'Code'

Leenes, R.E.; Koops, E.J.

Published in:
International Review of Law, Computers & Technology

Publication date:
2005

Link to publication in Tilburg University Research Portal

Citation for published version (APA):
Leenes, R. E., & Koops, E. J. (2005). 'Code': Privacy's Death or Saviour? *International Review of Law, Computers & Technology*, (3), 329-340.

INTERNATIONAL REVIEW OF LAW COMPUTERS
& TECHNOLOGY, VOLUME 19, NO. 3, PAGES 329–340, NOVEMBER 2005

‘Code’: Privacy’s Death or Saviour?

RONALD LEENES and BERT-JAAP KOOPS

ABSTRACT *Software code regulates behaviour and maybe even more so than legal code. For instance, digital rights management systems can prevent users from breaching copyrights more effectively than copyright law itself can. The relationship between ‘code’ and privacy is more complex than is the case with copyright. Where technology in general seems to have a negative impact on privacy, technology could equally be used for enhancing privacy. This article discusses the nature of ‘software code’ in relation to privacy. It argues that, often, privacy threats are not implemented in code on purpose, but that privacy erosion is nevertheless an inexorable side effect of technology. The paradigmatic reflex of data maximization, due to a lack of awareness on the part of developers – and users, is a major factor that leads to the erosion of privacy by technology.*

Introduction

The regulation of human behaviour can be achieved by various means.[1] Lawyers and legislators are all too familiar with the tool of legislation. Draft the rules you want people to adhere to and punish the offenders. Economists may point out that price is a more important motivator for people to behave in a desired way. Place a tax on liquor and people will consume less liquor, which is considered desired behaviour in most societies. Others may point out that, if norms are not internalized by society, they will not work. Hence, social norms could prove important and they are therefore actively promoted by means of media campaigns.[2] Finally, the physical environment can also be used for guiding people’s behaviour. Speed ramps are all too familiar examples of this kind of regulation. Lawrence Lessig, in his *Code and Other Laws of Cyberspace*, argued that architecture, as he called this latter kind of regulatory instrument, is increasingly used

Correspondence: Ronald Leenes,Tilburg University, TILT – Tilburg Institute for Law, Technology, and Society, PO Box 90153, 5000 LE Tilburg, The Netherlands. E-mail: r.e.leenes@uvt.nl.
Ronald Leenes and Bert-Jaap Koops are both associate professors in law and technology at Tilburg University.

ISSN 1360-0869 print/ISSN 1364-6885 online/05/030329-12 © 2005 Taylor & Francis
DOI: 10.1080/13600860500348572

for supplementing or even replacing traditional legal code as a mechanism for controlling behaviour.[3] He was interested in a particular kind of architecture, that of the Internet. By the architecture of the Internet he meant not only the atoms that make up the Internet, namely the cables, routers and computers, but also the bits, namely the software and protocols.

Lessig argued that, through 'code', by which he meant the design of the hardware and software elements that populate cyberspace and the design of the communication protocols that allow these elements to interact with one another, cyberspace is becoming a perfect tool of control.[4] Both the government and the private sector are embracing 'code' as a way of regulating the behaviour of people, both online and offline. In addition, while there are public debates about whether rules on behaviour are to be imposed by the three other modes of regulation presented above, as these instruments are primarily used in the public sector with its democratic legislative processes, this is much less the case with 'code'. There is no legislator who can be held accountable for the rules embedded in 'code', as this kind of regulation primarily emerges in the laboratories of corporations: 'code' suffers from a democratic deficit. Even worse, the rules themselves are opaque and can change without consultation or notice, while the level of compliance brought about by 'code' is almost absolute.

Lessig, following William Mitchell, emphasized that 'code is law'.[5] This conclusion may be too far-fetched, but in any case the intangible regulatory characteristics of 'code' make it a phenomenon in need of further study.

