Information privacy, the right to receive information and (mobile) ICTs

Litska Strikwerda

The first part of this paper is about the notion of (information) privacy and its grounding in law. It discusses the tension between the right to privacy and the right to receive information. The second part of this paper explores how (mobile) ICTs challenge and complicate privacy claims and satisfy the right to receive information.

Keywords: information privacy, right to receive information, ontological friction, dialectical process, (mobile) ICTs

Introduction

On 12 May 2010 a plane crash in Libya killed more than one hundred people. Seventy of them were Dutch. The sole survivor was a nine-year-old Dutch boy. The next day Dutch newspapers published pictures of victims as well as their names, ages and addresses. Journalists had found this personal information on the victims' social networking sites.

The press performs an important task in society: it imparts information to individual citizens (ECtHR, 21 December 2004, Busuioc v. Moldova, Appl. No. 61 513/00, § 56). The above-mentioned example raises the question, however, as to how many details about other citizens individuals are entitled to know.

The goal of this paper is to examine what information about individuals should be made public by the press and what information should remain private. As the example illustrates, the use of Information and Communication Technologies (ICTs) provides access to a large pool of personal information about individuals. Therefore, I will also explore how ICTs challenge and complicate the answer to the question raised.

The example at stake is about a static point of access to the Internet: both the journalists who found the personal information and the individual citizens who provided it probably used an ordinary desktop computer or maybe a laptop. As the following example will illustrate, mobile devices might further challenge and complicate the answer to the question regarding what information about individuals should be made public and what information should remain private.

In August 2009 the Dutch dance festival Sunset Grooves ended in a riot. When a group of people turned against the police, police officers panicked and fired shots. A 19-year-old visitor of the festival was killed and six people were wounded. Using mobile phones with a camera and Internet access, people present at the festival almost immediately posted videos and pictures of the riot on YouTube. These pictures and videos not only appeared in newspapers and on news programs on television, but also in court, where they were used as evidence to convict the hooligans who attacked the police (see for instance Rechtbank Rotterdam, 19 February 2010, LJN: BL4554).

In the next section I will begin the discussion with a definition of (the right to) privacy and explain why information about people constitutes an important aspect in this regard. I will then argue that an individual citizen's claim for privacy must always be weighed against the wishes of other citizens to receive information, which also constitutes a right. Next, I will determine whether or not there is an equilibrium between information privacy and the right to receive information by identifying a «principle of proportionality.» This will be followed by a discussion on why (mobile) ICTs challenge and complicate information privacy claims and also satisfy the right to receive information. Finally, I will present the conclusion that (mobile) ICTs increase the amount of information available (thereby decreasing the level of information privacy and satisfying the right to receive information), but that they do not change the equilibrium between information privacy and the right to receive information that is determined by the proportionality principle.

Privacy: definitions and general remarks

According to Article 8 of the European Convention on Human Rights (ECHR) «everyone has the right to respect for his private [...] life.» This human right can also be found in, for instance, the UN Universal Declaration of Human Rights (Article 12) and the UN International Covenant on Civil and Political Rights (Article 17). It is not entirely clear, however, what is meant by «private life.» The European Court of Human Rights (ECtHR) is of the opinion that «the concept of 'private life' is a broad term not susceptible to exhaustive definition» (ECtHR, 29 April 2002, Pretty v United Kingdom, Appl. No. 2346/02, § 61).

As the EU Directive on privacy and electronic communications (2002/58/EC) points out, the development of new ICTs has emphasized one specific aspect of the right to respect for private life: the protection of personal data. This aspect of the right to respect for private life is called «information privacy» and will be the focus of this paper.

In the 1960s the American lawyer Alan F. Westin was the first to give a definition of information privacy. In his book *Privacy and freedom* (1967) Westin defines information privacy as «the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others» (Westin 1967: 7).

