Improving privacy protection in the area of behavioural targeting

Zuiderveen Borgesius, F.J.

Publication date
2014
Document Version
Final published version

3 Privacy

What are the privacy implications of behavioural targeting? To answer this question, this chapter distinguishes three perspectives on privacy in section 3.1: privacy as limited access, privacy as control over personal information, and privacy as the freedom from unreasonable constraints on identity construction. The three perspectives highlight different concerns during the behavioural targeting process.[340]

Section 3.2 discusses the right to privacy in European law, and the privacy case law of the European Court of Human Rights. The European Court of Human Rights interprets the right to privacy generously, and refuses to define the scope of protection. Section 3.3 discusses three privacy concerns regarding behavioural targeting. First: chilling effects relating to massive data collection on user behaviour. Second: the lack of individual control over personal information. Third: social sorting and the risk of manipulation. Section 3.4 concludes.

3.1 Three privacy perspectives

Many people have no trouble thinking of an example of a privacy violation.[341] Countless civil rights organisations aim to defend privacy, and judges have to apply the concept.[342] But after more than a century of attempts by scholars from various

---

[340] As noted, this study uses "privacy", and "private life" interchangeably. Article 7 of the EU Charter of Fundemantal Rights and article 8 of the European Convention on Human Rights use the phrase "respect for private and family life". See in detail on the difference between "private life" and "privacy" González Fuster 2014, p. 82-84; p. 255. This study also uses "fundamental rights" and "human rights" interchangeably (see on these terms González Fuster 2014, p. 164-166).
[341] See Nippert-Eng 2010.
[342] See Bennet 2008 for an overview.

disciplines, it has been impossible to agree on a definition. Privacy has been called "elusive and ill-defined",[343] "a concept in disarray",[344] and a "messy, complicated, and rather vague concept."[345] Looking for a privacy definition in literature "we find chaos",[346] "nobody seems to have any very clear idea what the right to privacy is",[347] and "even its pronunciation is uncertain."[348]

As noted, in this study three privacy perspectives are distinguished: privacy as limited access, privacy as control over personal information, and privacy as the freedom from unreasonable constraints on identity construction.[349] The classification is based on work by Gürses, who discusses three privacy research paradigms in the field of software engineering.[350]

The classification helps to structure discussions about privacy. However, there are no clear borders between the three privacy perspectives, which overlap in different ways. Furthermore, none of the three privacy perspectives is meant as absolute. Privacy as limited access doesn't suggest that people want to be completely alone. Privacy as control doesn't suggest that people should have full control over data concerning them. And privacy as the freedom from unreasonable constraints on identity construction doesn't suggest that people should be allowed to lie to everyone to improve their image.

---

[343] Posner 1978, p. 393.
[344] Solove 2009, p. 1.
[345] Boyd 2011, p. 497.
[346] Inness 1996, p. 3.
[347] Thomson 1975, p. 312.
[348] Marshall 1975, p. 242.
[349] Many other classifications are possible. For instance, Solove distinguishes 6 perspectives (Solove 2002), and Rössler distinguishes three perspectives (Rössler 2005, p. 6). Another possible distinction is that between relational and informational privacy (see e.g. Dommering & Asscher 2000; Kabel 2003).
[350] Gürses uses a slightly different terminology and distinguishes (i) "privacy as confidentiality: hiding", (ii) "privacy as control: informational self-determination", and (iii) "privacy as practice: identity construction" (Gürses 2010, p. 24-32) See for a similar taxonomy Berendt 2012.

Privacy as limited access

In the late 19th century, the invention of the snap camera by Kodak enabled people to create photos on the spot. Until then, people needed to be still for a picture, so people had to cooperate when a picture was taken of them. But the new cameras made it possible for the paparazzi to take photos of people without being noticed.[351] In 1890 this led two US authors, Warren & Brandeis, to write an influential article: "The right to privacy."[352]

> Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual what Judge Cooley calls the right "to be let alone." Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that "what is whispered in the closet shall be proclaimed from the house-tops."[353]

Warren & Brandeis argued for legal protection of privacy, to safeguard "the right to be let alone."[354] They suggested that the common law implicitly recognised a right to privacy already, citing precedents on, for example, breach of confidence, copyright, and defamation. Ever since, scholars, judges, and lawmakers have tried to adapt the concept of privacy to cope with new developments and new technologies.[355]

This study categorises Warren & Brandeis in the group of the first privacy perspective: privacy as limited access to the private sphere. The privacy as limited

---

[351] Solove 2009, p. 15.
[352] Warren & Brandeis 1890.
[353] Warren & Brandeis 1890, p. 195, internal footnote omitted.
[354] Warren & Brandeis don't actually define privacy as the right to be let alone (see Gavison 1980, p. 437).
[355] See e.g. ECtHR, Von Hannover v. Germany, No. 59320/00, 24 September 2004, par. 74. See also Gassman & Pipe 1974, p. 12.

access perspective is categorised together with privacy as secrecy,[356] confidentiality,[357] solitude,[358] seclusion,[359] and as a right not to be annoyed.[360] Privacy as limited access emphasises the freedom from interference by the state or others. Privacy as limited access is about a personal sphere, where people can remain out of sight and in peace. Gavison describes the limited access perspective well.

