belgium, France, and a host of other countries have followed.[161] Thus, instead of relying on "code" to incorporate law-enforcement access, they have settled for a merely legal solution in the form of an investigative power: if the police encounter encoded data, they can command decryption.

The upshot is that cryptography 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 the export controls that effectively hampered law-abiding citizens and businesses from adopting strong cryptography on a large scale.[162] 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."

3. Balance

Technology appears to be a key driver in enabling law enforcement to pry deeper into the personal sphere, often invisibly and from a safe distance. The balance of privacy with new investigation powers is supposedly made time and again by the legislature and the courts, but because technology is developing, so is the reasonable expectation of privacy surrounding technology. After all, there is less expectation of privacy when surfing the Internet than when watching television at home or when walking streets that have clearly visible 24-hour camera surveillance. Likewise, the case of location data[163] suggests that perhaps somewhere in the not too far-away future, people's movements may also lose the reasonable expectation of privacy since localization is becoming an increasingly common side-effect of technology.[164]

161. *See* Regulation of Investigatory Powers Act, 2000, 23, §§ 49–55 (Eng.), *available at* http://www.opsi.gov.uk/acts/acts2000/20000023.htm; Law No. 2001–298 of Nov. 28, 2000, Moniteur Belge/Staatsblad [M.B.] [Belgian Monitor], Feb. 3, 2001, p. 2909, 2912 (amending Belgian Code of Criminal Procedure, art. 88); Law No. 2001-1062 of Nov. 15, 2001, O.J., Oct. 16, 2001, p. 18215 (amending French Code of Criminal Procedure, tit. IV), *available at* http://www.legifrance.gouv.fr/WAspad/UnTexteDeJorf?numjo=INTX0100032L. Also, see the entries on Australia, Ireland, Trinidad & Tobago, India, Malaysia, and Singapore in Koops, *supra* note 148; the latter three examples have limited scope only.

162. *See infra* Part III.B.2.

163. *See infra* Part III.B.1.

164. Michael Levi & David S. Wall, *Technologies, Security, and Privacy in the Post-9/11 European Information Society*, 31 J. L. & SOC'Y 194, 211 (2004) ("[A] by-product of . . . technologies is the traffic data flow that is generated through usage, which records the individual's movements, actions, and behavior.").

One, therefore, may argue that "code" is changing the traditional balance of privacy and law enforcement in many 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 also may be sweepingly monitored with speech and voice recognition and are increasingly subjected to data retention. Informational privacy disappears 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"—that is, 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 has 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? 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 also may 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 recognize. Anonymizers enable Internet activities with less of a chance of being traced. Sunglasses will help to thwart face recognition, and a Faraday cage will make your home impenetrable to electronic spies. Many examples like these can be given of technologies that help to counteract invasive technologies.

Nevertheless, the impression is that the privacy-threatening code is more developed and more widely used than the privacy-enhancing code. One of the reasons for this is that citizens themselves are responsible to use protective technologies, and they usually have no reason—and often no knowledge or awareness—to bear 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; 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 gained a definite foothold, if not with the general public, then at least with technology-aware citizens and criminals. But as the case of cryptography shows, governments have not been happy with privacy technologies, precisely for the reason that they hamper law enforcement. And although cryptography-curbing proposals and laws 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.[165] 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. The bottom line seems to be that law enforcement always trumps privacy.

B. *National Security*

The interest of national security is closely related to that of law enforcement; we, therefore, do not go into great detail here. Nevertheless, there is one significant difference worth mentioning. Protecting national security is, by its nature, closely intertwined with secrecy and stealth. Security agencies investigations thrive 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 (for example, sunbathers on a deserted stretch of beach), thermal imagers, and "smart dust"[166] are but a few examples of the increased potential for covert intelligence. We describe two areas that illustrate the various ways in which this increase occurs.

165. *Cf.* Alison A. Bradley, *Extremism in the Defense of Liberty? The Foreign Intelligence Surveillance Act and the Significance of the USA PATRIOT Act*, 77 TUL. L. REV. 465 (2002).

166. *See* Riva, *supra* note 125, and accompanying text.

1. Case 1: Location Data

One example of the ever increasing potential for information gathering is the booming area of location data. This is not specific to national security—we might equally well have treated it under the heading of law enforcement or commerce—but it is certainly an area where security agencies will benefit in ways not yet fully grasped.

Technically, localization is closely related to two technologies.[167] The first is mobile telephony, where network-based systems can locate a mobile phone, or cell phone. The network "knows" in which cell a phone is located, but not precisely where in the cell. However, as the granularity of the cells vary in size from a few hundred meters in city centers to tens of kilometers in sparsely populated areas, the precision with which the phone's location can be determined also ranges accordingly. This means that the precision can be fairly precise, at best. But there are ways to enhance localization to a scale of several to tens of meters, for instance, by triangulation using the speed and angle with which a mobile phone enters or leaves a cell and comparing signals received by various cells at the same time. Such refinements are being developed and installed in order to provide location-based service.[168]

The second technology is the Global Positioning System (GPS). This is a system of U.S.–owned satellites, initially launched and still in use for defense purposes, but increasingly also used in civil applications, that enable a handheld device to determine its location through the time and its position relative to three or more satellites. GPS enables localization with a precision of around ten meters; presumably, defense devices may reach a higher precision of around one meter. Contrary to the network-based location systems, the satellite network does not "know" where the device is, since it is the device itself that computes its location. Nevertheless, if combined with a mobile phone, wireless radio transmitter (in a GPS "transceiver"), or a disk and program that stores coordinates every minute (a GPS recorder), GPS can also give information about the location to third parties.[169]

---

167. *See* Linda Ackerman, James Kempf & Toshio Miki, *Wireless Location Privacy: Law and Policy in the U.S., EU and Japan*, THE INTERNET SOCIETY (ISOC) MEMBER BRIEFING #15 (2003), http://www.isoc.org/briefings/015/briefing15.pdf (providing an illuminating and brief description of the technologies).

168. This will be discussed further below.

169. Apart from these major technologies associated with mobile communications, it should be noted that other technologies may also increasingly provide location information. An example is RFID tags, *see infra* Part III.D.2, which might for instance lead to information about a person—or that person's clothes, shoes, or bag—entering or leaving a shop being stored in a database.

As David Phillips has shown, there are at least three major drivers behind emerging "wireless telecommunication systems" that "incorporate surveillance capacity, particularly the capacity to track and record individuals' locations."[170] The first—and for the U.S., perhaps the most important—is emergency response systems that can now benefit from location data from a caller's mobile phone to immediately track where the phone call—and presumably the emergency—originates and, through a combination of digital maps and routes, the fastest way to get there. The FCC has, through the Wireless Communications and Public Safety Act of 1999,[171] established "Emergency 911,"[172] requiring wireless operators to guarantee a high degree of localization. It is up to the operators whether they want to ensure this through network-based localization or GPS.[173]

The second driver behind location technologies is the business interest in location-based services (LBS). These are services based on fairly precise location data, within a range of several to tens of meters. Knowing the exact location of potential customers is immensely attractive for enterprises: it opens up opportunities for on-the-spot advertising ("Coming up on your right is a Wendy's—veggie burger for only $ .99!") and information services (call a national weather line and receive the local forecast). It also enables companies to track and to control employees ("Why did you stay at the local pub for forty minutes?") or simply to enhance efficiency (for example, taxi and shipping companies). A particularly interested sector is the automobile industry: car-navigation systems are booming, literally telling drivers how to get wherever they want to go; road-toll systems might efficiently compute tolls without cars having to slowly pass toll stations; rental-car companies can check speeding or driving on forbidden mud tracks; and car owners feel safer if the car is locatable in case of a carjacking. In fact, a major application seems to be parents' providing their children with location-indicating technology in order to safeguard against kidnapping.[174]

Finally, the third location-technology driver is surveillance. Law-enforcement and national-security agencies are interested in location

170. J. David Phillips, *Beyond Privacy: Confronting Locational Surveillance in Wireless Communication*, 8 COMM. L. & POL'Y 1, 1 (2003).

171. 47 U.S.C. § 615 (2000).

172. 911 Service, 47 C.F.R. § 20.18 (2005).

173. *See* Phillips, *Beyond Privacy*, *supra* note 170, at 3–5. For more extensive analysis, see J. David Phillips, *Texas 9-1-1: Emergency Telecommunications and the Genesis of Surveillance Infrastructure*, 30 TELECOMM. POL'Y (forthcoming 2006).

