4. Privacy

Dr. Jaap-Henk Hoepman, TNO and Radboud University Nijmegen, the Netherlands.
Drs. Marc van Lieshout, TNO, the Netherlands.

5.294 woorden

4.1 Privacy: a fundamental right

What is privacy?

The definition of privacy which is presented by Zureik et al. (2010) captures most relevant dimensions that usually can be found: (1) the right to be let alone (no intrusion by third parties if not wanted), (2) limited access to the self (e.g. refuse to open the door of your house if you don't want to), (3) secrecy (e.g. correspondence, such as e-mail must remain confidential)), (4) control of personal information (e.g. being able to know what the super market or the tax office have collected about you), (5) personhood (e.g. you may experiment with your identity, if that makes you happy), and (6) intimacy (no one can enter the very private sphere around you if not allowed to do so). These six dimensions are loosely related to a classical distinction made by Westin (1967), differentiating between various spheres of privacy: solitude, intimacy, reserve and anonymity. These two definitions show that privacy is a relatively broad concept that captures various aspects of ordinary life.

When looking from the angle of information and communication technology, the focus is primarily on the informational dimension of privacy. It deals with personal data that floats around and that may be used - outside direct control - of the subject to which the data relate. In this context one can define privacy as the right to control the release of personal information about oneself, even when that data is collected and stored by a third party.

Although proper security mechanisms to protect personal information are necessary to prevent unauthorised access and use of that information, it is important to understand that privacy is not the same as confidentiality (or data security). The right to privacy also stipulates that personal data is only collected when this is necessary, that no more personal data is collected than needed, and that this data should only be used for the purpose for which it was originally collected. Also, people have the right to view and update personal information held by others about themselves.

The importance of privacy

Privacy is not only a personal value, but also a common societal value. Offering a personal shelter to all has potential benefits for society as a whole. It is a prerequisite for realising all of one's own potentials and to be able to develop one's own opinion, which in turns contributes to the development and innovation of society as a whole (Solove, 2010). Privacy has always been related with freedom: being free from intrusion against one's will, and being free in choosing one's own life path, so being autonomous. The origins of this position stem from liberal thinkers such as John Locke who state that free individuals are for the benefit of a free and open society.

But what about people who say 'I have nothing to hide'? This often heard argument (sometimes phrased as 'If you have nothing to hide you have nothing to fear') is wrong for several reasons. First of all, it assumes that privacy is about hiding wrong, illegal, things. But all of us have many innocent, perhaps even irrelevant things that we would not like to reveal to others, such as our salary, our PIN code, our sex-life, and many more. Secondly, things that are legal or harmless now, may be illegal in the future. If you reveal them now, they may harm you lat-

er. Similarly, things that are normal in one context (a party, a holiday) are frowned upon in another context (at work).

The threat to privacy

The invention of computers has made it possible to store data in digital databases that can be searched very efficiently. Furthermore, the rise of the Internet has made it easier to interconnect databases. This allows for more complex searches and mining for more complex patterns. Data collected in one context (e.g. your work) becomes connected to data collected in another context (e.g. your private life).

In fact we live in an 'information society'. In economic terms, information has become a resource (like oil, water, etc.). Information, including personal information, has economic value. In societal terms, information is increasingly used as the fabric with which we build relations with our peers, our friends and family. We use mobiles, email, or social networks (like Facebook) to stay in touch. In fact we increasingly use such social networks to build and expose our own self-image or identity. Much of that information is very private in nature, but is stored centrally by the social networks, and accessible to 'the whole world' (unless you have applied the right privacy settings.[1]). This personal information is the main economical resource of these networks. It is therefore in the interest of such networks to collect as much (personal) information as possible, in order to increase company value.

Another threat to privacy is the increased aversion to risk in our current society. In the 20th century, the western world has experienced a tremendous economic growth. People are much better off now than they were a century ago, and as a result they stand to lose much more. In the last decades this has led to the development of a 'risk-averse society' where increasingly stronger levels of control are implemented to prevent mis-happenings and to limit risks. Camera-surveillance is an example of this trend (Beck 1990, Giddens 1992)

The 9-11 terrorist attacks and the events that followed have further increased the need for so-called homeland security, to protect our society from outside attacks. This has resulted in invasive anti-terrorism laws and increased surveillance. Airport security has intensified because of this, including the development of so-called body scanners. And governments surreptitiously gain access to more and more sources of data, like the US government that monitors international bank transfers of EU citizens through the international banking network SWIFT [COM(2010)385 final]

Legal measures

One typical approach to protecting privacy is using legal measures. Most prominent is the Universal Declaration of Human Rights. In article 12 it is stated that 'No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.' This right to protection is repeated in the European Charter of Fundamental Rights (2000) which states that everyone has the right to respect for his or her private and family life, home and communications (article 7) and everyone has the right to protection of personal data (article 8). The distinction between both articles is telling: while article 7 relates to privacy, article 8 relates to personal data. In our approach we would consider article 8 to relate to the informational dimension of privacy. As we will show, in current practices both articles become more closely related.