> Our interest in privacy (…) is related to our concern over our accessibility to others: the extent to which we are known to others, the extent to which others have physical access to us, and the extent to which we are the subject of others' attention.[361]

Roughly, two categories within privacy as limited access can be distinguished.[362] First: privacy as confidentiality. When others access information that a person wishes to keep for him- or herself, there's a privacy interference. Second, privacy interferences can occur when people are disturbed, or interrupted, for instance by telemarketers. Varian speaks of privacy as a "right not to be annoyed."[363]

Privacy as limited access aptly describes many privacy infringements. Seeing privacy as limited access implies that too much access to one's private sphere interferes with privacy. A classic example is privacy violations by paparazzi that intrude on private affairs. Section 3.3 discusses how tracking people's activities for behavioural targeting can interfere with privacy as limited access.

---

[356] Posner 1978. See Solove 2002, p. 1105.
[357] Gürses 2010, p. 24.
[358] Westin 1970, p. 31.
[359] American Law Institute 1977.
[360] Varian, p. 102.
[361] Gavison 1980, p. 423.
[362] Posner 1981, p. 31, note 7. See also Solove 2009, p. 21-24.
[363] Varian 2009, p. 102. The European Court of Human Rights says that receiving unwanted or offensive spam amounted to an interference with a person's right to respect for his private life. But the Court didn't find that Italy should have done more to comply with its positive obligations (ECtHR, Muscio v. Italy, No. 31358/03, 13 November 2007 (inadmissible)).

While too much access to a person fittingly describes many privacy violations, the perspective also has weaknesses. In some ways, the privacy as limited access perspective is too narrow. For example, people often want to disclose information about themselves to others, but still have expectations of privacy. Disclosing personal information is an important part of building relationships, and of functioning in society.[364] Hence, the social dimension of privacy seems to receive insufficient attention under the privacy as limited access perspective. And sometimes people want to disclose information to firms to receive personalised service. Solove notes that privacy as secrecy is problematic as well, as many situations that people would describe as a privacy infringement don't concern information that is secret.[365] Private matters such as a person's debts can hardly be described as a secret.[366] In sum, many aspects of privacy seem to be outside the scope of privacy as limited access.

Privacy as limited access is also too broad, according to Solove. The right to be let alone is a great slogan, but as a definition it's too vague. "A punch in the nose would be a privacy invasion as much as a peep in the bathroom," says Allen.[367] Solove adds that privacy as limited access doesn't explain which aspects of one's life are so private that access shouldn't be permitted.

> The theory provides no understanding as to the degree of access necessary to constitute a privacy violation. In the continuum between absolutely no access to the self and total access, the important question is where the lines should be drawn – that is, what degree of access should we recognize as reasonable?[368]

---

[364] See Solove 2009, p. 23; Rouvroy 2008, p. 25.
[365] Solove 2009, p. 24.
[366] Solove 2009, p. 24.
[367] Allen 1988, p. 7.
[368] Solove 2009, p. 20.

Among others, Nissenbaum says that in a modern society it's hard to define what is private.[369] "Despite a superficial elegance," adds Bennet, "one cannot restrict privacy rights and claims to the domain of the 'private' because contemporary socio-technical systems have blown away these clear distinctions."[370] What should be seen as private when discussing social network sites?[371]

In conclusion, while the privacy as limited access perspective has weaknesses, the perspective fits well when discussing many privacy infringements.

Privacy as control

At the end of the 1960s several books, sometimes called "the literature of alarm",[372] discussed the threats of the increasing amount of personal information that the state and other organisations gathered, often using computers.[373] In his book Privacy and Freedom, Westin introduced a privacy definition that would become very influential:

> Privacy is the claim of individuals, groups or institutions to determine when, how and to what extent information about them is communicated to others.[374]

This can be summarised as privacy as control. Around the late 1960s many feared that state agencies or other large organisations were amassing information about people. The use of computers for data processing added to the worries. Some feared that computers would make decisions about people.[375] Westin summarises the anxieties

---

[369] Nissenbaum 2010, chapter 6.
[370] Bennet 2011, p. 541-542.
[371] See on privacy management by young people on social network sites boyd 2014.
[372] Gassman & Pipe 1974, p. 12.
[373] See e.g. Packard 1966; Westin 1970; Miller 1971; Sieghart 1976. See for more references Blok 2002, p. 243-247, Regan 1995, p. 13-14.
[374] Westin 1970 (reprint of 1967). Warren & Brandeis made a similar remark: "The common law secures to each individual the right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others" (Warren & Brandeis 1890, p. 198).
[375] Bennett 1992, in particular p. 118-123; Mayer-Schönberger 1997, p. 221.

well. “You do not find computers in street corners or in free nature; you find them in big, powerful organisations.” [376] (Nowadays computers and smart phones are everywhere, but often data still flow towards large organisations.)