Lessig illustrated 'code as code' in, amongst others, the domain of privacy. His analysis was that privacy-threatening technology has upset the fragile traditional privacy balance. His solution to restoring the balance was vested on property law and 'code': the use of privacy-enhancing technology (PET). Was Lessig correct in his analysis and do the solutions he proposed offer opportunities for correcting the balance? This paper explores the relation between technology and privacy on the basis of a number of examples of IT applications and side effects.[6] The paper starts with a brief outline of Lessig's notion of 'code as code'. Then it will briefly look into a number of case studies that show the privacy-threatening potential of technology in action.

'Code as Code'

Lessig's notion of software as a means of regulating behaviour is not entirely new. It is an instance of what Joel Reidenberg had earlier coined *lex informatica*.[7] What it comes down to is that (information) policy can be embedded in network designs and standards as well as in the applications that run on top of these networks. These standards constrain the user's behaviour by making certain behaviour possible or impossible. Take Adobe Acrobat as an example. If the author of a PDF file determines that the ordinary user may read their document online and may also make low-resolution prints, but may not copy, modify or print the document at a high resolution, these policies can be embedded in the document. The PDF file contains meta-data that instruct the software application that is used for displaying the document, such as Adobe Acrobat reader or Apple Preview, to honour the document creator's policies. 'Code', therefore, can be used as a policy instrument, both consciously and unconsciously.

In comparison with traditional legal rules, 'code' has some particular characteristics that are worth mentioning.[8] Legal rules largely work *ex post*, whereas 'code' works *ex ante*: certain norm-violating behaviour is simply made impossible by the technology. Secondly, enforcement is relatively inescapable: whereas one can choose to disobey speed limits, most people cannot choose to disobey the restrictions imposed by a PDF file. 'Code' therefore has the potential to be fairly effective.

There is also the aspect of legitimacy. Looking at the enactment of rules, we may observe some less favourable characteristics in 'code'.[9] Firstly, rules embedded in technology are more opaque than the rules enacted by the legislator: they are not written down and, hence, are not open for inspection. Even worse, they can be changed without notice. Apple, for instance, has recently and quietly changed the iTunes application so that it no longer plays songs that make use of Real Networks' Rhapsody technology, which allowed iPod users to buy songs in Real's online stores.[10] In addition, 'code' can be and most of the time is implemented by private enterprises instead of the (elected) legislature. This means that 'code' is to a certain extent an instrument in the hands of the market, instead of in the hands of the state. Hence, 'code' may transcend the borders of what the law permits. This raises interesting questions. For instance, what does this means in terms of an obligation to compliance? Should we adhere to rules that limit our statutory rights or are these rules null and void?[11] In addition, should the legislature interfere when private coders go too far?

Technology, Privacy and Lessig's 'Code'

We now have a basic understanding of the concept of 'code' as a regulatory instrument. A clear example of 'code' in action can be found in digital rights management (DRM) systems. The aforementioned Adobe Acrobat reader is an example of such a system and so are Windows Media Player and Apple iTunes. These applications allow the user to access content in the way mandated by the rights holder. The software determines what the user can do with the content and simply restricts any action that is not in accordance with the permissions granted by the rights holder. The analogy with traditional legal rules is clear. Copyright law restricts the usage of copyrighted material. People are only permitted to access or copy songs with the rights holder's consent. The permission for certain specified uses is granted when someone buys an audio compact disc (CD) in a store. However, a notable difference between the traditional copyright scheme, which covers buying a traditional CD and the new 'code' scheme of buying the same songs in a DRM system is that the DRM system offers much more control over the usage of the content.

In certain areas of law, such as intellectual property law, the meaning of 'code' is fairly straightforward. In other domains, such as privacy,[12] it is much more ambiguous. Obviously, technology may affect privacy, as it allows for monitoring and surveillance and, therefore, clearly offers the potential for collecting, combining and profiling personal information that we want to keep to ourselves. But does technology embed privacy-threatening norms? Or does 'code' regulate behaviour in the way DRM systems do by preventing certain behaviour?