In national legislation the right to privacy is generally recognised in the Constitution. The Dutch Constitution for example states that all Dutch citizens have a right to privacy (article

[1] Note however that sometimes, privacy settings are ignored or adjusted by organisations. Facebook did so in 2010 when adjusting all privacy defaults to 'open to the world'. This was heavily criticized and as a consequence Facebook had to change its privacy policy back again.

10). Though not referring to an absolute right (even constitutional rights need to be balanced against each other) privacy can thus not easily be 'traded away'.

It is especially the right to protection of personal data that is of relevance for this chapter. This right has led to some important European Directives.[2] The two most relevant ones are the directive 'on the protection of individuals with regard to the processing of personal data and on the free movement of such data' (Directive 95/46/EC) and the directive 'concerning the protection of personal data and the protection of privacy in the electronic communications sector' (Directive 2002/58/EC). This latter Directive has meanwhile been inserted in a larger Directive (2009/136/EC) which integrates two directives (one on Universal Service as well) and a Regulation on consumer laws. Some aspects of the 2002/58/EC directive have been elaborated in more detail in the new Directive.

Directive 95/46/EC formulates a number of criteria for the lawful processing of personal data. These criteria refer in turn to a set of privacy principles which has been formulated by the OECD already in 1980 (OECD 2011). Each processing of personal data means a possible infringement on the privacy of the people whose data are collected and processed. This is only allowed when it can be justified on the following aspects:

1. it serves a legitimate aim
2. it is lawful
3. collecting and processing the data is necessary (for instance to deliver a service or a product).

When collecting data can be justified, the collection process itself should meet the following criteria:

1. it should serve a clear purpose
2. the purpose cannot be achieved in another, less invasive way (subsidiarity)
3. the data collection should be proportionate (not excessive and in line with the purpose)
4. safeguards should be in place (security measures, quality of data)
5. the rights of the 'data subjects' should be guaranteed (informed consent, right to access and correct the data)

An important exception to the safeguards presented is the need to infringe upon someone's privacy because of national interest or a relevant public interest (Data protection directive 95/46/EC article 3). The fight against serious crimes and terrorism may require that privacy infringements are necessary. A relevant tool in this respect is the possibility to retain data for a specific period of time. The European Data Retention Directive (2006/24/EC) prescribes that all European countries are obliged to determine a specific period of time in which traffic and location data need to be retained. The Netherlands choose for a period of twelve months, which is double the minimum period of time posed as minimum standard by the European Data Retention Directive. Protecting the borders of Europe against illegal immigrants requires exchange of personal data between border authorities. Emergency services also have the opportunity to infringe upon someone's privacy in case of an alert that requires direct intervention. In all these cases the main question is the extent of privacy infringement which is acceptable and the safeguards which should be in place to support citizens in exercising their democratic rights. This is not an easy playing field. A relevant phenomenon is the so-called *function creep*: over time the functionality of a system may change and grow, encompassing functions which are different from the original purposes of the system. An illustration of function creep is provided by the public transport card. Public transport cards are RFID-based cards today. Travel data are stored for optimising transport efficiency and for reducing fraud in travelling. Every now and then intelligence services request

[2] Directives oblige Member States to develop national laws which implement the content of the Directive.

travel data in order to track criminals. The rise in requesting these data has been manifold since the introduction of the RFID-based public transport card. It is however not known how many additional criminals have been caught by using these data. It is thus hard to assess the justification of this privacy infringement. Data were never collected with the aim to use them for tracking criminals. National interest may play a role here and may – as stated above – legitimate the use of these data. Commercial objectives form another purpose for data collection (to offer non-travel related services, for instance). The Dutch owner of the public transport card, TransLink, had formulated offering commercial services with no direct link to travel functionalities) as a purpose for the intended data collection. The Dutch Data Protection Authority considered this to be out of scope of the original purpose of the data collection and thus requested TransLink to reconsider and reformulate its strategy towards using collected and aggregated travel data.[3]