174. "[T]he main reason that these devices have suddenly gained popularity is their ability to track the location of children." Waseem Karim, *The Privacy Implications of Personal Locators*, 14 J.L. & POL'Y 484, 486 (2004). This is also one of the RFID technology uses that appear to gain increasing attention. *See infra* Part III.D.2.

information of mobile–phone calls. Telecommunication operators are required to make available to these agencies the location of the cells in which phone calls took place.[175] It is true that this has not driven the development of technology as much as the first two drivers—government surveillance has merely followed existing technological developments here. Nevertheless, there is a certain driving force here, particularly if mandatory data retention is enacted and made applicable to mobile location data.[176]

Now why is this important for national security? Security and intelligence agencies will benefit immensely from the host of detailed location information that is slowly but inevitably becoming available about persons. They already receive cell-site location data from mobile telephones when they order operators to produce traffic data. More importantly, once more applications and services are based on precise network-based localization or on GPS transceivers, agencies may order more data from those who process the location data, or, perhaps, they may even intercept them wirelessly in some ways. Moreover, such data may be combined with other data. For instance, retrieved location data may lead to a CCTV tape that shows an image of the person phoning in the supermarket or at the gas station. Also, it is not inconceivable that obligatory location tracking for national-security purposes will be established as well, just as localization in "Emergency 911" (E911) has been mandated.[177]

Perhaps more immediately relevant will be the active localization that national-security agencies can use. GPS recorders or transceivers can be attached to vehicles and boxes, and as they grow smaller, to suitcases or clothes. Law enforcement already has used a GPS recorder successfully to track a murder suspect's truck movements to the grave where he reburied his victims.[178] This differs from a traditional direction transponder in that there is no need to follow the item itself, which always entails the risk of discovery; one can simply and inconspicuously

175. In the U.S., CALEA, 47 U.S.C. § 1006 (2000), has been interpreted as to cover "the location of a cell site location at the beginning and termination of a call," Communications Assistance for Law Enforcement Act, 64 Fed. Reg. 51,710, 51711 (Sept. 24, 1999). The same holds for the Netherlands, where article 126n of the Code of Criminal Procedure—ordering delivery of traffic data—includes the location of the cells in which someone used a mobile phone. *Wetboek van Strafvordering* [Sv], art. 126n (2006).

176. *See, e.g.*, *Council of the European Union, Draft Framework Decision on the Retention of Data*, at 9, COM (2004) 15098 (Apr. 28, 2004) (requiring location and traffic data), *available at* http://register.consilium.eu.int/pdf/en/04/st08/st08958.en04.pdf.

177. *See* 911 Service, 47 C.F.R. § 20.18 (2005).

178. *See* State v. Jackson, 46 P.3d 257, 261 (Wash. Ct. App. 2002); David A. Schumann, *Tracking Evidence with GPS Technology*, WISC. LAW., May 2004, at 9, 9 (further detailing the *Jackson* circumstances).

check the route followed afterwards by retrieving the device and reading the recorded GPS data.

To sum up, this case shows that technology enables increasing, systematic, and covert localization of individuals. Security agencies join in and profit from the market and E911 developments—just as law-enforcement agencies and businesses will benefit from location technologies. It is not unlikely these government benefits may be reinforced by legal requirements for government-surveillance purposes, demanding storage and production of location data in a variety of cases. The associated privacy shift is significant, since localization is possible on a much wider scale and also can be executed *ipso facto* by retrieving stored location information. This substantially impacts the reasonable expectation of privacy that people have traditionally had in movement: they may have been visible at a certain time at a certain place, but much less traceable for a longer period of time. The continuous localization current and future technologies offer, thus, significantly contributes to the "disappearance of disappearance" that is a defining characteristic of the information age.[179]

2. Case 2: Cryptography revisited

In the case of cryptography discussed in the previous section, we mentioned that cryptography perturbed national security, mainly because if foreigners use it, eavesdropping becomes useless. 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, this was followed up by the Wassenaar Arrangement,[180] 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.[181] The thrust of the arrangement is to allow export of only weak (easily crackable) cryptography and to require licenses for export of strong cryptography. As the 1990s evolved, the controls were increasingly controversial, especially in

179. Levi, *supra* note 164, at 206 (internal quotes omitted) (quoting Kevin D. Haggerty & Richard V. Ericson, *The Surveillant Assemblage*, 51 BRITISH J. SOCIOLOGY 605, 619 (2001)).

180. Wassenaar Arrangement for Export Controls for Conventional Arms and Dual-Use Goods and Technologies (July 12, 1996) *as amended*, *available at* http://www.wassenaar.org/guildines/guidelines.doc; *see generally*, WHITFIELD DIFFIE & SUSAN LANDAU, SUN MICROSYSTEMS LABORATORIES, THE EXPORT OF CRYPTOGRAPHY IN THE 20TH CENTURY AND 21ST 2 (2000), http://research.sun.com/features/tenyears/volcd/papers/22Diffie.pdf.

181. *See* Wassenaar Arrangement, Dual-Use List, Category 5, Part 2, Information Security, *available at* http://www.wassenaar.org/controllists/index.html ("Category 5—Part 2"); Export Admininstration Regulations, 15 C.F.R. § 730.3 (2005).

the U.S. since they hampered electronic commerce, and were practically unenforceable, given that strong cryptography programs could be downloaded from many places on the Internet. After several relaxations in the U.S.[182] 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.

But there is more. In the "law-enforcement" case description,[183] we asserted that cryptography has retained its foothold as a privacy-enhancing technology. But 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 cryptography systems, like the Advanced Encryption Standard,[184] are reliable and do only what they are supposed to do because the protocols have been published and scrutinized extensively.[185] However, for *implementations* and concrete products, this may be different. 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 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

182. *See* 65 Fed. Reg. 2492–2502 (Jan. 14, 2000) (codified in scattered portions of 15 C.F.R. chap. 7).

183. *See supra* Part III.A.

184. *See* NATIONAL INSTITUTE OF SCIENCE AND TECHNOLOGY (NIST), ANNOUNCING AES (2001), *available at* http://csrc.nist.gov/publications/fips/fips197/fips-97.pdf.

185. *See* IAIK Krypto Group, AES Lounge, http://www.iaik.tu-graz.ac.at/research/krypto/AES/ (last visited Nov. 15, 2005) (hosting a plethora of links to papers written concerning the AES standard). The page is a funded through the European Union's Sixth Framework Programme (FP6), the agency responsible for the European Research Area (ERA). *Id.*; *see also* Council Decision 1513/2002/E, 2002 O.J. (L 232) 1, *available at* ftp://ftp.cordis.lu/pub/documents_r5/natdir0000029/s_1831005_20021107_150652_6FPL021654en.pdf; What is FP6, http://www.cordis.lu/fp6/whatisfp6.htm (last visited Nov. 15, 2005).

> with the enciphered message. NSA analysts could read the message traffic as easily as they could the morning newspaper.[186]

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

3. Balance

The cases show that, 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 of 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" favors a significant shift of the balance to the detriment of privacy, a push that only legislatures and courts can check 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.

In these domains, the principal value to be protected clearly seems to be security at the cost of a whole range of other competing values: dignity, self-evaluation, and protected communication being prominent victims. Interestingly, cost, a value that ordinarily favors giving up one's private sphere, is also affected. The measures taken to increase security are costly and are likely only to increase in the future.[187]

C. *E-Government*

We started this Article with a discussion of Bentham's Panopticon, the ultimate way government could spy on and control its 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 its citizens, but instead Soft Sister guards

186. Wayne Madsen, *Crypto AG: The NSA's Trojan Whore?*, 63 COVERT ACTION Q., Winter 1998, at 36, 36 (footnote omitted).

187. The aforementioned EU proposal on data retention, *Draft Framework Decision on the Retention of Data*, *supra* note 176, has been highly criticized, partly on the basis of the burden on citizens and service providers. *See, e.g.*, INVASIVE, ILLUSORY, ILLEGAL, AND ILLEGITIMATE: PRIVACY INTERNATIONAL AND EUROPEAN DIGITAL RIGHTS (EDRI) RESPONSE TO THE CONSULTATION ON A FRAMEWORK DECISION ON DATA RETENTION (Gus Hosein ed., 2004), http://www.privacyinternational.org/issues/terrorism/rpt/responsetoretention.html.

and looks after them,[188] 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 (e-government), following the advances of e-commerce. In the U.S. Vice-President Al Gore's *Reengineering Through Information Technology* program,[189] 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 informational privacy protection.[190]

In the rise of e-government, citizens are more and more seen as customers who deserve levels of service delivery comparable to those in the private sector.[191] Service delivery should be simpler, more efficient, and more customer-friendly. Information technologies, especially the Internet, are 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.

The Internet and closed networks have a huge potential impact on the privacy of citizens in the public sphere because they allow the fiction we call "government" to become reality. Government in most countries is composed of a multitude of agencies of varying size, each of them responsible for a particular set of tasks with corresponding responsibilities. And each keeps their own records to carry out their daily operations.[192] The Social Welfare agency, for instance, has to have re-

188. Paul Frissen, *Public Administration in Cyberspace*, *in* PUBLIC ADMINISTRATION IN AN INFORMATION AGE: A HANDBOOK 33, 35 (I.Th.M. Snellen & W.B.H.J. van der Donk, eds., 1998).

189. AL GORE, OFFICE OF THE VICE-PRESIDENT, REENGINEERING THROUGH INFORMATION TECHNOLOGY: ACCOMPANYING REPORT OF THE NATIONAL PERFORMANCE REVIEW (1993), *available at* http://govinfo.library.unt.edu/npr/library/reports/it.html.