At first sight, the answer to the first question seems to be no. Technology and, in particular, information and communications technology (ICT) facilitates monitoring and searching. However, there seem to be no privacy-relevant rules hardwired in 'code' as is the case in the DRM example. The cases where privacy-relevant rules are hardwired are, on the contrary, more likely to be found in the privacy protection area. Examples here are the relatively well-known World Wide Web Consortium (W3C) projects

Platform for Internet Content Selection (PICS)[13] and Platform for Privacy Preferences Project (P3P).[14] The PICS allows content providers to add meta-data describing the nature of the content to Internet content. These meta-data can then be used in user applications for filtering content on the basis of the user's preferences with respect to what content they want to access or block. While originally designed for helping parents and teachers protect children from unsuitable material on the Internet, privacy-protecting meta-data and filters can also be assigned, thereby broadening the scope of use.[15] If content providers label their content with meta-data describing their use of personal data provided by the user, this would allow the user's application (a web browser, for instance) to decide whether a website honours the user's privacy preferences. Even more to the point is the P3P, as this is specifically designed for matching user privacy preferences with service provider privacy policies. The P3P offers users the means of expressing their privacy preferences and provides for protocols that allow websites to present their privacy policies in machine-readable form (XML). The user's browser can then alert mismatches between the user's locally stored privacy preferences and those of the website they want to enter.

Thus, at first glance, 'code' in itself does not appear to affect end-user behaviour in the way it does in other domains. Furthermore, 'code' appears to offer end-users means of taking more control over their personal information. Does this mean that 'code' is privacy's saviour?

Technologies of Control

Privacy or, for the purpose of this paper, informational privacy, namely data protection or the right to control one's own personal data, is not an absolute right, but one that has to be balanced against other values. In the domain of law enforcement, the right to keep one's personal data to oneself has to be balanced against society's need for preventing crime or locating criminals. The result of this balancing act is that law enforcement agencies are given powers to invade people's private spheres. The extent of these powers may change over time, depending on many circumstances. Nevertheless, constitutional law set limits to these powers. For instance, article 8 of the European Convention on Human Rights and Fundamental Freedoms (ECHR) determines the circumstances that may warrant breaches of privacy.[16] Basically, infringements should be proportional to the legitimate goals of the regulation and the goal should not be attainable by other less infringing measures. It is here that the traditionally American notion of 'reasonable expectation of privacy' is also coming into play in Europe. The balancing test of deciding when a privacy violation is necessary in a democratic society depends, after all, on the seriousness of the privacy violation and this in turn relies to a certain extent on the way or amount of privacy that people experience in that particular context. The 'reasonable expectation of privacy' notion changes over time and gives rise to complex case law, particularly with respect to the online world.[17]

What makes matters possibly more complicated is that people generally base their online expectations on offline experiences and expect to have the same level of protection online. In the case of new privacy-invasive technologies, users may therefore have an unwarranted expectation of privacy. An example here is webradio or webcasting, which, to the average user, is the same as traditional radio, but carried by ethernet instead of by ether radio waves. However, from a privacy perspective, there is a crucial difference. Whereas listening to a traditional radio cannot be monitored, its online twin allows for monitoring and, in fact, is monitored. This is due to the fact that webradio is essentially a pull medium: the listener's application has to request the server to start an audio stream to it. Webcasters are obliged to keep (detailed) records of the IP addresses of the machines[18] that receive these audio streams, what was streamed to them, and for how long, for royalty collection purposes. These listening logs are then provided to collective rights management organizations, such as UK Phonographic Performance Limited, which charge the webcasters the appropriate fees for broadcasting the material they offer.[19]

IPs can often be traced to individual users and, hence, the listening logs reveal data about the individual preferences of webradio listeners. It goes without saying that these data can then be used for constructing profiles of these listeners, which can then be used for all sorts of possibly desirable uses, such as customized offers and release notices for new albums of favourite artists, as well as undesirable uses, such as price discrimination or exemption of services.

This example shows two interesting facets of the privacy aspects of new technology. Firstly, as mentioned, the vast majority of users will not be aware that their behaviour is monitored, as the false offline analogy has put them on the wrong track. The second observation is that there is no pressing need to use data that can be traced back to individual users for the purpose of royalty collection. UK Phonographic Performance Limited or, so we hope, is not interested in knowing which individuals listen to the broadcasts: they only want to be able to charge webcasters for the actual audience. The technology offers them a way of making a much more correct estimation of the 'consumption' of the songs when compared to traditional radio. However, for counting pricked-up ears they could equally well have used a more privacy-friendly way, such as using a one-way encrypted version of the IP address that cannot be traced back to individual listeners. The reason they have opted for IPs is presumably not one of malevolence, but of ignorance of the privacy implications of their choice.