Technical measures

Informational privacy deals with the release and control of *personal identifiable information (PII)* – information that can be linked, with reasonable effort, to a natural person. A reasonable effort in this context is for example to use data in several different databases (even if some of those are not under your immediate control) to establish such a link. This is why the European Article 29 Working Party (an organisation formed by the European Data Protection Authorities and initiated as consequence of Article 29 of the European Data Protection Directive 95/46/EC) expressed the opinion (Art29WP 2010) that an IP address is personal information: using the database of the Internet Service Provider (ISP), the name and address of the account holder that correspond to that IP address can be determined.

The goal of technical measures to protect privacy is to make it difficult (if not impossible) to link a piece of information to a natural person, and to give a user control over its personal data once it has given that data to someone else. We note that surprisingly few tools are available to control data once it has been released. So we focus on the so called Privacy Enhancing Technologies (PET) to hide the link between persons and their personal data. These technologies aim to achieve a certain level of *anonymity*, *unlinkability* or *unobservability* (Hansen & Pfitzmann 2011).

Anonymity is defined as 'the state of being not identifiable within a set of subjects', which captures the intuitive notion of 'hiding in the crowd'. *Unlinkability* guarantees that two events or data-items cannot be linked to each other. Examples of such events are visiting several websites, or sending several emails. Examples of such data-items are your subscription to a newspaper, or your current place of work. Finally, *unobservability* guarantees that nobody is able to tell whether a certain event (like sending a message) did or did not take place.

A powerful attack against these privacy properties is called *traffic analysis.* It can be used to determine the sender and receiver of a message without looking at the content of the messages, and therefore works even if such messages are encrypted. It typically involves monitoring several network links under one's control, and trying to correlate the messages one sees on different links. Traffic analysis (and the related concept of network analysis that maps relationships among people based on user profiles on social networks) is a powerful tool to determine the mutual relationships between people in a group, and is often used in criminal investigations (for example requesting the phone and/or e-mail records of suspected individuals). Data retention ensures that the relevant (historic) communication data is available to achieve this.

[3] Although it did not in fact prevent the subsequent introduction of the OV-chipcard in the Netherlands.

Some techniques

We will briefly describe some of the basic privacy enhancing techniques that can be used to combat traffic analysis and implement certain levels of unlinkability.

Pseudonyms can be used to hide the relationship between a real natural person and some personal data. Nicknames or arbitrary numbers can serve this purpose, as long as the relationship between pseudonym and a real person is unknown.

Mix networks are deployed to thwart traffic analysis and to achieve unlinkability. Traffic analysis works under the assumption that incoming and outgoing messages at a server can be related to each other by looking at their content, size and the time and order they came in and went out again. Mix networks make this harder, by re-encrypting incoming messages before sending them out, and padding all messages with extra bits to make them the same size. Mix networks also use a store-and-forward process whereby a server stores incoming messages until a certain number of them have been received before sending them out in random order. A well-known implementation of a mix network is Tor.[4]

Secret sharing is a technique that allows one to split a message (or a key) into several shares such that each share all by itself contains no information about the message. To reconstruct the message, all, or a subset of the shares need to be brought together.

Anonymous credentials are a form of anonymous attribute certificates. Similar to attribute certificates, such credentials express a property about a subject (like 'the bearer of this credential is over 18 years old'), that is signed by an authority that can verify the validity of the claim. Traditional attribute certificates are not anonymous, because the same certificate is presented whenever one wants to convince someone about the validity of a claim.

Privacy by design

The technical opportunities to prevent personal data to be misused can be complemented with other measures. Organisational measures may help preventing unauthorised access to personal data. This may include specific privacy officers who need to create more awareness for privacy aspects throughout the organisation. Large companies, such as Google and Nokia, employ officers whose main task is the formulation and safeguarding of a privacy policy for the company, raising awareness within the company for privacy issues and presenting the company in the outside world when privacy is at stake. In the Netherlands, the Dutch Data Protection Agency had such a role as well.

Since all information systems need to comply with national and international regulations and laws, a variety of tools have been developed that support a more integrated or holistic approach towards the role of privacy in developing and using new systems. This approach is known as *privacy by design*. Privacy by design adopts the perspective that privacy should not be regarded as an issue that needs to be taken into account when a system is ready for use but that privacy should be adopted as one of the *design parameters* of a system, already in the early stages of systems design. Privacy by design not only considers technological measures as means to safeguard privacy of individuals but includes physical and organisational measures as well. This requires an analysis of the privacy risks *before* a system is developed. *Privacy impact assessments* (PIA) offer a methodological framework to assess these risks (Van Lieshout et al 2011).