A 1972 UNESCO report warned that digital information about a person “may be used as the basis for passing judgment on him, a secret judgement from which there can be no appeal and which, because it is based on a computer, is thought to be objective and infallible.” The report adds that such decisions could be based on information that’s wrong, irrelevant, or taken out of context: “in fact the information used may be inexact, or out of date or of no real significance, with the result that the final conclusion amounts to a ‘scientific sophism’.”[377]

A 1974 report by the Organisation for Economic Co-operation and Development (OECD) said that the idea of privacy was – or should be – shifting from the limited access approach to the control approach.[378] The report suggests that, if people fear that organisations make decisions about them without the possibility of having a say in the decision process, the answer doesn’t have to lie in ensuring that information isn’t collected. Having control over information concerning oneself may be at least as important.

> The concept of privacy in the sense of data surveillance is undergoing adaptation to the modern setting. The earlier notion that privacy is the ability of an individual to withhold information about himself, a “right to be left alone”, is changing to a more practical current view required of man in a complex social environment. The concept is therefore shifting from the right of preventing the extraction or collection of

[376] Quoted in Bing 2007, p. 78, who relies on notes from a symposium in Paris around 1972.
[377] UNESCO 1972, p. 429.
[378] See for criticism on OECD’s “fair information practices” Clarke 2000; Clarke 2002; Bonner & Chiasson 2005.

> personal facts, to the extension of control over information recorded on an individual in a personal register. The new definition emphasizes the conditions placed on information content, and the control over dissemination and use of personal data.[379]

Seeing privacy as control over information implies that a lack of control, or losing control, over personal information interferes with privacy. As Gürses notes, two categories of privacy harm can be distinguished: experienced harm, and expected harm.[380] Experienced harms are adverse effects that result from data processing. Calo calls this objective harm, "the unanticipated or coerced use of information concerning a person against that person."[381] A loss of control over information can indeed lead to harm. For example, if a firm used somebody's personal information to charge that person higher prices, the lack of control leads to quantifiable harm for the person. A profile that suggests somebody is a terrorist could cause delays at a border control, or worse. A dossier that says somebody is a troublemaker could wreck a career.[382]

Another aspect of lack of control is the *feeling* of lost control, which could be called expected harm,[383] or subjective harm, "the perception of loss of control that results in fear or discomfort."[384] Many people are uncomfortable with organisations processing large amounts of information about them – including when no human ever looks at

---

[379] Gassman & Pipe 1974, p. 12-13 (emphasis original). In the US, a similar suggestion was made to redefine privacy as control over personal information (United States Department of Health, Education, and Welfare 1973, p. 38-41). That same report introduces a version of the fair information principles (p. 41); see chapter 4, section 1.
[380] Gürses 2010, p. 87-89. She doesn't limit her discussion to harms resulting from a lack of control over personal information, but discusses privacy concerns in general.
[381] Calo 2011, p. 1133 (see specifically about marketing: p. 1148).
[382] Ohm speaks of a "database of ruin" (Ohm 2010, p. 1748). To illustrate, in the United Kingdom construction companies used a secret black list to deny jobs to construction workers that were deemed troublesome (Boffey 2012).
[383] Gurses 2010, p. 87-89.
[384] Calo 2011, p. 1143.

the data.[385] People vaguely know that data about them are being collected and stored, but don't know how these data will be used. Solove compares the feeling of helplessness with the situation in Kafka's *The Trial*.[386] The main problem is "not knowing what is happening, having no say or ability to exercise meaningful control over the process."[387]

Privacy as control emphasises people's freedom to decide what should happen with information concerning them. Seeing privacy as control has the advantage of respecting people's individual preferences. Furthermore, privacy as control covers situations where one wants to share information with some, but not with others. The privacy as control perspective accommodates that people have different privacy wishes.

The privacy as control perspective can be recognised in legal practice. For instance, in 1982 the German Bundesverfassungsgericht formulated the right to informational self-determination: "the right of the individual to determine for himself whether his personal data should be divulged or utilized."[388] The Court doesn't suggest that people should have full control over data concerning them; in a modern society it's often necessary to process personal data.[389] Privacy as control has deeply influenced European data protection law.[390]

Westin's control definition also impacted scholarship.[391] Many authors use similar descriptions, such as Fried, who writes privacy "is not simply an absence of information about us in the minds of others; rather it is the *control* we have over

---

[385] See International Working Group on Data Protection in Telecommunications (Berlin Group) 2013, p. 2-3. Some suggest there can't be a privacy interference if no human looks at the information (see e.g. Posner 2008, p. 254; Van Der Sloot 2011, p. 66).
[386] Solove 2004, p. 38.
[387] Solove 2004, p. 38.
[388] Bundesverfassungsgericht 25 March 1982, BGBl.I 369 (1982), (Volks-, Berufs-, Wohnungs- und Arbeitsstättenzählung (Volkszählungsgesetz)), translation by Riedel, E.H., Human Rights Law Journal 1984, vol. 5, no 1, p. 94, p. 101, paragraph II.
[389] Idem, p. 101, paragraph II. See also González Fuster 2014, p. 176-177.
[390] See e.g. Mayer-Schönberger 1997; Bennett 1992, p. 14.
[391] See generally De Graaf 1997, Blok 2002; Regan 1995.