In the webradio case, IPs function as the virtual breadcrumbs that allow service providers to track and monitor individual Internet users and usage. This is also the case for search engines, such as Google, which store IPs and the search queries submitted from these IPs and for websites that store the IPs of their visitors along with their click paths. All these data can be used for profiling and monitoring Internet users and all that is needed for creating a really rich data source is to associate the IPs with real individuals. Other features of the Internet contribute to these rich data sources as well. For example, cookies enhance the capabilities of profiling by storing information on the user's personal computer (PC), for instance about preferences, last visited page and user name and identification, but also markers left by advertisers or advertising service providers such as DoubleClick that allow them to spot individual users. These data can later be read by other websites. Although people are aware they leave a trail while surfing on the Internet,[20] the awareness of what can be done with this data is less well known. In addition, the ability that organizations such as DoubleClick have for linking data from a large variety of websites is unknown to the public at large. The profiling capacity of suppliers of banners and pop-up advertisements dwarfs that of their customers (the individual corporations), as these latter only have insight into the behaviour of their own visitors, whereas DoubleClick receives data from clicks on any of the sites that host their customers' banners.[21]

Besides IPs as the modern equivalent of breadcrumbs, mobile phones also leave valuable traces as telecom operators are able to track the location of a cell phone to within tens to hundreds of meters, depending on the cell size. This occurs not only when they are used to place telephone calls, but they also provide data that reveal information about their users in standby mode. Moreover, much more precise location technologies are being developed that open up business opportunities for providing location-based services, such as on-the-spot advertising. Imagine the following sort of text message appearing on your cell phone soon: 'Hungry? Around the next corner you will find a Pizza Hut which offers you a free Coke on the purchase of a Quattro Stagioni Pizza. Do come in!' In addition, dating services, way finders, and even games[22] can be based on the location data provided by mobile phones. Convenience and new services are the driving forces for this use of location data.

Mobile phone numbers and their associated calling patterns are also used. Obviously, mobile phone operators need phone numbers in order to establish connections and for billing purposes. However, some mobile phone operators go beyond this primary necessary use and use calling patterns or customer profiles for detecting theft, payment fraud and identity fraud.[23] For example, calling patterns can be used for noticing changes in a user's behaviour and, hence, can be a signal that a phone has been stolen. In addition, non-paying customers who are disconnected from the service and who obtain a new phone under a false identity may be recognized by comparing stored profiles against the new user's behaviour.

Privacy-infringing Code?

The examples we have given show that information technology (IT) benefit users as they offer services that are conveniently better or completely new. On the other hand, the use of these services leaves traces that can be exploited by service providers and others for uses that are undesirable from a privacy perspective. The exploitation of personal data in these cases was not built-in the technology on purpose, but it is nevertheless a side effect. However, there are two areas that represent notable exceptions to this observation about unintentional privacy threats: law enforcement and national security.

As of old, law enforcement and national security have been prime contenders in privacy debates, as they aim at safeguarding a secure and just society. Their interest is to reveal what the 'bad guys' want to keep hidden. Hence, there has always been pressure to allow state agencies to collect data and infringe upon citizens' privacy. However, the imminent risk in giving law enforcement agencies and national security agencies too many powers has also always been acknowledged. As a result, there is a system of checks and balances in place that should limit the powers of these agencies in invading our privacy. For example, the legal power to intercept telecommunications is limited by the requirement of a court order and other safeguards such as probable cause.

Interception provides a good example of intentional 'code'. Telecom operators have been forced to design or adapt their equipment in such a way that wiretaps are possible. Telecommunications developments in the 1990s were thought to render classical wiretaps largely irrelevant and, therefore, governments have enacted legislation in order to safeguard the interceptability of telecommunications equipment. In the USA this was established by the adoption of the Communications Assistance for Law Enforcement Act of 1994, which requires that telecommunications carriers ensure that their equipment, facilities and services are capable of, among other things, enabling the government to intercept communications content and address call-identifying information.[24] The European

Union (EU) followed shortly afterwards with a Council Resolution,[25] which was subsequently implemented in the EU member states.