During the 2010-annual meeting of data protection agencies gathering in Jerusalem a resolution was adopted that was centred on the notion of privacy by design. The resolution prescribes that technology, business practice and physical measures go hand in hand. The following seven privacy principles show the way forward:

1. Be *proactive* instead of reactive.

[4] http://www.tor.org

2. Privacy should be a *default* setting.
3. Privacy should be *embedded* in the design.
4. Privacy-embedded systems still should offer *full functionality*.
5. Privacy-embedded system should offer *end-to-end security*.
6. *Visibility* of measures taken and *transparency* on processes should be guaranteed.
7. Keep *users* in the centre of the development process.

Notwithstanding the intuitive appeal these guidelines may have, not many systems are developed today on the basis of these principles. A positive example however, is the design of a body scanner to be used at airports (Cavoukian 2011). In the case of body scanners both technological, business practice and physical measures are integrated to shield off private data as much as possible without negative consequences for the functionality of the system (detecting objects that might pose a threat in airplanes).

4.3 The future of privacy

Revocable privacy: resolving the tension between security and privacy
Security and privacy are seen as conflicting requirements (Cavoukian 2010). It is widely believed that they are a 'zero-sum' game (Schneier 2008): security cannot be achieved without sacrificing privacy, and vice-versa. This tension between security and privacy is felt in many areas of public policy making. Examples include camera surveillance, systems for road pricing, interconnecting national and international databases for law enforcement purposes, national ID-cards and their integration into national systems for identity management and e-government. Due to the high political importance given to homeland security, this has resulted in approaches to increase societal safety that disregard the privacy of the citizens. Similarly, when designing privacy enhancing technologies (PET), no attention is being paid to the quite reasonable request to also consider societal security issues.

This is an unfortunate state of affairs. In fact, it is our belief that in a democratic society the terms and conditions for using a public infrastructure are determined by society as a whole as part of the democratic decision making process, balancing several societal needs. PETs, as well as security mechanisms, for public infrastructures should be designed following these terms and conditions. One approach to reconcile security and privacy requirements can be found in using the concept of *revocable privacy*.

It is necessary to realise that legal or regulatory attempts to remedy the imbalance between security and privacy are inadequate by itself. Rules and regulations may change over time, allowing for more possibilities to gather information about people. Such 'function creep' occurs frequently, as we indicated earlier: once a system offers certain ways to collect data, sooner or later politicians, government officials or law enforcement will ask for an extension of powers. Therefore, the solution must be found in limiting possibilities at the outset, through technical means, in the architecture and design of the system. This makes it impossible to change the rules after the fact. This line of reasoning follows the idea that 'architecture is politics'[5] and 'code as code'[6] (Lessig 1999), and is inspired by the 'Select before you collect' principle (Jacobs 2005). To change the rules, the system has to be redesigned completely. Should such a redesign be performed, old data collected with the old system remains inaccessible.

In essence the idea of revocable privacy is to design systems in such a way that no personal information is available, unless a user violates the pre-established terms of service. A system implements revocable privacy if the architecture of the system guarantees that personal data is revealed only if a predefined rule has been violated. Examples of such rules are 'spending

[5] Attributed to Mitch Kapor, see http://blog.kapor.com/index9cd7.html?p=29
[6] 'Code (the executable code of a computer program) as code (norms, laws, i.e. the code of conduct)'.

digital money twice is illegal', or 'users should pay for services rendered' or 'you should not access data unless you have the right to do so'. Technical measures (comparable to the use of unlinkable pseudonyms, secret sharing or mixing networks as discussed earlier) are used to guarantee this.

EU developments

Ten years after 9/11 we can observe that homeland security has left its traces in the 'privacy landscape'. A recent communication of the European Commission identifies eighteen different information systems and approaches that have been developed or are under development for safeguarding European countries and citizens against terrorism, organised and serious crimes and illegal immigration. Examples of such systems are the Schengen Information System, the Visa Information System, EuroDAC (for collecting fingerprints), the Customs Information Services, and the Advanced Passenger Information system. Systems not yet in place but under development are a full-fledged Passenger Name Record system and an Entry-Exit system.[7] Co-operation and legislation is practised in a number of initiatives and directives. A relevant directive in this respect is the Data Retention directive we mentioned before that regulates the storage of traffic and location data. This directive serves as a test case since two European countries (Germany and Rumania) have declared the directive to run counter to their constitution.