Information privacy is a key aspect of the right to respect for private life because information about us is part of our identity (ECtHR, 29 April 2002, Pretty v United Kingdom, Appl. No. 2346/02, § 61). As Floridi (2005: 195) explains:

> «My» in «my information» is not the same as «my» in «my car» but rather the same as in «my body» or «my feelings»: it expresses a sense of constitutive *belonging*, not of external *ownership*, a sense in which my body, my feelings and my information are part of me but are not my (legal) possessions.

In sum, information about us is part of our nature or being (ontology): «we are our information.» Therefore, Floridi argues for an «ontological interpretation» of information privacy (Floridi 2005: 185). He claims personal data should not be seen as arbitrary labels about a given person, but rather as constitutive traits of that person (Floridi 2005: 198).

The desire for (information) privacy: a dialectical process

According to the American anthropologist Robert F. Murphy (1964: 1257) the desire for privacy, common to us all, can be seen as a *dialectical process* (in a Hegelian sense, i.e., a process of initial contradiction that leads to a greater synthesis). On the one hand, «an area of privacy […] is maintained by all, and reserve and restraint are common, though not constant, factors in all social relationships» (Murphy 1964: 1257). Following the German philosopher and sociologist Georg Simmel, Murphy (1964: 1257) claims that «society could not perdure if people knew too much of one another.» On the other hand, people have to release information about themselves, at least to some extent, in order to be able to participate in society: «if social interaction is to be made possible, a public life must be at one and the same time a private life» (Murphy 1964: 1258). Therefore, Murphy (1964: 1260) views social distance as «a pervasive factor in human relationships and the necessary corollary of association.»

The desire for information privacy, as a specific aspect of privacy, can be seen as a dialectical process too, if interpreted ontologically. Westin (1967: 7) considers:

> […] each individual is continually engaged in a personal adjustment process in which he balances the desire for privacy with the disclosure and communication of himself to others, in the light of the environmental conditions and social norms set by the society in which he lives. The individual does so in the face of pressures from the curiosity of others and from the processes of surveillance that every society sets in order to enforce its social norms.

Westin (1967: 19) explains that a propensity for curiosity lies in each individual. In modern society, people's curiosity is (partly) satisfied by the press through radio, newspapers, television, magazines, etc. (Westin 1967: 55).

The dialectical process described by Murphy and Westin can be recognized in law as well. Not only the claim for information privacy that is an aspect of the right to respect for private life, but also people's curiosity constitutes a human right. According to the ECHR (Article 10 § 1), the right to freedom of expression includes the freedom «to receive and impart information and ideas.»

As the ECtHR has explained in the *Guerra* case «the public has a right to receive information as a corollary of the specific function of journalists, which is to impart information and ideas on matters of public interest» (ECtHR, 19 February 1998, Guerra and others v. Italy, Appl. No. 14 967/89, § 53). In conclusion, the right to receive information has a rather passive nature: it entitles an undefined public, presumably individual citizens, «to receive information and ideas on matters of public interest that the media choose to impart» (Helberger 2006: § 2).

In principle, Article 10 § 1 ECHR allows no state interference with the choice of journalists regarding what information or ideas they wish to impart. However, journalists must not overstep the boundaries set in Article 10 § 2 ECHR.

According to Article 10 § 2 ECHR the freedom of the press can be restricted if is «necessary in a democratic society» for, among other things, «the protection of the reputation or the rights of others» or «for preventing the disclosure of information received in confidence.» Both grounds for restriction are elements of the right to respect for private life (Van Dijk et al. 2006: 665).

Within the «necessary in a democratic society» test, the ECHR relies on the principle of «proportionality» (Van Dijk et al. 2006: 747). The proportionality principle entails that the extent of the restriction must be in keeping with the aim pursued.

In sum, the right to respect the private life of a given person, which protects among other things his or her reputation and confidential informa-

tion, might give rise to a restriction of the freedom of the press. This means that the right to receive information from individual citizens, as a corollary of the freedom of the press, must always be weighed against the right of information privacy, which is an aspect of the right to respect the private life of other citizens.

Yet the question arises: Under what circumstances is it *proportional* to restrict the right to receive information about individual citizens in order to protect the information privacy of other citizens? Answering this question will be the aim of the next section.