The 11 September 2001, 2004 Madrid, and July 2005 London terrorist attacks have fuelled discussions for allowing enforcement and security agencies even more powers and access to the kinds of data discussed in this section. Recently, the discussion at the European level, as well as in various EU member states, on introducing a requirement for all telecoms providers (mobile phone operators as well as Internet service providers) to keep records of all traffic data of European citizens for a duration of 1–3 years clearly underscores this trend.[26]

The law enforcement and national security examples differ from the cases described earlier. Here, we clearly see that technology is shaped intentionally in order to facilitate privacy infringements. Law enforcement agencies are capable of and have the authority for intercepting all sorts of communication. Privacy infringement in this case is intentional and not a by-product.

When we combine these examples with the earlier examples of unintentional by-product privacy threats, we see that technology offers ever more opportunities for large-scale monitoring, from intercepting all communications to monitoring the movements of people, both online, through Google searches, weblogs and DoubleClick logs and offline, with location data. The parties capable of monitoring are usually the people in power, governments and large corporations, who have a vested interest in personal information for various reasons. Since they set the rules, one cannot expect monitoring efforts to decrease. This need not necessarily be for reasons of malicious intent of monitoring for the sake of gaining more control, but it may equally well be an effect of function creep. New applications, such as webcasting, offer slightly more control than the previous ones and, although there may be some opposition to this potential increase in control, people usually gladly accept the new possibilities for the sake of enhanced convenience. As time goes by, the increased control is no longer seen as a side effect, but as an intrinsic characteristic of the new application. When this happens, the reasonable expectation of privacy with respect to the application in question has slipped away. Moreover, all along this process ever-new features or capabilities are introduced that amplify and reinforce the process, ultimately leading to a gradual erosion of privacy.

Technologies of Freedom

The previous section sketched a dark image of the impact of technology on privacy. How does this relate to the fact that technology can also be used for protecting privacy, such as the PET example we mentioned earlier? Lessig, in fact, placed his hopes for privacy in the information age on two instruments: giving people property rights in their personal information and enforcing these through PETs. The commodification of personal information guarantees that data processors have to approach individual people in order to 'buy' and process personal information, which is a radically different mechanism to the *ex post* legal sanctions that are currently enacted in data protection legislation. PETs can be seen as instruments for negotiating the terms under which a particular data subject is willing to grant permission to use their personal information. We will not go into the property rights part of the solution here.[27] Instead, we will briefly discuss some examples of PETs in order to show their prospects and limitations.

The notion of PETs was coined in the early 1990s in a joint publication by the Dutch and Ontarian Data Protection Authorities.[28] The key notion of PETs is that a minimum amount of personal data is collected for a specific goal and that all other data are shielded-off. PETs can make decisions on behalf of their user about whether or not to make use of a particular service and what personal data are to be disseminated. Another example of a real-life PET is biometrics, which is used as an instrument for controlling restricted access to a secure building or area. Authorized visitors, such as employees, can obtain a smart card that holds biometric data, such as an iris scan or a fingerprint scan. The smart card is only handed out after verification of the identity and legitimate rights of the person. When they want to enter the restricted area, the biometric scan of the iris or fingerprint is matched with the template stored on the card, without consulting central databases. There is no need to store information about the individual requesting access: the fact that it is the same individual as one who has a legitimate access card suffices for the goal of restricting access. Biometric data combined with a smart card can thus enhance privacy while allowing for legitimate control of people.

Yet another use of PETs can be imagined at the crossroads between organizations, by implementing what is coined 'privacy by design'. Here, privacy protection is implemented in 'code' by maintaining data walls between sectors and applications. In the current (Dutch) practice of housing benefits, the responsible agency receives income data from the tax authorities and rental data from the housing corporation. These data determine the entitlement and amount of housing benefit of a client. The PET solution for this service does not rely on the exact income of a client being provided by the tax authority, but on a response of 'yes' or 'no' to a query asking whether the citizen's income is below a relevant threshold.