information about ourselves."[392] Similar descriptions have been used in literature on privacy on the internet.[393] Schwartz concludes that the control perspective has become "the traditional liberal understanding of information privacy."[394] He adds that "[t]he weight of the consensus about the centrality of privacy-control is staggering."[395]

Approaching privacy as control over information also has its weaknesses. According to Solove, privacy as control is too broad a definition, because it's unclear what "control" means. "We are frequently seen and heard by others without perceiving this as even the slightest invasion of privacy."[396] Furthermore, the definition seems to promise too much. In a modern society people must often disclose personal information to the state and other organisations.[397] If people had full control over their data, the tax office wouldn't be very successful. On the other hand, the control perspective doesn't imply that people should have full control over personal information; the right to privacy isn't absolute. The definition of privacy as control over personal information can also be criticised for being too narrow, says Solove. For instance, some privacy violations aren't covered by the definition, like being annoyed or disturbed during quiet times.[398]

Furthermore, the privacy as control perspective receives criticism because it puts too much emphasis on individual interests.[399] Many scholars argue that privacy is an important value for society, rather than merely an individual interest.[400] "Privacy has a value beyond its usefulness in helping the individual maintain his or her dignity or develop personal relationships",[401] says Regan. She adds: "society is better off if

---

[392] Fried 1968, p. 482. See also Miller, who describes privacy as "the ability to control the circulation of information relating to him" (Miller 1971, p. 25).
[393] Kang writes "control is at the heart of information privacy" (Kang 1998, p. 1266). Froomkin describes privacy as "the ability to control the acquisition or release of information about oneself" (Froonkin 2000, p. 1463).
[394] Schwartz 1999, p. 1613.
[395] Schwartz 2000, p. 820.
[396] Solove 2009, p. 25.
[397] See Schwartz 1999, p. 1663-1664; Blume 2012, p. 29.
[398] Solove 2009, p. 25-29.
[399] See e.g. Allen 1999; Solove 2009, p. 25-29.
[400] See e.g. Simitis 1987; Regan 1995; Schwartz 1999; Schwartz 2000; Westin 2003; Rouvroy & Poullet 2009; De Hert & Gutwirth 2006; Allen 2011; Van der Sloot 2012.
[401] Regan 1995, p. 221.

privacy exists."[402] Another problem with seeing privacy as control is that control is hard to achieve in practice. Approaching privacy as control leads to a focus on informed consent, like in data protection law.[403] Chapter 7 discusses practical problems with informed consent in the area of behavioural targeting.

Privacy as identity construction

Recently, a third perspective on privacy has become popular among scholars: privacy as the freedom from unreasonable constraints on identity construction. In 1998, three decades after Westin's book, Agre discussed the privacy implications of new developments such as networked computing. He notes that "control over personal information is control over an aspect of the identity one projects to the world (…)."[404] He adds:

> Privacy is the freedom from unreasonable constraints on the construction of one's identity.[405]

This perspective, privacy as identity construction for short, is popular among European legal scholars discussing profiling.[406] Hildebrandt says the definition emphasises the link between privacy and developing one's identity. Furthermore, the definition shows that one's identity isn't something static, as it speaks of identity construction. People aren't born with an identity that stays the same their whole life. A person's identity develops, and that person can try to influence how others see him or her.

---

[402] Regan 1995, p. 221.
[403] Mayer-Schönberger 1997; Hoofnagle & Urban 2014.
[404] Agre 1998, p. 7.
[405] Agre 1998, p. 7 (capitalisation adapted).
[406] See e.g. Rouvroy 2008; Gürses 2010; Hildebrandt 2010; Hildebrandt 2011a; Roosendaal 2013. See for criticism on the identity construction perspective De Andrade 2011.

Arguably, privacy as identity construction includes privacy as limited access. Sometimes, people need to be free from interference to develop their personality, an aspect of their identity.[407] The Human Rights Committee of the United Nations says "privacy refers to the sphere of a person's life in which he or she can freely express his or her identity, be it by entering into relationships with others or alone."[408]

Privacy isn't only about keeping others at a distance or keeping things confidential. Privacy also concerns how people present themselves, how they manage their image – for instance by disclosing or withholding information. Hence, the identity construction perspective includes privacy as control over personal information. Furthermore, privacy as identity construction highlights the social dimension of privacy, and captures the relevance of context.[409] "Privacy is also implicated in users' ability to control impressions and manage social contexts," say boyd and Ellison.[410] Gürses agrees, and speaks of "privacy as practice."[411] She adds that under this perspective, privacy can be "seen as the negotiation of social boundaries through a set of actions that users collectively or individually take with respect to disclosure, identity and temporality in environments that are mediated by technology."[412]

Privacy isn't merely about control. Privacy is about not *being* controlled.[413] "The difficulty with privacy-control in the information age," says Schwartz, "is that individual self-determination is itself shaped by the processing of personal data."[414] Privacy as identity construction concerns protection against unreasonable steering or manipulation – by humans or by technology. If the environment unreasonably manipulates somebody, privacy may be violated. The environment includes technology, and could include personalised ads or other information. Many fear that