190. *See* Perri 6, Charles Raab & Christine Bellamy, *Joined-Up Government and Privacy in the United Kingdom: Managing Tensions Between Data Protection and Social Policy, Part I*, 83 PUB. ADMIN. 111 (2005).

191. *See* F. LESLIE SEIDLE, RETHINKING THE DELIVERY OF PUBLIC SERVICES TO CITIZENS (1995).

192. A study commissioned by the Ministry of the Interior in the Netherlands showed that there are some 30,000 of these registrations in the Netherlands, a considerable amount, given that it has a population of 16 million people. H. BLEKER, W.J. LAMERIS & D.L.W. ZIELHUIS, ELEKTRONISCHE BESTANDEN VAN HET BESTUUR [ELECTRONIC RECORDS OF THE

cords to provide citizens on welfare their monthly benefit. They have to keep track of who is entitled to what amount of benefit, what is paid and when, and other data. It is safe to say that almost all records in public offices are computer databases nowadays. And, as agencies increasingly are wired-up, their databases can be combined—to offer both online services and the holistic services e-government rhetoric heralded. The wiring-up of previously separated databases also leads to data exchange between agencies and to combining data 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 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 its own data. To illustrate what the combination of personal data in the context of e-government purports, two cases are explored.

1. Case 1: Pro-Active Service Delivery

The benefits for the citizen derive from the fact that once the wired government knows the identity of a citizen, 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 the applicant paid (available to the housing corporation, which in some cases is a public agency). Information from the various government databases can therefore be used to prepopulate (online) forms or even to make decisions on the basis of the data already available, without a need for citizens to apply for these services altogether. This latter type of service delivery is called pro-active service delivery[193] and shows precisely what is meant by the aforementioned Soft-Sister concept: government taking active care of its citizens by combining the available information on citizens, determining their rights (and obligations), and taking action on these without waiting for

---

ADMINISTRATION], BDO CONSULTANTS 70 (1998), http://www.minbzk.nl/contents/pages/5351/onderzoekelektronischebestandenvanhetbestuur.pdf.

193. *See* DUTCH MINISTRY OF THE INTERIOR AND KINGDOM RELATIONS, CONTRACT WITH THE FUTURE: A VISION ON THE ELECTRONIC RELATIONSHIP BETWEEN GOVERNMENT AND CITIZEN 27 (2000), *available at* http://www.minbzk.nl/contents/pages/3925/contract_with_future_5-00.pdf (English version).

the citizens to call for these actions.[194] This paternalistic notion may appeal to some and is part of government policy in some countries, such as the Netherlands. In *Contract with the Future*,[195] a Dutch policy paper in which pro-active service delivery is adopted as Dutch policy, the primary reasons for doing so are mentioned: "Services are improved, there is an increased take-up of previously unused services and legal equality increases, as do effectiveness and efficiency."[196]

The idea of combining databases in the sense described above made national headlines in the Netherlands at the end of 1997, when the city of Groningen announced that it was going to use combined databases to locate citizens entitled to various services for people with insufficient means. Various studies in the early 1990s had shown that considerable numbers of people entitled to these benefits and subsidies failed to apply for them.[197] The initial experiments carried out in Groningen and a number of other cities[198] have shown that combining data from different data sources can indeed help to locate people entitled to certain benefits, although the effectiveness varies. Local services gained more than nationally available ones. This is not unsurprising as national services are better known to the public than local services.[199] The experiences with combining data sources in Groningen and elsewhere in the Netherlands have spurred the uptake of pro-active service delivery in the Netherlands, and it was adopted as one of the pillars of Dutch e-Government in 2000.[200]

E-government has matured since 2000 and more advanced examples of pro-active service delivery can be witnessed at various places. A recent study commissioned by the European Commission discusses a number of them in their report on best practices in back-office integration in Europe.[201] Common themes where we see examples of pro-active

---

194. *See* Frissen, *supra* note 188.

195. CONTRACT WITH THE FUTURE, *supra* note 193.

196. *Id.* at 27.

197. For instance, Van Oorschot concluded that up to 26% of the people in the city of Rotterdam entitled to Housing benefits do not apply for them. *See* WIM J.H. VAN OORSCHOT, TAKE IT OR LEAVE IT: A STUDY OF NON-TAKE-UP OF SOCIAL SECURITY BENEFITS 151 tbl. 5.2 (1994). These numbers are consistent with findings in numerous other studies. *See, e.g.*, SOCIAAL CULTUREEL PLANBUREAU (SCP), ARMOEDEMONITOR 1997 [POVERTY MONITOR] (1997), *available at* http://www.scp.nl/publicaties/boeken/9057491044/Armoedemonitor_1997.pdf.

198. *See* DUTCH MINISTRY OF SOCIAL AFFAIRS AND EMPLOYMENT, TERUGDRINGEN NIET-GEBRUIK VAN INKOMENSAFHANKELIJKE VOORZIENINGEN; PILOTS BESTANDSVERGELIJKING [RETURNING USE OF INCOME-RELATED BENEFITS, PILOT REPORT] (1999).

199. *See id.*

200. *See* CONTRACT WITH THE FUTURE, *supra* note 193.

201. *See* JEREMY MILLARD ET AL., REORGANISATION OF GOVERNMENT BACK OFFICES FOR BETTER ELECTRONIC PUBLIC SERVICES—EUROPEAN GOOD PRACTICES (BACK-OFFICE

service delivery on the basis of data interoperability are child allowances (for instance, in Ireland and Spain) and tax filing (in Finland and Spain). Child allowance is triggered by birth notifications received by the civil registration service. The process is partially automated in the case of a first child. In this case the parents receive a partially filled out form. In the case of subsequent children there is no need for form filing at all, and payments start automatically after the responsible agency receives the birth notification.[202]

The report also noted:

> In each of the countries (Finland, Ireland and Spain) from which the above cases are taken, there have been few, if any, problems with data privacy, either because of legal restrictions or objections by the citizen. Such conditions do not obtain in all European countries, which makes the offer of pro-active services much more problematic there.[203]

However, the examples described so far only concern a very limited number of databases and agencies involved; child allowance is triggered by a birth-notification form the civil registry, for instance. It is not difficult to imagine more and more agencies and registers becoming involved in this type of service delivery, leading to an increasing amount of personal data becoming "connected." This will certainly affect privacy.

The Dutch city of Enschede provides an example of what is to come with respect to linking databases concerning individual citizens in pro-active service delivery in their project "my counter."[204] Once the citizen has identified himself to the city online, the system provides personalized advice and news. The user is, for instance, notified on the progress of his applications, the expiry of passport and driver's license, but also information on roadwork and town planning in the user's immediate neighborhood can be provided. These types of personalized services are customary in the commercial domain, where it is part of customer relationship management (CRM). The Enschede example shows the use of multiple databases, residing at different municipal agencies. The potential privacy impact may surpass that in the private sector because it may impact on rights and obligations of citizens.[205]

REORGANISATION), *available at* http://www.epsigate.org/sample_content/back_office_reorganisation_final_report.pdf (2004).

202. *See id.* at 99–104.

203. *Id.* at 42.

204. *See, e.g.*, *"Digitaal Kluisje" Voor Burgers Enschede* [*"My Digital Counter" for Enschede Residents*], BURGER@OVERHEID, July 14, 2004, http://www.burger.overheid.nl/nieuws/?id=594.

205. *See infra* Part III.C.2.

The effects of data exchange for the benefit of pro-active service delivery arise not only as a result of the actual combination of data previously unassociated but also because it acts as a catalyst for even more exchange. Access to information in databases can be provided on the basis of many attributes associated to a person (such as their 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 or duplicates. Names and addresses can be written in many different ways; this is not only the case with "foreign" names containing diacritics, but also with ordinary names which give rise to different spellings: omission of middle initials, additions to names, maiden names, or other variations. 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 or addresses produces many mismatches and non-matches due to variations.

As a consequence there is a tendency to use a single unique identification number for a large variety of, if not all, government databases. Recent developments illustrated this tendency in the Dutch medical sector. In 2002, the Dutch Data Protection Authority (College Bescherming Persoonsgegevens in Dutch) issued a policy paper arguing for the use of sectoral unique identification numbers instead of a single identification number for all government databases.[206] This scheme allows for inherently better data protection than the use of a single identification number, since it prevents unnecessary merging of databases. The policy has, in principle, been embraced by the Dutch government,[207] 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 now seems to tilt the balance instead towards adoption of the generic Citizen Service Number (BurgerServiceNummer, BSN) that is currently being developed as an overarching government ID number.[208]

206. J.A.G. VERMISSEN & A.C.M. DE HEIJ, COLLEGE BESCHERMING PERSOONSGEGEVENS, ELEKTRONISCHE OVERHEID EN PRIVACY: BESCHERMING VAN PERSOONSGEGEVENS IN DE INFORMATIE-INFRASTRUCTUUR VAN DE OVERHEAD [ELECTRONIC GOVERNMENT AND PRIVACY: PROTECTION OF PERSONAL DATA IN THE INFORMATION STRUCTURE OF GOVERNMENT] 16–17 (2002), *available at* http://www.cbpweb.org/downloads_av/av25.pdf.