Privacy risks are particularly imminent in cases where organizations share or exchange information. The sharing of information can be beneficial for both citizens as well as data-processing agencies and, hence, is not necessarily a bad thing. In order to be able to share data and do this in an efficient way, standardization and the use of unique identifiers is often introduced. The downside of this scheme is that data can easily be linked. Furthermore, misuse of the combined data is hard to prevent. PETs can help here as well. Instead of setting up data exchange on the basis of a single unique identification number, such as a social security number, a meaningless but unique number can be used for serving as a reference to deliberately fragmented and, as such, only partially accessible personal data domains. Technology can then be used for enforcing compliance with data protection regulations and safeguard the data subjects' informational privacy.[29]

The examples show that technology can be used for enforcing privacy regulation at various levels in the interaction between users, systems and networks. Some of the examples place control over personal data in the hands of the data subjects themselves, while others limit the amount of data that can be collected and used for profiling purposes. If this is indeed as appealing as it sounds, then why are PETs not widely used in real life?

The Trouble with Privacy-enhancing Technologies

The reasons why PETs are not widely proliferating, to use an understatement, are manifold. They concern both end-users, namely customers and citizens, as well as service providers, namely governments and commercial enterprises. On the consumer side the reasons for non-adoption of the kinds of PETs they could install and use, such as the P3P, range from ignorance of privacy threats or of the existence of PETs or not seeming to care about privacy to the overhead of time and frustration that installing these applications means for almost all consumers. Moreover, if consumers wants to take their privacy seriously and decide not to disclose all sorts of personal information and not to accept cookies, they will soon discover that surfing on the Internet is a less than thrilling experience. Most websites at present do not accept web browsers that refuse cookies, and when they do offer few services, as these rely heavily on cookies being set in the consumer's browser. In addition, even if the consumer accepts cookies but is unwilling to provide all sorts of irrelevant data, such as their date of birth, as requested by an online store, they will discover that services such as buying goods online is simply impossible: fields irrelevant for the service as such are often mandatory fields on online forms.

The bottom line for client-side PETs is that, as long as there is no marketplace where companies compete on privacy, the individual consumer does not have a real option to withhold personal data. Hence, the implementation of client-side PETs is to a large extent not very realistic.

From the perspective of service providers there are two principal reasons not to implement PETs: lack of interest and ignorance with respect to alternatives. The former we have already briefly discussed: industry has a vested interest in collecting personal data for marketing and profiling purposes and, hence, has very little incentive to change. This is all the more so since individual consumers are powerless and governments are slow at best and unwilling at worst to intervene too strongly in the emerging online world.

The second reason, ignorance, is probably even more important. Since, in our opinion, the best opportunities for saving privacy from a slow death lie in this area, we now turn to this aspect in more detail.

The Wrong Paradigm

In government, but also in industry, it is too easily assumed that the identity of the user is essential to providing a service, establishing trust or accountability or improving service delivery. Within the public sector, for instance, it is usually taken for granted that the government should know the citizen's identity in order to perform any task or service. However, often this need not be the case at all. For example, when a neighbourhood planning committee collects comments from citizens through a website, it will usually list the names and addresses of the participants in order to be able to check whether only people with a genuine interest in the neighbourhood are participating. If there is a requirement of only being permitted to participate in the online hearing when one actually lives in the neighbourhood, then one could use other less privacy-invasive checks than listing individual identities. The check on neighbourhood residency can, for example, be done by another agency than the one running the online hearing. Technology can facilitate such privacy-friendly verification in numerous ways, depending on the desired level of security, from anonymous or pseudo-anonymous smart cards with biometrics handed out by a municipality to each citizen to merely publishing a generic access code in the local newspaper. Indeed, biometrics is a technology that may be used in a non-identifying way by allowing compartmented access to the relevant characteristics of a person stored on a smart card. In fact, technology in general offers countless possibilities to make a wide range of distinctions between anonymity and identity.