The right to receive information and information privacy: an equilibrium

Following Floridi, an «equilibrium» between the right to receive information and information privacy can be found by identifying «a common, lowest threshold of *ontological friction* below which human life becomes increasingly unpleasant and ultimately unbearable» (Floridi 2005: 191, emphasis added, LS). In short, ontological friction is about how difficult or easy it is to access information, including information about others. The lower the level of ontological friction, the easier it is to access information, and vice versa. Therefore, low levels of ontological friction lead to a low level of information privacy and high levels of ontological friction lead to a high of level information privacy (Floridi 2005: 187).

Ideally, we all want to reap the benefits from a low level of ontological friction (a lot of information, including information about others) and a high level of information privacy (little information about ourselves). However, the combination of both is impossible (Floridi 2005: 197).

In balancing between the right to receive information and the right to information privacy the ECtHR has adopted the criterion of «public interest.» In the *Busuioc* case the ECtHR states:

> Whilst the press must not overstep the bounds set, inter alia, in the interest of «the protection of the reputation or rights of others,» it is nevertheless incumbent on it to impart information and ideas of *public interest*. (ECtHR, 21 December 2004, Busuioc v. Moldova, Appl. No. 61 513/00, § 56, emphasis added, LS)

In sum, the ECtHR uses the criterion of public interest to determine whether a restriction of the right to receive information from individual citizens in order to protect the information privacy of (an)other citizen(s) is proportional.

In the *Fressoz and Roire* case the ECtHR ruled, for instance, that it was not proportional to interfere with the right to receive information from the public in order to protect the information privacy of the company chairman

of the Peugeot factory, whose (confidential) tax assessments had been published by journalists in an article. The article was published during an industrial dispute, which was widely reported in the press. The factory workers were seeking a pay rise, which the management was refusing. The article showed that the company chairman had received large pay increases, while at the same time opposing his employees' claims for a raise. The ECtHR was of the opinion that «by making such a comparison against that background, the article contributed to a public debate on a matter of general interest» (ECtHR, 21 January 1999, Fressoz and Roire v. France, Appl. No. 29 183/95, § 50, 53).

The question arises: What sort of information is in general of «public interest»? Following Westin (1967: 55), not only information about «public figures» who have chosen a life in the spotlights, such as politicians or actors, can be of public interest, but also information about «anyone who happens to be touched by a 'public event'.» So, *subjects* of public interest are either public figures or ordinary citizens who have experienced something special.

It is not easy, however, to determine what is the *object* of public interest and what is not. According to Ingram and Henshall (2008: Ch. 62), who have written a practical guide for journalists, «there is a dividing line between those things which the public has a right to know and those which individuals have a right to keep private, no matter how interesting they might be to other people.» They provide the following example:

> If a public figure's strange behaviour in the privacy of his own home has no possible effect on his public role, the media cannot claim they have a duty to report it. (Ingram & Henshall 2008: Ch. 62)

So, there is no public interest in information about a public figure if there is no connection with his or her public role. Analogously, one could say there is no public interest in information about an individual «touched by a public event» if there is no connection with that event. For example, if a bus driver causes an accident with many casualties (a «public event») there is no need for the public to know his or her sexual orientation. If the accident was caused by drunk driving, there might be a public interest in knowing that he or she is an alcoholic.

In conclusion, it is proportional to restrict the right to receive information from individual citizens in order to protect the information privacy of another citizen if the information is not of public interest. Information is of public interest if it is about a *subject* of public interest (a public figure or an individual touched by a public event) and an *object* of public interest (this means there is a connection between the public role of the subject of public interest or the public event the subject is touched by, and the information).

(Mobile) ICTs, a challenge and complication to information privacy

ICTs are «fundamentally challenging and complicating» information privacy (Sullins 2010: 130). Firstly, ICTs decrease the level of ontological friction (and thus the level of information privacy). Secondly, the social use of ICTs seems to change the dialectical process in which the desire for (information) privacy is weighed against the desire to participate in society.