207. *See* CONTRACT WITH THE FUTURE, *supra* note 193, at 41.

208. *See* M.A. BRENDA, ZORG INDENTIFICATIE NUMMER: ONDERZOEK CONSEQUENTIES INVOERING ZIN VOOR ZORGVERZEKERAARS EN ZORGAANBIEDERS [Care Identification Number: Researching Consequences of Setting-Up CIN for Care Insurers and Care Providers], *available at* http:www/nictiz.nl/kr_nictiz/default.asp?datoom=1900; *Uniek Zorgnummer op Losse Schroeven* [*Unique Care Number on Loose Propellers*], AUTOMATISERING GIDS [AUTOMATION GUIDE], Mar. 12, 2004, http://www.automatiseringsgids.nl/news/default.asp?nwsId=26437.

Efficiency, therefore, is a primary reason not to diversify identification systems.

2. Case 2: Using Citizen Data for Secondary Purposes

The previous case discussed data interoperability for the benefit of citizens. These same mechanisms can also be used against citizens. Combating fraud is such an example of the use of data interchange that easily springs to mind. In order to combat fraud with General Assistance benefits in the Netherlands, data is exchanged between the local General Assistance Offices (GSD), the Office for Employee Insurances (UWV), the Tax Authorities (Belastingdienst), and the Information Management Group (IB-Groep), by means of a gateway maintained by the Intelligence Agency (Inlichtingenbureau).

But also in the case of legitimate citizen behavior, data exchange can be used against the citizen. The reliance on single cross-sector identification numbers facilitates "cross-fertilization" of services. For example, databases on hospitalization might be merged with other databases in order to make profiles of people that have a high "hospital risk"; insurance companies might subsequently use such profiles to diversify insurance costs. Although we are not aware of serious forms of "cross-fertilizing" of government services at present, software that enables such data merging exists, and thus, at least in theory, allows the creation of new policy instruments. For instance, you only receive a rental allowance if you have paid all your fines. Or, 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); or, your request for a building permit is processed with priority if you have submitted your income tax on time over the past five years. There may be some citizens who appreciate such schemes, but others will feel threatened that government agencies know details of their lives the agencies do not need to know to do their proper job.

Misuse of data sources is facilitated by the developments sketched. Interrelated government databases allow, for instance, social-security permitting 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[209] and social welfare employees are known to have used

209. *See* JAN NAEYÉ ET. AL, INTEGRITEIT IN HET DAGELIJKS POLITIEWERK: MENINGEN EN ERVARINGEN VAN POLITIEMENSEN [INTEGRITY IN DAILY POLICE WORK: OPINIONS AND EXPERIENCE OF POLICEMEN] (2004); *Agenten Misbruiken Massaal Politie-Informatie* [*Agents Massively Abuse Police Force Information*], JUROFOON, Apr. 22, 2004, http://www.jurofoon.nl/nieuws/weblog.asp?id=1141.

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 via cross-linking. On the contrary, the enlargement of both the databases' scope and the number of people who have access to them increase the risk of "interesting excursions" and misuse.

3. Balance

Within the public sector, "code" is affecting the balance between privacy and what "the government" knows of its citizens. In the case of e-government the problem is not so much the government prying deeper into the private sphere by collecting previously unavailable data. Instead, the problem is the combination of data already available to government, albeit to distinct organizations and agencies. Whereas the citizen used to present only a fragment of himself to a particular government agency, the agency in question increasingly is capable of recollecting the citizen's other fragments, as well, by linking–up with other government agencies.

The principal driving forces that lead to increasingly transparent citizens are efficiency gains for both government and citizen, greater convenience for the citizen,[210] but also equality before the law since preventing or fighting fraud can be seen as a way to give everyone his rightful share. In a sense, one can even argue that privacy values such as *individuality* and *integrity*, the desire to be seen as an individual person and not to be flattened out, are served by data interoperability since it allows more aspects of the citizen to be taken into account in delivering services. However, on balance, one must acknowledge that citizens become more transparent as a result of pro-active service delivery and the associated integration and interoperability of data sources. The modernization of government, embodied in the aims to improve efficiency and service delivery, seems to prevail over privacy interests.[211]

It is unclear whether citizens care about their loss of privacy. Regardless, whether it is really necessary to affect the privacy of citizens in the present manner to achieve the goals as set out remains an interesting question. Is it possible to deliver pro-active services, to increase efficiency, and to improve convenience without invading people's private spheres more than before? The answer to this question, according to some, is yes. A balance between privacy-protection interests and effi-

210. The Dutch tax authorities cleverly market this kind of benefits in their slogan: "We can't make it nicer for you, but we can make it more convenient."

211. *See* Perri 6, *supra* note 190, at 111.

ciency and service-delivery improvements can be maintained.[212] What advocates propose is to maintain a balance through implementing "privacy by design"—implementing privacy protection in code by adopting PETs and by maintaining data walls between sectors. Applications can be constructed in such a way that only the necessary minimum of information is revealed. For instance, for 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. This is an application of the PET notion, as introduced by the Dutch and Ontarian Data Protection Authorities: construct technology in a way that the minimum amount of data necessary for the specific goal is used and shield-off all other information.[213]

But why do such alternatives to sacrificing privacy for the improvement of efficiency and service delivery not seem to be used in practice? This may well be unintentional. Maybe it is more a case of unawareness or lack of appreciation of the privacy-enhancing possibilities of technology. Also, the cost of implementing proper privacy-protecting "code" may be deemed too high. Policy makers and systems developers are hardly aware of the alternatives to personalized access to services.

It is too easily assumed that government access to citizen data is essential to improve service delivery. For instance, it is usually taken for granted that the government should know the identity of the citizen to perform any task or service. But this is often not the case. For example, when a neighborhood planning committee collects comments from citizens through a website, it will usually collect names and addresses of the participants to be able to check whether only people with a genuine interest in the neighborhood participate. If there is a requirement of only being permitted to participate in the online hearing when one actually lives in the neighborhood, then one could use other, less privacy-invasive, checks as well. The check on neighborhood residency can be done by another agency than the one running the online hearing. Depending on the desired level of security, technology can facilitate such privacy-friendly verification in numerous ways, from anonymous or

212. *See* VERMISSEN, *supra* note 206; George Radwansky, Privacy Commissioner of Canada, The Privacy Challenge: Connecting Citizens with All Levels of Government (May 9, 2002), *available at* http://www.privcom.gc.ca/speech/02_05_a_020509_e.asp; *cf.* C. Bellamy, Perri 6 & C. Raab, *Joined-Up Government and Privacy in the United Kingdom: Managing Tensions between Data Protection and Social Policy, Part II*, 83 PUB. ADMIN. 393, 412–13 ("Certainly, there is no *general* balance between privacy and data sharing. Rather, settlements are worked out in particular vertically-defined policy fields, and vary in relation to different privacy risks and data protection principles. Nor is there any single agency responsible for striking a 'balance.'").

213. REGISTRATIEKAMER, 2 PRIVACY-ENHANCING TECHNOLOGIES: THE PATH TO ANONYMITY 22 (1995), *available at* http://www.ipc.on.ca/docs/anoni-v2.pdf.

pseudonymous smart cards with biometrics a municipality provides 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, 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.

D. *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 in order to target current or potential customers in a more effective, personalized way. Moreover, e-mail 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 out 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, showing higher prices on a website based on a "high-risk" profile, or allowing only customers with a "right" profile to pay afterwards; this happens regardless of whether the individual in the zip-code area indeed has a low income. Moreover, personalized 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 prompts: "persons who bought this book also enjoy reading *Erotic Japanese Woodcuts*," showing an image of the eroticizing 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 distinct, 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, the government adopts commercial uses of data.

1. Case 1: Transaction Monitoring in Mobile Telephony and Banking[214]

Carrying out transactions, 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 the phone numbers of both the caller and the recipient to establish a connection. They also need to keep track of the call's duration for billing purposes as most phone operators use time base billing. Similarly, banks need to know the account numbers of payors 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 secondary purposes. Suspects in a Dutch high-profile child murder case, for instance, were located in Spain following a cash withdrawal from a cash dispenser.[215] Transaction data generated during mobile phone calls or financial transactions may also be used to build profiles of the behavior 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 maintains individual customer profiles and notices radical changes in customer's behavioral pattern. When a mobile phone is stolen or lost and later used by someone other than the owner, this will be noted by the monitoring system. The new user is likely to produce a calling pattern that is completely different from the owner's pattern. The profiles can also be used to notice defaulters. When a customer fails to pay his bills (defaults), he will ultimately be disconnected from the service. If the defaulter were to reapply for the service and be accepted, for instance, because of the use of a false name, the

214. This section is based on ANTONIUS ADRIANUS PETRUS SCHUDELARO, ELECTRONIC PAYMENT SYSTEMS AND MONEY LAUNDERING: RISKS AND COUNTERMEASURES IN THE POST-INTERNET HYPE ERA (2003).