The same mechanism applies to the use of cookies. Cookies are an easy way of keeping track of information between page views, both within a single session and between distinct sessions. Within sessions, however, cookies are no longer necessary for conveniently storing temporary information. All web server programming languages offer session support features, thereby obliterating the need for session cookies.[30] In addition, as to cookies that aim at recognizing returning visitors, one could equally well ask visitors to identify themselves. However, the privacy-friendly option seems simply not to be considered in practice. The fact that, contrary to the new requirements of the Directive on Privacy and Electronic Communication,[31] most European websites do not ask visitors for their consent for placing cookies reinforces our impression that industry is simply not very aware of the (privacy) issues surrounding cookies. In fact, many cookies have undoubtedly been implemented because they were considered the fastest and easiest way of getting the site going in the first place and, hence, were not installed with the intention of collecting user data.[32] Again, we see that the paradigm of privacy protection as the starting point, which might be inferred from data protection regulations, is ignored in practice. Instead, another paradigm is dominant: to follow technology along its natural path of data collection and to worry about privacy only as an afterthought.

Why are data minimization, collection limitation, purpose specification and other privacy architecture principles not the norm in practice, as they seem to be the norm on paper in data protection law? This is because data maximization and identification are the paradigmatic reflexes of system designers. They are the first things that spring to mind when people design systems for offering online services. Data protection as such stands powerless against this mechanism, because it is based on a different paradigm, which is not incorporated in the people who decide, through design or policy, on the way that technology is shaped.

Conclusion

IT and privacy have a hard time passing through the same door. Some have gone as far as proclaiming privacy dead in the information age.[33] We do not want to go that far, since we still think that some form of privacy is a necessary feature of the fabric of our society.[34]

Therefore, it is important that there exist possibilities for citizens and consumers of regaining some control over their personal data. Technology may play an important role in this respect. However, equally important is the education of industries and governments, as well as individual consumers and citizens. Industries and governments have to become aware of the fact that, what they try to establish, be it trust, individuality, one man, one vote or something else, can always be established in a more privacy-friendly way than they may envision at first sight. Privacy by design should be promoted in these circles. Individual consumers and citizens have to become aware that personal data is important and that, without proper precautions, their data will be used for purposes that do not benefit them in the end. Finally, the legislature is of crucial importance.

Technology alone cannot do the trick, nor can public awareness. We subscribe to a conclusion drawn by a European Commission working party in 1998 with respect to the P3P:

> A technical platform for privacy protection will not in itself be sufficient to protect privacy on the web. It must be applied within the context of a framework of

> enforceable data protection rules, which provide a minimum and non-negotiable level of privacy protection for all individuals.[35]

What this paper boils down to then is the notion that, if we want to preserve an acceptable level of privacy, we will need a paradigm shift from data maximization to privacy by design. In order to achieve this, all regulatory instruments available will be called for. Only a concerted effort of legal regulation, self-regulation, awareness raising, organizational measures and technological measures may save privacy from slowly suffocating to death in technology's all too-embracing arms.

Notes and References

[1] Lawrence Lessig, *Code and Other Laws of Cyberspace*, Basic Books, New York, 1999.

[2] The 'Smoking kills' notices on cigarette boxes is an example of this kind of attempted social influencing.

[3] Lawrence Lessig, *Code and Other Laws of Cyberspace*, Basic Books, New York, 1999.

[4] *Ibid*.

[5] *Ibid*, p 6.

[6] These cases are derived from the ones presented in R E Leenes and B J Koops, 'Code' and privacy, in L Asscher (ed.), *Coding Regulation. Essays on the Normative Role of Information Technology*, Information Technology & Law Series, T.M.C. Asser Press, 2005.

[7] Joel Reidenberg, Lex Informatica, The Formulation of Information Policy Rules Through Technology, Tex. L. Rev 76 (1998) 553. He had addressed the issue of the relation between technical standards and legal rules earlier in Reidenberg, *Harvard Journal of Law &Technology*, p 301, 1993.

[8] See Joel Reidenberg 1998, *supra*, 553 for a more extensive overview of the advantages of *lex informatica*. See also Asscher 2005, *supra*, for an extensive account of the notion of 'code as law'.

[9] On the legitimacy of 'code', see extensively the chapter by Lodewijk Asscher in Asscher 2005, *supra*.