ICTs decrease the level of ontological friction (and thus the level of information privacy)

ICTs decrease the level of ontological friction (and thus the level of information privacy), because their usage provides more (in amount and detail) information about individuals. Floridi (2005: 186) states:

> According to one of the most widely accepted explanations, digital ICTs exacerbate old problems concerning information privacy because of the dramatic increase in their data *Processing* capacities, in the speed (or *Pace*) at which they can process data, and in the *Quantity* and *Quality* of data that they can collect, record and manage. This can be referred to as the 2P2Q hypothesis.

The 2P2Q hypothesis can be further explained as follows. ICTs have large capacities and possibilities for *processing* personal data (EU Directive 2002/58/EC, preamble, § 5). In addition to an increase in the amount of data and the speed (*Pace*) at which they can process, ICTs provide for data that contain more comprehensive information about their users and their actions (Van Est, Hafskjold & Sandsgaard 2006: 45). From the increased *quantity* and *quality* of data gathered by ICTs, new methods of data analysis and data mining are emerging (Van Est, Hafskjold & Sandsgaard 2006: 45).

I would like to add that ICTs do not only increase the *availability* of information, but also the *accessibility*. Whereas in the past many people had to share one computer to find information, in the library for instance, today it is not unusual for one person to have (access to) many computers. In my case, I have access to a desktop computer at home and at work, a laptop, and an advanced mobile phone. And computing access has not only become more common, it has also become more flexible. Computing access is possible everywhere: at home, at work, on the train, in the pub, etc. This phenomenon is called «ubiquitous computing» (Weiser 1993).

The level of ontological friction (and thus information privacy) could be increased if the amount of information available through ICTs were to be regulated by *law* or by individuals *themselves*, dependent on the type of information at stake. As I see it, ICTs provide for roughly two types of information creation that are a threat to information privacy: information that is

automatically processed and stored and information that is made available by individuals themselves. The amount of information that is automatically processed and stored by ICTs can be regulated by law; the amount of information made available by individuals can be regulated by the individuals themselves.

Information that is automatically processed and stored by ICTs includes traffic and location data. Traffic data are processed for the purpose of the conveyance and billing of a communication on an electronic communications network and can consist of «data referring to the routing, duration, time or volume of a communication» (EU Directive 2002/58/EC, Article 2 (b), preamble § 15). Location data are «processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user» (EU Directive 2002/58/EC, Article 2 (c)).

The EU has established a Directive on privacy and electronic communications (2002/58/EC) to «ensure […] protection of […] the right to privacy, with respect to the processing of personal data in the electronic communication sector» (Article 1). It holds, for instance, that «specific legal, regulatory and technical provisions» should be made in order to protect the right to privacy «in particular with regard to the increasing capacity for automated storage and processing of data» (Preamble § 7, Articles 6 and 9).

It should be added, however, that the EU's Directive on privacy and electronic communications has been amended by EU Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks. This Directive holds, for instance, that «given the importance of traffic and location data for the investigation, detection, and prosecution of criminal offences […] there is a need to ensure […] that data that are generated or processed [...] are retained for a certain period» (preamble § 11, Article 3). So, although law can regulate the amount of information that is automatically processed and stored by ICTs, it seems to give priority to another interest (the prosecution of crimes) instead of information privacy.

Information that is made available by individuals can, for instance, consist of pictures, personal reflections on everyday life on weblogs and personal websites, or videos on YouTube (Van Est, Hafskjold & Sandsgaard 2006: 45). Facebook's latest enhancement also enables individuals to provide location data. Using a GPS- equipped phone, travelling Facebook users can «check in» at the nearest landmark. This location information appears as a status update (Morgan 2010).

People can decide for themselves what information they put online. They can, for instance, choose which pictures they want to publish on their personal website or which videos they want to post on YouTube.

And as Floridi (2005: 186) points out, ICTs do not only threaten people's information privacy, but also offer them new possibilities to protect their information privacy. One can think here of technologies that enable us to encrypt, firewall or protect information with passwords or a PIN code (Floridi 2005: 186).