The widespread introduction of information systems that serve to protect Europe against terrorism etc. has consequences for the privacy of European and non-European citizens. Function creep can be demonstrated to have occurred in the application of DNA profiles for solving serious crimes. Over time more detailed profiles could be exchanged and the use of these profiles was broadened from serious crime to much more mundane and ordinary crimes (Dahl & Saetnan 2009).

The European Commission and related parties such as the European Data Protection Supervisor and the Article 29 Working Party are discussing the follow-up of the Data Protection directive (95/46/EC) and the elaboration of recent communications and directives that regulate specific parts of the 'privacy landscape'. A new Data Protection directive should further harmonise data protection laws across member states, and should take into account new technological developments (internet of things, for instance) and new social developments as well (the emergence of social media) with the associated risks and problems. It also introduces an explicit 'right to be forgotten'. This development goes hand in hand with a revision of tasks and responsibilities of the national Data Protection Authorities. Within the Netherlands the revision of the Dutch DPA (Commissie Bescherming Persoonsgegevens) moves into the direction of a stronger supervisory role and less attention for awareness raising and information provision.

Fundamentally different approaches

Most legal and all technological protection for our privacy focuses on limiting the amount of personal information that is collected in the first place. This is a limited approach, and also one that is not very effective when people are willingly revealing very personal information on social networks (like Facebook), and seem generally quite eager to provide personal information for a small benefit (for example when applying for loyalty cards). Instead people like Hildebrandt and Jeroen van den Hoven argue for a harm based approach (in what Hildebrandt (2008) calls 'Ambient Law') that protects a person against unwarranted application of profiles one is not aware of, by requiring that people are treated equally despite obvious differences. The benefit of this approach is that it allows people to be more open and

[7] For a complete overview see COM (2010) 385 final

thus obtain the advantages of sharing information on the Internet (like when using social networks like Facebook), while having legal protection against abuse of this information. A drawback is that the users have to rely on government and businesses really not to abuse the data, and on enforcement agencies to enforce this.

Another radical different approach is presented by Bert Jaap Koops (2010). He promotes data maximization and dual transparency. Data maximization should offer all of us access to all available data, thereby creating a 'level playing field' that makes no distinction between parties. Dual transparency means that both the data subjects and the process of data collection and storage are fully transparent.

4.4 Conclusions

This chapter has explored the various aspects of privacy. Privacy bears strong relations with data protection (of personally identifiable information) but captures spatial and corporeal dimensions as well. It represents a social value that is safeguarded in the Dutch constitution and the European Charter for Fundamental Rights. In offering appropriate tools to safeguard privacy we have introduced privacy by design and privacy enhancing technologies. They present a starting point reconciling privacy requirements with requirements posed by homeland security. Though often positioned as a trade-off (more privacy means less security and the other way around) the alternatives presented show that privacy and security can be reconciled. This brings us to the following conclusions:

1. Privacy requires a multidisciplinary perspective: one should integrate technological, social and legal perspectives.
2. Through new information technologies much more opportunities to gather and use data emerge; this not only has an impact on (informational) privacy but it requires broadening the scope to spatial and corporeal dimensions as well (as these dimensions are currently not covered by data protection legislation).
3. Over the past decades new approaches to protecting privacy have emerged such as privacy enhancing technologies and privacy by design that reconcile seemingly opposing interests (such as privacy against homeland security). One example of how they can be reconciled is Revocable Privacy
4. More radical approaches to privacy exist, given todays' development. They adopt a different perspective to how privacy should or could be safeguarded such as a harm based approach, data maximisation instead of minimisation and dual transparency.

Resources

The following resources contain valuable information about privacy.

General websites and blogs

- Privacy Rights Clearinghouse: http://www.privacyrights.org/
- Chilling Effects Clearinghouse: http://chillingeffects.org/
- Dataloss database: http://datalossdb.org/

Civil liberties organisations

- Electronic Privacy Information Centre (EPIC): http://epic.org/
- Privacy International , UK: https://www.privacyinternational.org/
- Bits of Freedom (BoF), the Netherlands: http://www.bof.nl

Policy and legal institutes

- European Data Protection Supervisor (EPDS): http://www.edps.europa.eu/
- Article 29 Data Protection Working Party, Europe: http://ec.europa.eu/justice/policies/privacy/workinggroup/index_en.htm
- College Bescherming Persoonsgegevens (CBP), The Netherlands: http://www.cbpweb.nl

These resources, and many more, can be accessed through http://wiki.science.ru.nl/privacy as well.