---

[407] Hildebrandt 2011a, p. 381. See also Hildebrandt et al. 2008a, p. 11.
[408] Human Rights Committee, Coeriel et al. v. The Netherlands, Communication No. 453/1991, U.N. Doc. CCPR/C/52/D/453/1991 (1994).
[409] Hildebrandt 2011a, p. 381-382. See generally on the importance of context for privacy Nissenbaum 2010.
[410] boyd & Ellison 2007, p. 222.
[411] Gürses 2010, p. 31.
[412] Gürses 2014, p. 22.
[413] Thanks to Aleecia M. McDonald. I borrow this phrase from her.
[414] Schwartz 1999, p. 1661 (capitalisation adapted).

too much personalised information could surreptitiously steer people's choices. For example, if a person's cookie profile suggests that he or she is conservative, a website could show that person primarily conservative content. Such personalisation might influence that person's political views, without him or her being aware. Hence, content personalisation could lead to a constraint on the construction of one's identity, and possibly an unreasonable constraint.[415] Section 3.3 discusses behavioural targeting and the risk of manipulation.

The identity construction perspective raises the question of what identity means. There's a huge body of literature from various disciplines on the term identity.[416] FIDIS, an interdisciplinary research project on the Future of Identity in the Information Society, distinguishes two aspects of identity. First, there's a person's identity or image, as seen by others: a set of attributes. This is identity from a third person perspective. FIDIS speaks of the "common sense meaning identity."[417] A second aspect of one's identity is how a person sees him- or herself, from a first-person perspective. This could also be called somebody's individual identity, or self-identity.[418]

Like every privacy perspective, privacy as identity construction has weaknesses. For instance, it could be criticised for being too broad. Many kinds of influences could be seen as "unreasonable constraints" on identity construction. But perhaps not all these situations are best described as privacy violations.[419]

---

[415] Hildebrandt 2011a, p. 381. Westin, who sees privacy primarily as control, discussed the risk of unreasonable manipulation through subliminal advertising, "tampering with the unconscious" (Westin 1970, chapter 11).
[416] See for introductory texts on identity, with references to various disciplines Kerr et al. 2009a; Roosendaal 2013; Hildebrandt et al. 2008a.
[417] Hildebrandt et al. 2008a, p. 47.
[418] Hildebrandt et al. 2008a, p. 47. They also speak of the "relational notion" of identity.
[419] For instance, let's assume that photoshopped pictures in the media convey beauty ideals that deeply influence some people. If the altered pictures influence how people perceive themselves (too fat, too thin…), there may be an unreasonable constraint on the construction of their identity. This would bring the situation within the scope of privacy as identity construction. On the other hand, it could also be argued that such constraints aren't "unreasonable." Following that reasoning, there wouldn't be a privacy interference.

In conclusion, three groups of privacy perspectives can be distinguished: privacy as limited access, privacy as control over personal information, and privacy as the freedom of unreasonable constrains on identity construction. Each privacy perspective has strengths and weaknesses. Each perspective could be criticised for its scope, or for its vagueness. But in this study, the focus isn't on the exact scope of a definition that follows from a privacy perspective. This study doesn't argue that one privacy perspective is better than the other. The three perspectives highlight different aspects of privacy. Using one privacy perspective to discuss a problem doesn't imply that the other perspectives are irrelevant.

3.2 The right to privacy in European law

This section discusses the right to privacy in European law, and begins with an historical introduction. An early example of a rule that protects privacy interests, among other interests, is legal protection of the home against intrusions by the state or others. Protection of the home was granted in English case law from the sixteenth century,[420] and in the French Constitution of 1791.[421] Privacy-related interests also play an implicit role in court decisions prohibiting the publication of confidential letters from the eighteenth century.[422] Continental European law grants authors the *droit de divulgation*, that lets authors decide whether their work may be published.[423] Among the interests protected by this right are privacy-related interests.[424]

Legal protection of privacy-related interests in the area of press publications dates back centuries as well. The French Constitution of 1791 protected the freedom of the press, but also included protection against "[c]alumnies and insults against any

---

[420] King's Bench 2 November 1765, Entick v. Carrington [1765] EWHC KB J98 95 ER 807. See on such early case law Cuddihy 2009, p. ixi.
[421] Title IV, article 9 of the French constitution of 1791.
[422] See for instance the case Chancery Court, Pope v. Curl [1741] 2 Atk. 342.
[423] See e.g. the European Copyright Code, article 3.2 (The Wittem Project 2010); Hugenholtz 2012, p. 347-348.
[424] Mayer-Schönberger 2010, p. 1864-1865.

persons whomsoever relative to their private life."[425] The law has provided protection against the use of one's image for a long time. In 1889 a German court ordered the destruction of photos of Otto van Bismarck on his deathbed, which were taken without his family's consent.[426] A French court handed down a similar judgement in 1858 regarding a portrait of an actress on her deathbed.[427]