However, there is «no indication that privacy threatening and privacy enhancing capabilities are being balanced in an automatic manner» (Cas 2006: 16). It is probably for this reason, therefore, that the EU Directive on privacy and electronic communications (2002/58/EC) holds that «service providers who offer publicly available electronic communications services over the Internet should inform users and subscribers of measures they can take to protect the security of their communications for instance by using specific types of software or encryption technologies» (Preamble § 20, Article 4 (2)).

In sum, ICTs decrease the level of ontological friction (and thus the level of information privacy) because they provide for more available and accessible information about individuals. This information is automatically processed and stored by ICTs or created by individuals themselves and can be regulated by law and individuals themselves respectively. However, the law seems to give priority to another interest (the prosecution of crime) instead of information privacy and individuals do not seem to balance privacy threatening and privacy enhancing capabilities of ICTs.

I think individuals do not balance privacy threatening and privacy enhancing capabilities of ICTs in a way we would expect them to because the social use of ICTs seems to change the dialectical process in which the desire for (information) privacy is weighed against the desire to participate in society. Explaining this assumption will be the aim of the next section.

The social use of ICTs seems to change the dialectical process in which the desire for (information) privacy is weighed against the desire to participate in society

The social use of ICTs seems to change the dialectical process in which the desire for (information) privacy is balanced against the desire to participate in society. ICTs seem to have brought about a reconceptualization of the private and public sphere (Brey 2010: 52).

More and more social interactions are mediated by ICTs (Van Est, Hafskjold & Sandsgaard 2006: 44). Think here, for instance, of MSN, Twitter and social networking sites. They seem to «change social interaction and even our sense of privacy» (Van Est, Hafskjold & Sandsgaard 2006: 44). Sullins (2010: 131) states:

> It would seem that younger generations do not care that much about privacy rights, given their complete lack of propriety on social networking sites like MySpace and

Facebook. People are quite willing to give away the most intimate facts about themselves to millions of potential viewers.

It is difficult to discover why people are willing to reveal intimate facts about themselves. The relationship between social interaction, ICT and privacy is a highly complex one (Van Est, Hafskjold & Sandsgaard 2006: 44). In short, there seems to be a lack of awareness among (young) people of the importance of (information) privacy.

We used to decide on a case-to-case basis which information we wanted to share with other people. However, «our previous experiences cannot necessarily be 'translated' directly into the digital world, because ICT poses different possibilities and boundaries» (Van Est, Hafskjold & Sandsgaard 2006: 48). Information published on a social networking site or weblog is «potentially accessible to anyone, for an indefinite time» (Van Est, Hafskjold & Sandsgaard 2006: 48).

People do not always seem to realize that. This is probably due to «the discrepancy and contradiction between the subjective impression of the user and the objective reality» of the Internet (Cas 2006: 20). Sitting in front of a monitor in a separated space gives the impression of a high degree of anonymity (Cas 2006: 20). In reality, «being online is one of the less private things in life» (Floridi 2005: 192).

But awareness is rising, especially since it became known that job applicants are usually scanned on the Internet for information on personal interests and attitudes (Cas 2006: 19). Recently, a Web 2.0 suicide machine was established that allows a person to delete all of their social-networking profiles and thereby completely does away with their Web 2.0 alter ego (http://suicidemachine.org). It also removes tweets. The popularity of the Web 2.0 suicide machine seems to reflect this awareness: within half a year of its launch 1,176,563 friends had been «unfriended» and 504,978 tweets had been removed (http://suicidemachine.org).

However, «as an analogy with the 'digital divide', there appears to be a privacy divide: those who know and act accordingly, and those who don't and remain vulnerable» (Van Est, Hafskjold & Sandsgaard 2006: 47). Awareness-raising campaigns might help to increase the knowledge of those who need it.

In sum, the amount of information available through ICTs is only regulated by individuals to a limited extent, due to a lack of awareness among (young) people of the importance of (information) privacy. But because awareness is rising, I expect individuals to decrease their «information flow» in the future.