Key concepts

Privacy (in the context of information systems); also called: Data Protection:
: The right to control the release of personal information about oneself, even when that data is already collected and stored by a third party.

Personal Identifiable Information (PII):
: Information that can be linked, with reasonable effort, to a natural person.

Privacy by design:
: The concept that privacy should be adopted as one of the *design parameters* of a system, already in the early stages of systems design

Anonymity:
: The state of being not identifiable within a set of subjects.

Privacy Enhancing Technologies (PET)
: Technical measures to protect privacy.

Function creep:
: The notion that, over time, the functionality of a system may change and grow, encompassing functions which are different from the original purposes of the system

Revocable privacy
: The method to design systems in such a way that no personal information is available, unless a user violates the pre-established terms of service.

Literature

Article 29 WP 'Opinion 2/2010 on online behavioural advertising', June 22, 2010. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_en.pdf

Beck, U. (1992). Risk Society: Towards a New Modernity. London: Sage.

Cavoukian A. (2010). Privacy by design – the 7 foundational principles. Available at http://www.ipc.on.ca/images/Resources/7foundationalprinciples.

Cavoukian A. (2011). Whole body imaging in airport scanners – building in privacy by design. http://www.ipc.on.ca/images/Resources/wholebodyimaging.pdf [

Communication from the Commission to the European Parliament and the Council. 'Overview of information management in the area of freedom, security and justice'. COM(2010)385 final

Dahl and Sætnan (2009) 'It all happened so slowly – On controlling function creep in forensic DNA databases. *International Journal of Law, Crime and Justice* 37 (3), 83-103

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

Directive 2002/58/EC of the European Parliament and of the Council 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)

Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws

ENISA Ad Hoc Working Group on Privacy & Technology (2008). Technology-induced challenges in privacy & data protection in Europe.

Freid, C. (1968). Privacy. *Yale Law Journal* 77 (3), 475–493.

Giddens, A. (1990). The consequences of modernity. Cambirdge: Polity Press

Hildebrandt, M. (2008). A Vision of Ambient Law *Regulating Technologies*. Ed. Roger Brownsword and Karin Yeung. Oxford: Hart, 175-191. Available at: http://works.bepress.com/mireille_hildebrandt/4

Jacobs, B. (2005). Select before you collect. *Ars Aequi* 54, 1006–1009.

Koops, B.J. (2010), 'Het failliet van het grondrecht op dataprotectie', in: *J.E.J. Prins e.a. (red.), 16 Miljoen BN'ers? Bescherming van Persoonsgegevens in het Digitale Tijdperk*, Leiden: Stichting NJCM-Boekerij, 99-110.

Lessig, L. (1999). Code and other laws of cyberspace. Basic Books.

Lieshout M van, Kool L, Jonge M de, Schoonhoven B van (2011). 'Privacy by Design: an alternative to existing practice in safeguarding privacy'. *INFO, The Journal of policy, regulation and strategy for telecommunications, information and media*. Vol. 13, Nr. 6, pp. 55-68.

Pfitzmann, A., & Hansen, M. (2010) Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management – a consolidated proposal for terminology. http://dud.inf.tu-dresden.de/Anon_Terminology.shtml.

OECD Guidelines on the protection of privacy and the transborder flows of personal data (2011). http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html (visited 29 January 2011).

Schneier, B. (2008) What our top spy doesn't get: Security and privacy aren't opposites. *Wired*

Solove, D. J. (2010). Understanding privacy, Harvard University Press.

Solove, D. J. (2007). 'I've got nothing to hide' and other misunderstandings of privacy. *San Diego Law Review*, 44, 745–772.

Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. The implicit made explicit. *Harvard Law Review* IV (5), 193–220.

Westin, A. (1967). Privacy and Freedom, Atheneum, New York.

Zureik, E. & L. Harling Stalker (2010). The cross-cultural study of privacy. In *Zureik, E. et al (eds). Surveillance, privacy and the globalization of personal information*. McGill-Queen University Press, Montreal/London/Ithaca, 10.

Warren, S. & Brandeis, L. (1890). The right to privacy. *Harvard Law review*.