Confidentiality of communications is another privacy-related right with a long history. King Louis XI of France nationalised the postal service in 1464. Soon the state organised mail delivery in many European countries. This gave the state the opportunity to read the letters, which, for example, happened systematically in France. In response to such practices, many states in Europe included a right to the confidentiality of correspondence in their constitutions during the nineteenth century. Hence, it was the introduction of a new communication channel (the postal service) that eventually led to the introduction of a new fundamental right.[428] In the twentieth century, the right to confidentiality of correspondence was extended to a general right to confidentiality of communications in Europe.[429] To the modern eye, legal protection of the home, legal protection against excesses of the press, and the right to confidentiality of correspondence are examples of the protection of privacy-related interests. Since the end of the nineteenth century, scholars have focused on privacy as the common feature of these different interests.[430]

The legal protection of privacy at international level blossomed after the Second World War. The Universal Declaration of Human Rights from 1948 contains a

---

[425] French Constitution of 1791 (3 September, 1791), chapter V, par. 17. See Whitman 2004, p. 1172.
[426] Zweigert & Kötz 1987, p. 688.
[427] Tribunal civil de la Seine, 16 June 1858, D.P. 1858, III, p. 62 (Rachel). See Prins 2009. See on the question of whether privacy rights do – or should – continue after death McCallig 2013; Harbinja 2013; Edwards 2013; Korteweg & Zuiderveen Borgesius 2009.
[428] See on the history of the legal protection of confidentiality of communications Steenbruggen 2009, p. 11; Hofman 1995, p. 23 and further; Ruiz 1997, p. 64-70.
[429] See for example article 5(1) of the e-Privacy Directive, and article 8 of the EU Charter of Fundamental Rights.
[430] Schoeman 1984, p. 1. See the discussion of Warren & Brandeis in the previous section.

provision that protects privacy.[431] The International Covenant on Civil and Political Rights also protects privacy:

> 1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
>
> 2. Everyone has the right to the protection of the law against such interference or attacks.[432]

European Convention on Human Rights

The right to privacy is set out in the European Convention on Human Rights, a treaty of the Council of Europe that entered into force in 1953.[433] The Council of Europe is the most important human rights organisation in Europe. It's based in Strasburg and has 47 member states, including all EU member states. All Council of Europe member states have signed up to the European Convention on Human Rights.[434] Article 8 of the European Convention on Human Rights contains the right to respect for private and family life, one's home and correspondence. Hence, it protects the right to privacy and other interests.[435]

Article 8 of the Convention is structured as follows: paragraph 1 prohibits interferences with the right to private life. Paragraph 2 shows that this prohibition isn't absolute. In many cases the right to privacy can be limited in the view of other

---

[431] Article 12 of the Universal Declaration of Human Rights.
[432] Article 17 of the International Covenant on Civil and Political Rights.
[433] The official title is: European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14.
[434] See the website of the Council of Europe: <www.coe.int/en/web/portal/country-profiles> accessed 14 May 2014.
[435] The European Court of Human Rights uses the phrase "private life" rather than privacy, but as noted, this study uses the phrases interchangeably. See on the distinction González Fuster 2014, p. 255.

interests, such as the prevention of crime, or the rights of others.[436] Article 8 reads as follows:

> European Convention on Human Rights
>
> Article 8, Right to respect for private and family life
>
> 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.

Charter of Fundamental Rights of the European Union

The Charter of Fundamental Rights of the European Union is a document listing the fundamental rights and freedoms recognised by the EU. The Charter was adopted in 2000, and was made a legally binding instrument by the Lisbon Treaty of 2009.[437] The Charter copies the right to private life almost verbatim from the European Convention on Human Rights. But the Charter uses the more modern and technology neutral term "communications" instead of "correspondence." The article reads as follows:

---

[436] Using a phrase from the last section, "reasonable" constraints on the freedom of identity construction don't violate privacy.

[437] See article 6.1 of the Treaty on EU (consolidated version 2012). The institutions of the EU must comply with the Charter. The Member States are also bound to comply with the Charter, when implementing EU law (article 51 of the Charter).

> Charter of Fundamental Rights of the European Union
>
> Article 7, Respect for private and family life
>
> Everyone has the right to respect for his or her private and family life, home and communications.

It follows from the EU Charter of Fundamental Rights that its article 7 offers at least the same protection as article 8 of the European Convention on Human Rights. The Charter has a separate provision that lists the limitations that may be imposed on its rights.[438] Regarding the right to private life, the limitations are similar to those listed in the second paragraph of article 8 of the European Convention on Human Rights.[439] In addition to the right to privacy, the Charter contains a separate right to the protection of personal data.[440] That right is discussed in the next chapter of this study, which introduces data protection law.[441]

The European Court of Justice says the right to privacy in the Charter and the Convention must be interpreted identically.[442] "Article 7 of the Charter must (…) be given the same meaning and the same scope as Article 8(1) of the ECHR, as interpreted by the case-law of the European Court of Human Rights (…)."[443] The privacy related case law of the European Court of Human Rights receives most attention in this study, because it's more developed than that of the European Court of Justice.