Do ICTs satisfy the right to receive information?

Since (mobile) ICTs decrease the level of ontological friction, in principle they satisfy the right to receive information simply because there is more information that can be received. However, two reservations need to be made here. Firstly, the traffic and location data that the law allows ICTs to process and store automatically are not accessible for individual citizens, only for authorities that need them in order to fight crime (EU Directive 2006/24/EC, Article 4). Secondly, the fact that individuals themselves make information available through ICTs does not automatically mean others have the right to receive that information *through the press*: the proportionality principle applies (ECtHR, 6 February 2001, Tammer v. Estonia, Appl. No. 41 205/98, § 6566).

So, as the following examples will illustrate, journalists can make use of information about individuals that they have made publicly available through ICTs only if it is in the public interest. Using mobile phones with Internet access, Dutch politicians recently started to «twitter» during debates in Parliament. If a politician (a subject of public interest) for instance «twitters» his or her opinion on tax plans that have just been revealed (an object of public interest, because the information is connected to his or her public role), it would not be proportional to restrict the right to receive information from individual citizens and a journalist would be free to publish this tweet. But if the same politician «twitters» from home on the illness of his or her child (which is not an object of public interest, because the information is not connected to his or her public role) it would be proportional to restrict the right to receive information from individual citizens in order to protect the information privacy of the politician and a journalist should not publish such a tweet.

And if an individual touched by a public event (a subject of public interest) provides for information about that public event (an object of public interest), it would not be proportional to restrict the right to receive information from individual citizens and a journalist would be free to publish this information. One could think here of the videos of the dance festival riot, mentioned in the introduction, which were posted on YouTube by people who were present at the festival. But it is proportional to restrict the right to receive information from individual citizens in order to protect the information privacy of the person touched by a public event with regard to information that has no connection with the public event at all. Here, one can think of the other example given in the introduction: the full names, addresses or holiday pictures of the victims of the plane crash had no connection with that plane crash and a journalist would therefore not be at liberty to publish this kind of information.

It should be added here, however, that the press has a wider margin of appreciation with regard to a public figure than with regard to an individual

touched by a public event (ECtHR, 8 July 1986, Lingens v. Austria, Appl. No. 9815/82, § 42). The ECtHR explains: «unlike the latter, the former inevitably and knowingly lays himself open to close scrutiny of his every word and deed by both journalists and the public at large, and he must consequently display a greater degree of tolerance» (ECtHR, 8 July 1986, Lingens v. Austria, Appl. No. 9815/82, § 42). In sum, public figures who «live a life in the spotlights» are expected to be more discreet than individuals touched by a public event, and who probably never thought the spotlights would ever shine on them.

In conclusion, (mobile) ICTs satisfy the right to receive information because they provide for more information than can be received. But they do not change the equilibrium between information privacy and the right to receive information that is reached by the proportionality principle, if the information is received through the press.

Conclusion

Following Westin, I have defined information privacy as «the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.» This claim constitutes an important part of the right to respect for private life, as codified in, for example, Article 8 of the ECHR, because information about people constitutes part of their identity.

The desire for information privacy can be seen as a dialectical process: it is always balanced against the desire to participate in society. In law we see that the right to information privacy is balanced against the right to receive information, which is part of the right to freedom of expression (Article 10, ECHR).

I have found an «equilibrium» between the right to receive information and information privacy by identifying a principle of proportionality. It is proportional to restrict the right to receive information from individual citizens in order to protect the information privacy of another citizen if the information is not of public interest. Information is of public interest if it is about a *subject* of public interest (a public figure or an individual touched by a public event) and an *object* of public interest (this means there is a connection between the public role of the subject of the information, or the public event the subject is touched by, and the information).

(Mobile) ICTs challenge and complicate claims for information privacy because they provide access to more available and accessible information about individuals due to their technical features and social use. But I think they do not change the equilibrium I found between the right to receive information and information privacy.