215. *See Moeder Rowena Aangehouden in Spanje* [*Rowena's Mother Apprehended in Spain*], RTLNIEUWS.NL, Dec. 20, 2001, http://rtl.nl/(/actueel/rtlnieuws/)/components/actueel/rtlnieuws/12_december/19/buitenland/rowena.xml.

monitoring system would recognize this customer's behavioral patterns as one of a known defaulter. The phone numbers used and also the general calling behavior will match. Consequently, the service could be discontinued again.

Applications of behavioral monitoring, such as fraud detection and the detection of commercial opportunities, are important in the financial world, too. Electronic monitoring is used, for instance, during customer acceptance and credit-scoring procedures. By analyzing various types of data, providers of financial services can, on one hand, assess the commercial potential of a future customer. On the other hand, data analysis can also be used to assess whether acceptance of a potential customer is likely to result in a bad debt or whether other grounds exist to reject an applicant. Additionally, behavioral monitoring also can be used after applicants have been accepted. Once transactions have begun, behavioral monitoring can detect behavior that exceeds certain predefined limits or to make profiles of the behavior 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 amount of money involved, or other criteria. All of the 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 be valuable for law-enforcement purposes. For instance, behavioral monitoring may be used to detect and investigate money laundering.[216]

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 analyzed. This enables close scrutiny of communication patterns and transaction behavior, 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 capabilities that have emerged in the private sector; they may even make data collection and monitoring mandatory for law-enforcement purposes to combat telecommunications fraud and money laundering.

2. Case 2: Tag, You're It: RFID Will Get You[217]

There has always been a need to identify and trace products. For this reason, products carry manufacturer and product codes, and since the

---

216. In many countries, the banks are required to report remarkable transactions to the tax authorities. *See* Bank Secrecy Act, Pub. L. No. 91-508, 84 Stat. 1118 (1970) (codified at 31 U.S.C. §§ 321, 5311–5314, 5316–5322).

217. The Ontario Privacy Commissioner's report title inspires this subtitle. CAVOUKIAN, *supra*, note 124.

1970s, many products also carry a UPC (universal product code) or barcode 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 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.

An RFID system consists of a tag capable of transmitting, and sometimes receiving, information by means of radio signals. A radio receiver can pick up these radio signals for further processing. In comparison to optical scanning, reading RFID tags is quick: they can be read at seven items a second. Another clear advantage over optical tags is the fact they can be read even if they are covered by fog, snow, paint, or cardboard.

RFID tags come in various flavors.[218] Some tags carry chips that can hold a larger amount of data and can process data (for encryption or verification); they may even contain sensors (to measure temperature, for instance). Chipless tags offer fewer capabilities as they lack a microcprocessor (the chip) capable of processing and storing data. These chipless tags can store a more limited amount of data (typically 24 bits) and are cheaper to produce than chip-carrying tags. Another distinction relates to the power source driving the tag. A reader, with a limited range stretching about 10 meters, activates and powers passive tags. The advantage of these tags is that they do not need their own power source that can run out of power, and, hence, they can operate indefinitely, at least in theory. Active tags contain a power source and an active transmitter capable of sending the signal over a larger distance (up to several kilometers). Passive tags are smaller and cheaper to produce than active tags. They are usually read-only tags that cannot 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. This means that at present, they are not suitable for cheap mass consumer products. Prices are expected to drop to less than $0.05 a piece.[219] This would make them suitable to replace barcodes on most products and enter the supermarkets with possibly far reaching consequences for both suppliers and consumers.

---

218. *See id.* at 5–6.

219. *See* AUTO-ID CENTER, THE NEW NETWORK: IDENTIFY ANY OBJECT ANYWHERE AUTOMATICALLY 3 (2002), *available at* http://www.ifm.eng.cam.ac.uk/automation/documents/centerguide.pdf.

RFID tags carry a number and, as such, create opportunities to associate meaningful data to the item carrying the tag. The tag's identification signal itself may contain information, such as the producer, product type, size, color, production date, and toxicity. But it can also contain a unique identification code. Together these types of data in the tags open up vast possibilities to relate information to the tag. In its simple form only the meaningful data on the tag is used. The information can be used to provide location information, for instance, in supply chains or buildings, or for billing purposes at the counter. The specific data about the tagged item, such as color, size, and production date, may be used by, for instance, 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.").

When the data in the tags are associated with external data (stored in databases), the possibilities to track and trace items increases even more. The history of individual items can easily be stored and maintained throughout a tag's life-cycle. This also, of course, could be done with other types of tags, such as barcodes, but RFID data is easier to read, both in amount, as well as in effort; reading a bar code with 256 characters takes more effort than reading these from an RFID tag.

Current applications are relatively limited in scale due to the cost of present tags. But there are many plans to implement tags in large numbers. Esso (SpeedPass) and Shell (EasyPay) 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.[220] Many organizations, such as Tilburg University, have personal RFID cards to access office buildings. More practical for forgetful workers is the "chipping" of Mexican Ministry of Justice employees to access secure rooms in the Ministry.[221] 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. Employees in the harbors are also equipped with tags, allowing a detailed log of who has been involved with particular containers.[222] In Alexandria Hospital in Singapore, every patient,

220. JOHN A. WOLFF, IBM GLOBAL SERVICES, RFID TAGS: AN INTELLIGENT BAR CODE REPLACEMENT 7 (2001), *available at* http://www.qinetiq.com/home_ep/insight/insight_archive_may_2004/electronic_tagging.SupportingPar.0001.File.pdf.

221. Associated Press, *Update 7: Chip Implanted in Mexico Judicial Workers*, FORBES.COM, 15 July 2004, http://www.forbes.com/associatedpress/feeds/ap/2004/07/15/ap1457329.html.

222. *See Ports to Adopt RFID Security System*, RFIDJOURNAL.COM, July 17, 2002, http://www.rfidjournal.com/article/articleview/26/1/1/.

visitor, and staff member was issued an RFID card after the SARS outbreak in the spring of 2003.[223] 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.[224] Delta Air Lines is testing RFID tags attached to baggage to make tracking and tracing of luggage easier.[225] In the U.K., car license plates may be equipped with RFID to automatically identify cars traveling with speeds up to 320 km/h from up to 100 meters away.[226]

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 when they need replenishing. The American Wal-Mart chain, which 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 the U.K., the Tesco chain started a pilot project in a store in Cambridge. Gillette, Wal-Mart and Tesco co-operate in the RFID experiments.[227] Prada shoes has plans to implement RFID tags. They have also piloted RFID closets in some of their New York stores that respond to the garment taken into the dressing room. An interactive touch screen "enables the customer to select alternative sizes, colors, fabrics, and styles, or see the garment worn on the PRADA catwalk as slow-motion video clips."[228] Benetton and Marks and Spencer in the U.K. have announced plans to incorporate tags in clothing.[229] At the Tokyo International Bookfair 2003, a system was demonstrated that allows detailed in-store observation of people browsing books and magazines. "By placing tag readers on the shelves of bookstores, the new system allows booksellers to gain information such as the range of books a shopper has browsed, how many times a particular title was picked up and even the length of time spent flipping through

223. *See Singapore Fights SARS with RFID*, RFIDJOURNAL.COM, June 4, 2003, http://www.rfidjournal.com/article/articleview/446/1/1/.

224. In theory, this kind of tagging could also enable finding patient "zero," the patient who first shows the symptoms of a disease.

225. *See* Jason Collins, *Delta Plans U.S.-Wide System*, RFIDJOURNAL.COM, July 2, 2004, http://www.rfidjournal.com/article/view/1013.

226. *RFID-enabled License Plates to Identify UK Vehicles*, RFIDNEWS, June 10, 2004, http://www.rfidnews.org/news/2004/06/10/rfidenabled-license-plates-to-identify-uk-vehicles/.

227. *See* Aloire Gilbert, *Wal-Mart Tagging Fuels RFID Market*, ZDNEWS.COM, Dec. 22, 2004, http://news.zdnet.com/2100-9584_22-5501432.html.

228. Case Studies, Prada RFID Closet, http://www.ideo.com/case_studies/prada.asp?x=5 (last visited Nov. 15, 2005).

229. *See Benetton to Tag 15 Million Items*, RFIDJOURNAL.COM, Mar. 12, 2003, http://www.rfidjournal.com/article/articleview/344/1/1/.

each book."[230] 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.[231]

A final application of radiofrequency identification chips is to label people. The American company Applied Digital Solutions is marketing chips (VeriChip) which can be implanted into humans.[232] 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 down the missing person.[233] But other uses were soon found. The Baja Beach Club (with venues in Rotterdam and Barcelona) offers their members the option to have a VeriChip implanted for €25 to replace the traditional membership card.[234] The embedded chip offers their carrier the guarantee that he does not have to queue or reserve tables, and, perhaps most importantly, it allows him to order drinks to be put on his tab. "The bartender simply pings you with a handheld scanner."[235] 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 braggers and refuses them entry or by the local police officer interested in how much the Club member had to drink.