---

[438] Article 52 of the EU Charter Of Fundamental Rights; Note from the Praesidium, comments on article 7 (Praesidium 2000).
[439] See on the difference between article 52 of the Charter and article 8(2) of the Convention González Fuster 2014, p. 201.
[440] Article 8 of the EU Charter Of Fundamental Rights.
[441] See chapter 4, section 1.
[442] For brevity, the "Court of Justice of the European Union" is referred to as European Court of Justice in this study. See article 19(1) of the Treaty on EU (consolidated version 2012).
[443] CJEU, C-400/10, J. McB. v L. E., 5 October 2010, par. 53.

Living instrument doctrine

While scholars sometimes deplore the privacy's vagueness, the European Court of Human Rights uses the vagueness as an advantage. This way, the Court can apply the right to private life to unforeseen situations. The European Court of Human Rights interprets the rights granted in article 8 generously, and refuses to define the ambit of the article. The Court "does not consider it possible or necessary to attempt an exhaustive definition of the notion of private life."[444] The Court says it takes "a pragmatic, common-sense approach rather than a formalistic or purely legal one."[445] This allows the Court to adapt the protection of article 8 to new circumstances, such as technological developments. The Court's dynamic approach has been called the "living instrument doctrine."[446] The Court puts it as follows. "That the Convention is a living instrument which must be interpreted in the light of present-day conditions is firmly rooted in the Court's case-law."[447] The Court uses a "dynamic and evolutive" interpretation of the Convention, and states that "the term 'private life' must not be interpreted restrictively."[448]

> It is of crucial importance that the Convention is interpreted and applied in a manner which renders its rights practical and effective, not theoretical and illusory. A failure by the Court to maintain a dynamic and evolutive approach would indeed risk rendering it a bar to reform or improvement (…).[449]

---

[444] See e.g. ECtHR, Niemietz v. Germany, No. 13710/88, 16 December 1992, par. 29. The Court consistently confirms this approach. See e.g. ECtHR, Pretty v. United Kingdom, No. 2346/02, 29 April 2002, par. 61; ECtHR, S. and Marper v. United Kingdom, No. 30562/04 and 30566/04. 4 December 2008, par. 66.
[445] ECtHR, Botta v. Italy (153/1996/772/973), 24 February 1998, par. 27.
[446] Mowbray 2005.
[447] ECtHR, Matthews v. United Kingdom, No. 24833/94, 18 February 1999, par. 39. The Court started the "living instrument" approach in ECtHR, Tyrer v. United Kingdom, No. 5856/72, 25 April 1978, par. 31.
[448] Christine Goodwin v. United Kingdom, No. 28957/95, 11 July 2002, par 74; ECtHR, Amann v. Switzerland, No. 27798/95, 16 February 2000, par. 65.
[449] Christine Goodwin v. United Kingdom, No. 28957/95, 11 July 2002, par 74. See also ECtHR, Armonas v. Lithuania, No. 36919/02, 25 November 2008, par. 38.

The Court's dynamic approach is evident in the privacy case law. In 1978 for instance, the Court brought telephone calls under the scope of article 8, although the Convention speaks of private life and correspondence.[450] In 2004 the Court said: "increased vigilance in protecting private life is necessary to contend with new communication technologies which make it possible to store and reproduce personal data."[451] In the 2007 Copland case, the Court brought internet use under the protection of article 8. After repeating that phone calls are protected, the Court simply said that "[i]t follows logically that e-mails sent from work should be similarly protected under article 8, as should information derived from the monitoring of personal internet usage."[452] The Court adds that people have reasonable expectations of privacy regarding their use of the internet.[453]

The right to private life protects many aspects of personal development. In the 2008 Marper case, concerning storage of DNA samples in a police database, the Court lists some aspects of private life that it has brought under the scope of article 8.

> The Court recalls that the concept of "private life" is a broad term not susceptible to exhaustive definition. It covers the physical and psychological integrity of a person. It can therefore embrace multiple aspects of the person's physical and social identity. Elements such as, for example, gender identification, name and sexual orientation and sexual life fall within the personal sphere protected by article 8. Beyond a person's name, his or her private and family life may include

---

[450] ECtHR, Klass and others v. Germany, No. 5029/71, 6 September 1978, par. 41.
[451] ECtHR, Von Hannover v. Germany (I), No. 59320/00, 24 September 2004, par 70.
[452] ECtHR, Copland v. United Kingdom, No. 62617/00, 3 April 2007, par. 41 (capitalisation adapted, internal citations and numbering deleted).
[453] ECtHR, Copland v. United Kingdom, No. 62617/00, 3 April 2007, par 42. The European Court of Human Rights doesn't apply the same "reasonable expectation of privacy" test as US Courts. The European Court says: "A person's reasonable expectations as to privacy is a significant though not necessarily conclusive factor" (ECtHR, Perry v. United Kingdom, No. 63737/00, 17 July 2003, par. 37). See on the US Schwartz & Solove 2009, p. 106-137

> other means of personal identification and of linking to a family. Information about the person's health is an important element of private life. The Court furthermore considers that an individual's ethnic identity must be regarded as another such element. Article 8 protects in addition a right to personal development, and the right to establish and develop relationships with other human beings and the outside world.[454]

Horizontal effect

The Convention was originally envisioned to protect people against the state. The state has a negative duty not to interfere too much in people's lives. But the Court also derives positive duties for states from the Convention. Hence, sometimes the state has to take action to protect people from interferences by other private actors. The Court summarises this as follows.