[10] See, for instance, <http://www.theregister.co.uk/2004/12/15/apple_vs_real/>

[11] DRM systems, for instance, generally do not honour the copyright exemptions granted by copyright law. In The Netherlands, for instance, making a copy of a copyrighted work for personal use is allowed under Dutch law. Preventing people from making unauthorized copies of the works distributed by means of DRM systems contravenes this legal exemption.

[12] We limit the notion of privacy for this paper to informational privacy and leave other dimensions, such as relational and physical privacy, outside our scope.

[13] <http://http://w3.org/PICS/>

[14] <http://www.w3.org/p3p>

[15] See, for instance, <http://www.droit.fundp.ac.be/crid/eclip/pics.html>

[16] Article 8, ECHR:
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.

[17] For an overview of relevant US case law both offline as well as online see, for instance, Fred Cate, *Privacy in the Information Age*, Brookings Institution Press, Washington, DC, 1997.

[18] The address under which a computer can be reached on the Internet. One of the author's office Mac, for instance, has the IP address 137.56.38.21.

[19] See <http://www.kurthanson.com/archive/news/092304/index.asp>

[20] For instance, 87% of the repondents in an EC survey were said to be aware that personal data are stored and processed on the Internet. European Commission, *Questionnaire on the Implementation of the Data Protection Directive (95/46/EC): Results of Online Consultation*, 20 June to 15 September 2002.

[21] The fact that DoubleClick acquired Abacus, the holder of the world's largest conventional direct marketing database in 1999 makes it even more troublesome. See Lilian Edwards and Geraint Howells, Anonymity, consumers and the Internet: where everyone knows you're a dog, in C Nicoll, J E J Prins and M J M Van Dellen (eds), *Digital Anonymity and the Law: Tensions and Dimensions*, T.M.C. Asser Press, pp 207–247, 2003.

[22] It's Alive, a Swedish company, had a first with Botfighters, a location-based mobile game where people design a robot on the game's website and then battle against other players out on the streets, <http://www.itsalive.com>

[23] Ton Schudelaro, *Electronic Payment Systems and Money Laundering Risks and Countermeasures in the Post-Internet Hype Era*, Wolf Legal Publishers, Nijmegen, 2003.

[24] 47 U.S.C. § 1002 (a).

[25] Council Resolution of 18 January 1995 on the lawful interception of telecommunications (96/C 329/01), *Official Journal*, 4 November 1996.

[26] In October 2005 two traffic data retention proposals are pending in Europe: one by the Justice and Home Affairs Commission of the Council, and one by the Commission (21 September 2005). See <http://europa.eu.int> for more information.

[27] An extensive account of personal information as property rights can, for instance, be found in Corien Prins, Property and privacy: European perspectives and the commodification of our identity, in L Guibault and P B Hugenholtz (eds), *The Future of the Public Domain in IP*, Kluwer Law International, The Hague, London and Boston, 2005.

[28] Registratiekamer, *Privacy-enhancing Technologies: The Path to Anonymity*, Registratiekamer, Rijswijk, 1995.

[29] See A Campbell, *Privacy Architecture*, Government of Alberta, November 2003, for an example of such a system designed for the Canadian province of Alberta. This system received the HP Privacy Innovation Award in 2003.

[30] See for session support in PHP, a popular programming language for websites, <http://www.php.net/manual/en/ref.session.php>

[31] Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (directive on privacy and electronic communications).

[32] One of the author's can speak from experience here.

[33] For example, Reginald Whitaker, *The End of Privacy: How Total Surveillance is Becoming a Reality*, New Press, New York, 1999, A Michael Froomkin, The death of privacy?, *Stanford Law Review*, Vol 52, pp 1461–1543, 2000 and S Garfinkel, *Database Nation. The Death of Privacy in the 21st Century*, O'Reilly, Cambridge, 1999.

[34] See Leenes and Koops, 'Code' and privacy, *supra*, section 5.6, for an elaboration of this view.

[35] Working Party on the Protection of Individuals with Regard to the Processing of Personal Data, Opinion 1/98, Platform for Privacy Preferences (P3P) and the Open Profiling Standard (OPS), 16 June 1998.