The current applications are fairly straightforward and do not tilt the privacy balance too much. Objects can be identified by reading their tag: 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 cross the border of proportional use.

An obvious use of RFID tags is personalization of services. Objects and information displays may offer personalized 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 personalized information and discounts on the basis of tags worn by a passer-by.[236] In museums, the

230. RFID POSITION STATEMENT OF CONSUMER PRIVACY AND CIVIL LIBERTIES ORGANIZATIONS (2003), http://www.privacyrights.org/ar/RFIDposition.htm (internal quotations omitted) (quoting NIKKEI ELECTRONIC NEWS).

231. *See* Junko Yoshida, *Euro Bank Notes to Embed RFID Chips by 2005*, EETIMES ONLINE, Dec. 19, 2001, http://www.eetimes.com/story/OEG20011219S0016.

232. *See* VeriChip Corp., http://www.verichipcorp.com (last visited Nov. 15, 2005).

233. *See* VeriChip Corp., Infant Protection, http://www.verichipcorp.com/content/solutions/infant_protection.

234. *See* David Pescovitz, *RFID Chips for VIPs*, THEFEATURE.COM, May 22, 2004, http://www.thefeaturearchives.com/100662.html.

235. *Id.*

236. An already famous example is the scene in the movie *Minority Report* (Cruise/Wagner Productions 2002), where John Anderton (Tom Cruise) passes shop windows

various exhibits could provide tailored audio and visual information to the person viewing the object. The RFID tags in Euro notes to counter forgery, black-market transactions, and blackmailing, may 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, thus, can lead easily to profiling and monitoring. Corporations, but also governments, can track people by following the tags they wear or carry. Since tags can have an individual identification code, tracing individuals is possible. Moreover, combining data on the various tags a person carries allows for sophisticated monitoring of lifestyles and habits. For instance, someone entering a Shell station with a car equipped with Michelin tires, wearing Prada shoes and clothing, and paying with her EasyPay card, leaves a trace from both her shoes and her car tires. If this information is combined with purchases in shops, she runs the risk of becoming completely transparent. The purchases at Prada that could have been anonymous with cash, end up not to be anonymous; the EasyPay card gives away the customer's identity, if linked by willing retailers. This may all occur without her being aware of it: for one thing, people will rarely notice the tags, and if they do, they will tend to regard them as just another barcode, not realizing the RFID tags' tracking potential.

Thus, the use of RFID tags may seriously impact informational privacy.[237] Data from the tags can be collected without the carriers' explicit consent, even possibly without them 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 at CNet gave a preview of people tracking: "Delegates to the recent Communist Party Congress were required to wear an RFID badge

---

that not only show commercials, but also personally address passersby to draw their attention: "John Anderton, you look like you could use a Guiness." Recognition in the movie is done by a retinal scan, but RFID could be used just as well.

237. *See* Nissenbaum, *supra* note 99, at 135 ("RFID tags . . . significantly alter the nature and distribution patterns of information."); RFID POSITION STATEMENT, *supra* note 230; GAL ESCHET, A NEW CHALLENGE TO PRIVACY MANAGEMENT: ADAPTING FAIR INFORMATION PRACTICES TO RADIO FREQUENCY IDENTIFICATION TECHNOLOGY, MORRISON & FOERSTER LLP (2004), http://papers.ssrn.com/paper.taf?abstract_id=557441.

equipped with the tiny tag, which permitted their movements around the conference to be constantly tracked and recorded."[238]

Opposition to the use of radio tags is rising from privacy watchdogs, such as the American Civil Liberties Union (ACLU), the Electronic Privacy Information Centre (EPIC), the Electronic Frontier Foundation, and European Digital Rights (EDRi),[239] and from consumer organizations, individual consumers, and recently also politicians. 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.[240] Nevertheless, we think it is inescapable that tags will be increasingly used in products, because the benefits for commerce are simply too great. The real issue is *how* they will be used, for how long they will be used, and who will be able to read them under what conditions.

3. Blocking RFID

RFID tags can, as we have seen, pose serious threats to a person's informational privacy and 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, 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. Second, 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. Therefore, the tags can be shielded by metal foil to prevent radio waves from entering or leaving the tag.

Intelligent forms of misleading the readers are also under development. RSA Security is experimenting with "Blocker Tags." These tags can block RFID tags from being read by sending out fabricated data selectively (for example, only the range of tag id's assigned to Prada shoes) or universally. If embedded in a shopping bag, for instance, the

---

238. *China Raises the Red Tag*, *in Random Access*, CNET.COM, May 2003, *available at* http://www.rflink.co.kr/board/content.asp?idx=59&page=3&cate=e_rflink&search=&searchstring=.

239. *See, e.g.*, RFID POSITION STATEMENT, *supra*, note 230. Californian State Senator Debra Bowen 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. *See* SB 1834, 2004, 2003–2004 Legislature (Cal. 2004). The bill failed. *See* Claire Swedberg, *California RFID Legislation Rejected*, RFIDJOURNAL.COM, July 5, 2004, http://www.rfidjournal.com/article/articleview/1015/1/1/.

240. *See* Elisa Batista, *"Step Back" for Wireless ID Tech?*, WIRED.COM, Apr. 8, 2003, http://www.wired.com/news/wireless/1,58385-0.html.

blocker tags 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.[241]

Another way to disable RFID tags is by deactivating the tags once they have served their purpose. The MIT Auto-ID Center has proposed including a "kill switch" into the RFID specifications.[242] A number of RFID manufacturers, such as Philips Semiconductors have announced they will do so.[243] 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; even then, he may not be fully assured that the tag is actually disabled or that it will not be switched on again.

4. Balance

As in the case of e-government, technology facilitates large-scale information collection as well as information shielding, but it tends to favor only the former. The case of transaction monitoring eminently illustrates the power of IT to combine data. Through its use for fraud-detection, it is being widely employed, and, as a side-effect, may also serve other purposes, such as marketing or law enforcement. In fact, RFID, even though it is not yet as widely developed as transaction monitoring, shows similar aspects: it offers a host of information and data trails, which can be primarily created for specific purposes—for instance, streamlining supply chains, controlling access, or personalizing services—but which may subsequently be put to various other uses. RFID also illustrates the natural tendency of technology to create and spread data rather than contain it:[244] only after substantial protests from civil society has industry become aware of potential privacy threats and looked for ways to contain these.

Privacy-enhancing technologies, such as anonymizers, cookie crunchers, RFID blockers, and anti-spyware tools, can be used to curb data collection, but consumers have to make an effort (and bear certain costs) to protect their privacy with these tools and techniques. Moreover, often consumers are not aware of the covert data collection that is taking

---

241. *See* Ari Juels, Ronald L. Rivest & Michael Szydlo, *The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy*, *in* 10TH ACM CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY 103 (Vijay Atluri ed., 2003), *available at* http://www.rsasecurity.com/rsalabs/node.asp?id=2060.

242. *See* CAVOUKIAN, *supra* note 124, at 19.

243. *See* Posting of Pbecker to Digital ID World Editor's Corner, http://blog.digitalidworld.com/archives/000433.html (June 12, 2003, 10:15 MDT).

244. Or, to (mis)use part of the slogan attributed to Steward Brand: "Information wants to be free." *Keep Designing: How the Information Economy is Being Created and Shaped by the Hacker Ethic*, WHOLE EARTH REV., May 1985, at 44, 49 (transcript of program at Hackers Conference, Nov. 9–11, 1984).

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, cost, convenience, and preventing and monitoring fraud, simply seem to favor privacy-threatening technology much more than privacy-friendly "code."

IV. 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 analyzed. Privacy-related norms are rarely explicitly built into technology. As such, a Lessigish privacy "code" or a Reidenbergian *lex informatica vitae privatae* does not exist. Technology, in particular software and 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.[245]

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 developed and used in real life, its 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 is a technology of freedom, in practice, it rarely functions as such. Privacy-enhancing technologies (PETs) have been devised and propagated, but they have yet to be implemented on any serious scale.

This conclusion holds for both the public and private domain. 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. In the private sector, technology enables more control of people, from workplace and transaction monitoring to personalization of consumer relationships, with new applications like 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 compartmentalizing information. And the people

245. *See supra* Part III.A.1.

who usually decide on how technology is applied are precisely the people on the strong side of power relations—governments, businesses, and employers—who have an interest in gathering information about the people on the other side so 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 more control is possible via a new application, though that is not what the application was made for, it is fine nonetheless. People gladly adopt the new possibilities. In fact, after a lapse of time, one gets so used to this new control mechanism that one may no longer perceive it as a side-effect but as an intrinsic—and perhaps intended—characteristic of the technology. This is when the "reasonableness" of a privacy expectation shifts: 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 become so accustomed 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 jobs.

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 privacy, society gradually adapts to new technologies and the privacy expectations that go with them. If one is to stop this almost natural process, a conscious effort and considerable resources are required.