In conclusion, (mobile) ICTs increase the amount of information available and accessible (thereby decreasing the level of information privacy and satisfying the right to receive information), but they do not change the equilibrium between information privacy and the right to receive information that is reached by the proportionality principle. We only have the right to receive information about others through the press if the information concerned is of public interest.

Literature

Brey, P. (2010) Values in technology and disclosive computer ethics. In *The Cambridge handbook of information and computer ethics*, ed. L. Floridi, pp. 41–58. Cambridge: Cambridge University Press.

Cas, J. (2006) Technologies that affect privacy. In *ICT and privacy in Europe / Experiences from technology assessment of ICT and privacy in seven different European countries*, European Parliamentary Technology Assessment (EPTA), pp. 16–22. Retrieved 14 October 2010 from http://www.tekno.dk/EPTA

Floridi, L. (2005) The ontological interpretation of informational privacy. *Ethics and Information Technology*, 7, pp. 185–200.

Helberger, N. (2006) The «right to information» and digital broadcasting: About monsters, invisible men and the future of European broadcasting regulation. *Entertainment Law Review*, 2, pp. 70–80. Retrieved 14 October 2010 from http://www.ivir.nl/publications

Ingram, D. & Henshall, P. (2008) *The news manual, Volume 3: Ethics and the law*. Retrieved 14 October 2010 from http://www.thenewsmanual.net

Morgan, G. (2010) *Facebook checks in to location services*. Retrieved 14 October 2010 from http://www.newscientist.com/blogs/shortsharpscience/2010/08/facebook-checks-in-to-location.html

Murphy, R.F. (1964) Social distance and the veil. *American Anthropologist*, 66, pp. 1257–1273.

Sullins, J. (2010) Rights and computer ethics. In *The Cambridge handbook of information and computer ethics*, ed. L. Floridi, pp. 116–132. Cambridge: Cambridge University Press.

Van Dijk, P., Van Hoof, F., Van Rijn, A. & Zwaak, L. (Eds.) (2006) *Theory and practice of the European convention on human rights*. Antwerpen: Intersentia.

Van Est, R., Hafskjold, C. & Sandsgaard, J. (2006) Societal interaction. In *ICT and privacy in Europe / Experiences from technology assessment of ICT and privacy in seven different European countries*, European Parliamentary Technology Assessment (EPTA), pp. 16–22. Retrieved 14 October 2010 from http://www.tekno.dk/EPTA

Weiser, M. (1993) *Ubiquitous computing*. Retrieved 14 October 2010 from http://www.ubiq.com/weiser

Westin, A.F. (1967) *Privacy and freedom*. London: The Bodley Head.

Table of cases

ECtHR, 8 July 1986, Lingens v. Austria, Appl. No. 9815/82. Retrieved 14 October 2010 from http://www.echr.coe.int/echr

ECtHR, 19 February 1998, Guerra and others v. Italy, Appl. No. 14 967/89. Retrieved 14 October 2010 from http://www.echr.coe.int/echr

ECtHR, 21 January 1999, Fressoz and Roire v. France, Appl. No. 29 183/95. Retrieved 14 October 2010 from http://www.echr.coe.int/echr

ECtHR, 6 February 2001, Tammer v. Estonia, Appl. No. 41 205/98. Retrieved 14 October 2010 from http://www.echr.coe.int/echr

ECtHR, 29 April 2002, Pretty v United Kingdom, Appl. No. 2346/02. Retrieved 14 October 2010 from http://www.echr.coe.int/echr

ECtHR, 21 December 2004, Busuioc v. Moldova, Appl. No. 61 513/00. Retrieved 14 October 2010 from http://www.echr.coe.int/echr

Rechtbank Rotterdam, 19 February 2010, LJN: BL4554. Retrieved 14 October 2010 from http://www.rechtspraak.nl

Table of legal documents

EU, Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC. Retrieved 14 October 2010 from http://eur-lex.europa.eu

EU, 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). Retrieved 14 October 2010 from http://eur-lex.europa.eu