V. 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 several questions that relate to the legitimacy of "code" as law.[246]

246. For an elaboration of these questions, see Lodewijk Asscher's chapter in CODING REGULATION, *supra* note †.

A. *Can Rules Be Distinguished in the Code?*

Only rarely does code include specific privacy-related rules. One example is interceptability of telecommunications, where the built-in "rule" is that the government must have an option to intercept telecommunications if it so wants. Other examples are PETs, such as anonymizers 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.

Nevertheless, one might want to qualify this conclusion. It is true that rules are not consciously embedded, but given the scale and seriousness of the privacy-threatening side-effects, one could view privacy-curbing "rules" as being negligently built-in in technology. Code developers, marketeers, and policy-makers, through what Froomkin terms "privacy myopia,"[247] usually seem to disregard the negative privacy side-effects of technology, resulting in a substantial erosion of privacy. Hence, they may be thought to fail to "exercise the standard of care that a reasonably prudent person would have exercised in a similar situation" and, thus, perhaps commit "any conduct that falls below the legal standard established to protect others against unreasonable risk of harm," as a definition of negligence terms it.[248] In other words, they are responsible, nonetheless, for building in privacy erosion in technology.

Although this is perhaps stretching the term "rule" rather far, we are inclined to think that the development and application of code that negligently fails to take privacy effects into account can indeed be seen as embedding a "rule" in the technology, namely that privacy is unimportant and secondary to other values that the code primarily serves. Such technology indeed does serve to guide or control (what is perceived as) proper and acceptable behavior, since it considers privacy-infringement an acceptable outcome of its use.

---

247. Froomkin, *supra* note 8, at 1501.

248. BLACK'S LAW DICTIONARY 1061 (8th ed. 2000).

B. *Can the Rules Be Understood?*

Is how code works and what it does understandable? If so, are those rules transparent; are they accessible to the general public? Can the rules be *trusted*; is there any guarantee that rules are not changed during the game? Are code rules *reliable* in the sense that they are predictable?

These questions about the transparency and reliability of "code" can be answered straightforwardly with respect to the "negligently" built-in value of privacy erosion: this is not transparent, trustworthy, or reliable in the sense that people know the "rule" and trust it to "work properly." After all, it is a negative rule, a lack of privacy-awareness, and this void is not transparent.

With "intentional" code, the answer may be more subtle. 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 when "updating" technology. The debates in the U.S. over CALEA[249] and the wide interpretation the government gave to the interceptability requirement,[250] 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, 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. But on issues less dramatic than national security, electronic voting for instance, we cannot be sure at all that government does not monitor the individual voter's preferences,[251] unless open source software is used.[252]

With PETs, this is not the case. Precisely because people who are usually ardent defenders of privacy developed them to protect 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

249. Pub. L. No. 103-414, 108 Stat. 4279 (1994) (codified in scattered sections of 18 U.S.C. and 47 U.S.C.), *available at* http://www.askcalea.net/calea.html.

250. *See* U.S. Telecom. Ass'n v. FCC, 227 F.3d 450 (D.C. Cir. 2000); Communications Assistance for Law Enforcement Act, *supra* note 175, at 51711, and accompanying text.

251. Nor can we be sure that our actual vote is what the voting machines counted.

252. For a list of issues in the 2004 U.S. presidential elections, see Voting Privacy, Election Privacy Information Center, http://www.epic.org/privacy/voting/ (last visited Nov. 15, 2005).

cryptography products suggests.[253] 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 the fear that even PET products produced by privacy-minded people, particularly robust ones that thwart any kind of control, are being covertly altered.

C. *Are "Code" Rules Contradictory?*

Do rules 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 built-in privacy protection. 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 of uncrackable PETs to governments. 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, usually in such a way that it does not unreasonably restrict other interests at stake. Often, one can develop technology to threaten privacy not unnecessarily, while the technology still achieves 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 enterprises without offering the most intimate details of one's private life.[254] Such PETs can considerably curb the privacy-threatening side-effect of technology and "negligent code". And so, "code" can offer—in theory, at least—a consistent system of regulation allowing for degrees of privacy protection: privacy when possible, infringement when necessary.

253. *See* Madsen, *supra* note 186 and accompanying text.

254. Developing these notions is one of the aims of the European Union 6th Framework Programme and Information Society Technologies projects: "developing solutions to empower individuals to control their private sphere and manage their abilities." PRIME (Privacy and Identity Management for Europe), http://www.prime-project.eu.org/ (last visited Nov. 15, 2005).

D. *Is There a Sovereign?*

Does authority make the "code" rules? The main authority that makes "code" rules are code developers, who, through negligence, build in a slow erosion of privacy.[255] However, since this is a process of which the developers are largely unaware, one cannot really see them as an "authority" similar to a rule-making body. Nevertheless, the minions may still address them about the rules they unwittingly or carelessly create with respect to privacy infringement.

With government-mandated enforcement "code," on the other hand, there is a clear sovereign: the government. If a legitimate legislator—parliaments and the like—mandates built-in privacy infringeability, there is no specific problem of "code" legitimacy. If parliament decides that all telecommunications 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, perhaps operating sometimes 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).

E. *Is There a Choice?*

Can consumers and citizens choose not to obey the rules? Can citizens and consumers freely choose another system of law or 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. (Or, unpragmatically, they could also choose to use no telecommunications at all.) In principle, they can choose any array of technologies that fits 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 (mis)uses of technologies; they can and will be used against you. Choice also implies affordability, and although anonymizers or RFID blockers do not cost

255. *Cf.* Jay P. Kesan & Rajiv Shah, *Deconstructing Code*, 2004 YALE J.L. & TECH. 277, 277 *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=597543 (distinguishing between various kinds of code developers and arguing that "code developed by a university is likely to contain different values and biases, regarding societal concerns such as privacy, than code developed by a firm").

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 to which people have become accustomed.

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. Rarely can one choose to use a PET in such situations. It is the provider of goods and service, business or government, who should implement a PET; if they do not, the citizen or consumer cannot herself decide to use a PET: the system simply refuses anonymous communications, or it requires one to fill in fields with personal data that, in principle, has 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 commercial domain, one might look at the market to ensure choice, nevertheless, through use of companies offering consumers privacy-friendly services. In the public domain, one—so far—cannot choose between governments to conduct business with.

F. *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 both are 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 society continually gets used to new technology, the step of mandating the technology's control element may appear as a mere application of 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 circumvent control if they wanted to, even if the control was consistent with the law, there is no escaping control with built-in enforcement. In this way, "code" that applies existing legal norms concurrently makes the legal norm itself absolute.

Now, how does the notion of "code as law" work overall when it comes to privacy regulation? First, with "code" that negligently incorporates privacy erosion, there are serious problems. The incorporated "rule" is intransparent. There is no clear mechanism for addressing the authors of such "rules," since they are themselves hardly aware of them and neither are the policy-makers who could or should address them, and citizens and consumers hardly have a choice since there is insufficient supply of privacy-enhanced technologies.

Second, where technology explicitly functions as "code," in a handful of enforcement-enhancing technologies, such as tools of interceptable telecommunications and PETs, one can also voice concern over some elements. Notably, the intransparency of the "code" and the non-circumventability can be perceived as problematic.

VI. What is the Problem, Exactly?

Having surveyed and analyzed the relationship between "code" and privacy, we have noted several problems associated with embedding privacy-related rules in technology—notably intransparency, the lack of mechanisms to address the "rule-makers," and the lack of choice. Thus, we turn to the third part of our research question: does "code" cause shifts in privacy balances?

It is useful to distinguish two issues at stake, which may require separate treatment. The first—and minor—issue is intentionally privacy-related "code." Since only a minority of technologies consciously embeds privacy enhancement or privacy infringement, this issue affects privacy regulation to a minor extent only. Some things can be done to address flaws in the functioning of this "code" as privacy law, notably to enhance transparency and to deal with the uncircumventability that might too radically limit choice.

But perhaps these problems should not be exaggerated. We are talking about a minor part of the gamut of technology as we use it today, making the fact that one has no choice but to use this specific privacy-related technology less consequential. And the "codes" mentioned may be intransparent because we cannot exclude national-security-urged backdoors from being built-in; then again, we also cannot exclude the possibility that the world is teeming with Martians we just happen never to see because they are smart enough to stay invisible. Moreover, many traditional legal norms are not particularly transparent either. In short, in the relatively few cases in which privacy-related norms are built-in explicitly into technology, there are concerns of transparency and mandatory compliance, but these concerns may not differ radically from non-"code" forms of regulation, and perhaps we need not be gravely concerned that "code" seriously alters existing privacy balances.

This is different in the second, and larger, issue emerging from our analysis: the slow but gradual erosion of privacy that is a side-effect of much technological development and that can be seen as the negligent embedding of privacy infringement in code. The privacy balance clearly seems at stake. Despite the fact that some scholars have pointed out this development as a potential "death of privacy,"[256] the technological privacy erosion as such does not currently seem to be a serious academic and societal debate.[257]

One explanation for this could be that the gradual erosion of privacy is a natural process: as technology evolves, we gradually adapt ourselves to its possibilities, and while these possibilities stress information sharing and monitoring more than information shielding, the reasonable expectation of privacy is slowly being transformed as well.

Perhaps we should not ask ourselves what are the main problems with "code" and privacy, but rather, what is the problem anyway? Michael Froomkin, acting as the devil's advocate, has considered the possibility that we are dinosaurs, hopping around in a changing world where we do not see that other species with quite other world views will soon take over.[258] Looking back and clinging to privacy protection may be old-fashioned when we observe youngsters leaving massive data trails on the Internet and chatting intimate details into mobile phones in public, without regard for potential privacy effects. Likewise, consumers seem almost too willing to sell personal data for small discounts, not bothering to ask to what uses the data are subsequently put. Although this argument can be countered with the observation that a large part of this development is fed through ignorance—most people simply do not know what is being recorded and what can be and is done to their data—this still begs the question of how bad the seeming loss of privacy really is.

In other words, are there real—or realistic—horror stories to show that things go terribly wrong if "negligently privacy-threatening" technology develops unheeded? It may be difficult, actually, to pinpoint concrete examples of "privacy horror." Since privacy is a servant to many masters,[259] it is, in fact, other values that seem at stake. For in-

256. Froomkin, *supra*, note 8 (note the question mark in the title).

257. "Erosion of privacy" has been debated in the 9/11 context and before, centering on the United States' Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act, Pub. Law 107-56, 115 Stat. 272 (2001), the United Kingdom's Regulation of Investigatory Powers Act, 2000, 23, §§ 49–55, 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.

258. Michael Froomkin, Comments to Roundtable on Code and the Public Domain at University of Amsterdam Institute for Information Law (July 1–2, 2004).

259. *See supra* Part II.E.

stance, loss of privacy may lead to discrimination in quite a few cases, since individuals will be judged more on the sum of knowledge that people have about them and also on group profiles with which they share characteristics—thus, individuals will also be increasingly judged on the basis of non-relevant bits of knowledge or presumed information.[260] It also threatens values such as solidarity as enshrined in, among others, European societies, for example, when patients are judged by the knowledge of all their habits and predispositions, possibly leading to enormous insurance costs for people with "bad" lifestyles or "bad" genes. Privacy loss in situations like electronic voting may be detrimental to the democratic value of elections.

As these examples show, it is perhaps not specific individuals' horror stories that underpin concern over privacy-eroding "code," but rather the sum of situations in which individuals would experience loss of privacy. Central privacy-related values are at stake if, slowly but surely, multiple parts of daily life are becoming more transparent. An individual will feel harmed in her integrity because she feels less an individual, less autonomous, and less dignified when society treats her as a collection of information fragments rather than as an integral human being. Also, there is less scope for self-realization when there are ever fewer spheres and situations in which one can feel unobserved (or have such a reasonable expectation).

Moreover, one must also take into account the effects of such "code" for society as a whole. A transparent society where everybody may know everything about everybody else, or in which certain groups know everything about other groups, is quite a different kind of society than the essentially pluralistic and individualistic (Western) society of the early 21st century. Since society is continuously changing, this need not be a doom scenario—we simply do not know what such a society exactly is like—but we should be careful in embracing the prospect of such a world with the argument that it is the natural evolution of a technology-driven society.

In this respect, it is useful to review the precautionary principle that is a fundamental part of environmental law. The principle says that if full scientific certainty about the consequences of a particular activity on the environment is lacking, while all other conditions for taking measures are fulfilled, the (environment-protecting) measures should be taken. A more progressive formulation of the principle determines that precautionary measures should be taken when there are reasonable grounds for suspecting that a particular activity has a detrimental effect

260. *See* BART H.M. CUSTERS, THE POWER OF KNOWLEDGE: ETHICAL, LEGAL, AND TECHNOLOGICAL ASPECTS OF DATA MINING AND GROUP PROFILING IN EPIDEMIOLOGY (2004).

on the environment.[261] The comparison of privacy with the environment may be more apt than one might initially think, as Charles Sykes observed: "Privacy is like oxygen. We really appreciate it only when it is gone."[262] Privacy, like the environment, is invisible but very much a constitutive factor of the world in which we live, and again, as is the case with the environment, erosion of privacy is usually irreversible. This means that individuals should not give up privacy and that precautionary measures are called for until society knows more about the consequences of irreversibly giving up privacy.

VII. COUNTERING THE EROSION OF PRIVACY

What precautionary measures could address the gradual erosion of privacy through technology? Lessig suggests two pillars of tilting the balance of privacy back again. One is commodification of personal data, which is treating personal data as a commodity that the data subject owns, comparable to, for example, portrait rights marketed by celebrities.[263] 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 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.[264]

Moreover, there are various other arguments to judge this approach ineffective. How can someone control a piece of personal data, once it is sold and part of the opaque data-merging market? How could data sub-

261. *See* JONATHAN VERSCHUUREN, PRINCIPLES OF ENVIRONMENTAL LAW 56 (2003); Timothy O'Riordan et al., *The Evolution of the Precautionary Principle*, *in* REINTERPRETING THE PRECAUTIONARY PRINCIPLE 9 (O'Riordan et al. eds., 2001); Andy Stirling, *The Precautionary Principle in Science and Technology*, *in* REINTERPRETING THE PRECAUTIONARY PRINCIPLE 61; *cf.* United Nations Conference on Environment and Development, June 3–14, 2003, *Rio Declaration on Environment and Development*, princ. 15, U.N. Doc. A/Conf.151/26/Rev. 1 (Vol. 1) (Aug. 12, 1992) ("In order to protect the environment, the precautionary approach shall be widely applied by States according to their capabilities. Where there are threats of serious or irreversible damage, lack of full scientific certainty shall not be used as a reason for postponing cost-effective measures to prevent environmental degradation"), *available at* http://www.un.org/documents/ga/conf151/aconf15126-1annex1.htm.

262. SYKES, *supra* note 9, at 2.

263. *See* LESSIG, *supra* note 11, at 159–62.

264. J.E.J. Prins, *Property and Privacy: European Perspectives and the Commodification of our Identity*, *in* THE FUTURE OF THE PUBLIC DOMAIN (Lucie Guibault & P.B. Hugenholtz eds., forthcoming 2006).

jects control their data when confronted with "take it or leave it" contracts of powerful market parties? What will the administrative costs be of paying for use of personal data, perhaps on a royalty basis? And would such a system not require more processing of personal data in order to pay the data royalties? In short, this approach ultimately fails.[265]

Could Lessig's second pillar, Privacy-Enhancing Technologies (PETs), 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 others. They remain a mainly theoretical solution that has yet to prove its effect in practice. We discern several reasons for this: technology itself tends to combine and connect rather than to compartmentalize; information wants to be free rather than 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 online (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 keep privacy alive, a conscious and concerted effort is needed. The market will not stimulate and use PETs by itself; it is clear that government intervention is needed if privacy-enhancing "code" is really to carry weight to stem and stop 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.[266] Another interesting, if rare, example is the Data Protection Act 2000 of the German state of Schleswig-Holstein, which applies to public bodies; section 4 reads:

> (1) The data-processing body shall observe the principle of data avoidance and data economy.
>
> (2) Preference shall be given to products whose conformity with the data protection and data security provisions have been established by means of a formal procedure. The State Government shall make orders regulating the content and

265. *See id.*; Jessica Litman, *Information Privacy/Information Property*, 52 STAN. L. REV. 1283 (2000); Paul M. Schwartz, *Beyond Lessig's Code for Internet Privacy: Cyberspace Filters, Privacy-Control, and Fair Information Practices*, 2000 WISC. L. REV. 743.

266. *See* Reidenberg, *supra* note 117, at 218–19.

> format of the procedure and who is authorized to carry it out.[267]

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 and American legislation requires an "environment impact statement" to be made for certain activities, such as major construction activities, extraction of oil, and waste dumps, legislatures could impose an obligation to make a "privacy impact assessment" where cases of new technologies are being developed and marketed.

Second, there should be more binding mechanisms to respect privacy when possible and to infringe privacy only 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 the privacy risks of technology. As a corollary of a privacy impact assessment, 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 possible to uncover excesses and overly intrusive technologies at least. The control mechanism should also have some sanctioning power, like a prohibition of government purchases of privacy-unfriendly technologies or a power to fine companies that fail to make a privacy impact assessment or that market clearly privacy-unfriendly products.

Third, and perhaps most importantly, a PET action plan should raise the awareness levels of citizens, consumers, enterprises, government agencies, as well as 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 that is partly a result of privacy myopia. Only if people are aware that there is a "death of privacy" afoot and what this means for their future can (perhaps) a sufficient amount of leverage be established that can start to check the natural privacy-eroding tendency of technology.

267. Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein [State Data Protection Act, Schleswig-Holstein, Germany], GS SCHL.-H. II, 204 GL.NR. 4 (2000), *available at* http://www.datenschutzzentrum.de/material/recht/ldsg-neu/ldsg-n_e.htm.