> Although the object of article 8 is essentially that of protecting the individual against arbitrary interference by the public authorities, it does not merely compel the State to abstain from such interference: in addition to this primarily negative undertaking, there may be positive obligations inherent in an effective respect for private or family life (…). These obligations may involve the adoption of measures designed to

[454] ECtHR, S. and Marper v. United Kingdom, No. 30562/04 and 30566/04. 4 December 2008, par. 66 (internal citations omitted; capitalisation adapted).

> secure respect for private life even in the sphere of the relations of individuals between themselves (…).[455]

People can't sue another private party under the European Convention on Human Rights.[456] But people can complain to the Court if the state doesn't adequately protect their rights against infringements by other non-state actors. This way, the Convention's privacy right has a horizontal effect.[457] The Court says it "does not consider it desirable, let alone necessary, to elaborate a general theory concerning the extent to which the Convention guarantees should be extended to relations between private individuals *inter se*."[458]

The positive obligations can be far-reaching.[459] The Court requires states to *effectively* protect the Convention rights: "Article 8, like any other provision of the Convention or its Protocols, must be interpreted in such a way as to guarantee not rights that are theoretical or illusory but rights that are practical and effective."[460] A state can fail in its positive obligations to ensure effective protection of the right to private life if non-state actors handle personal data carelessly. For instance, having a data protection law that allows people to claim for damages after a data breach isn't always sufficient.[461]

Some commentators are sceptical of the horizontal effect of human rights.[462] Others say it's "self-evident" that human rights have horizontal effect.[463] Gutwirth argues that protecting a public interest is a more acceptable reason to interfere with privacy than aiming for profit.

---

[455] ECtHR, Z v. Finland, No. 22009/93, 25 February 1997, par. 36 (capitalisation adapted). See also ECtHR, Mosley v. United Kingdom, 48009/08, 10 May 2011, par 106.
[456] Article 34 of the European Convention on Human Rights.
[457] See generally Akandji-Kombe 2007; De Hert 2011; Verhey 1992, Verhey 2009.
[458] ECtHR, VGT Verein Gegen Tierfabriken v. Switzerland, No. 24699/94, 28 June 2001, par. 46.
[459] See generally on positive requirements following from article 8 of the European Convention on Human Rights in the field of data protection De Hert 2011. To what extent the EU Charter of Fundamental Rights has horizontal effect is unclear (see Kokott & Sobotta 2014, p. 225).
[460] ECtHR, Biriuk v. Lithuania, No. 23373/03, 25 November 2008, par. 37. See also ECtHR, Airey v. Ireland, No. 6289/73, 9 October 1979, par. 24-25.
[461] ECtHR, I. v. Finland, No. 20511/03, 17 July 2008, par. 47.
[462] See e.g. De Vos 2010.
[463] Gutwirth 2002, p. 38.

> If privacy is protected against acts of the public authorities, should it "a fortiori" not be protected against individual acts, too? After all, the government acts on behalf of the public interest, which seems to be a more legitimate reason for an invasion of privacy than, for example, personal profit seeking of a businessman.[464]

Three privacy perspectives in case law

The above-mentioned three privacy perspectives – privacy as limited access, privacy as control, and privacy as identity construction – can be recognised in the case law of the European Court of Human Rights, although the Court doesn't use this taxonomy.[465] Privacy as limited access lies at the core of article 8: "the essential object and purpose of Article 8, [is] to protect the individual against arbitrary interference by the public authorities."[466] But the Court also emphasises privacy as limited access in cases where non-state actors interfere with privacy. "The right to privacy consists essentially in the right to live one's own life with a minimum of interference."[467]

The Court mentions keeping personal information confidential as well. "The concept of private life covers personal information which individuals can legitimately expect should not be published without their consent (…)."[468] In some judgments, the reasoning of the Court reminds one of the perspective of privacy as a right to be let

---

[464] Gutwirth 2002, p. 38.
[465] See for an overview of the article 8 case law, using other taxonomies Harris et al. 2009, p. 361-424; Heringa & Zwaak 2006.
[466] ECtHR, Niemietz V. Germany, No. 13710/88, 16 December 1992, par. 31. Harris et al. also see privacy as limited access, "a private space into no-one is entitled to enter", as the core of the concept of private life (Harris et al. 2009, p. 367).
[467] This definition of privacy is taken from Parliamentary Assembly, Resolution 428 (1970) containing a declaration on mass communication media and human rights. The Court cited the definition in several cases, including cases where non-state actors infringed on privacy. See ECtHR, Von Hannover v. Germany (I), No. 59320/00, 24 September 2004, par 42; ECtHR, Von Hannover v. Germany (II), Nos. 40660/08 and 60641/08, 7 February 2012, par. 71; ECtHR, Mosley v. United Kingdom, 48009/08, 10 May 2011, par. 56.
[468] ECtHR, Flinkkilä and others v. Finland, No. 25576/04, 6 April 2010, par. 75.

alone. In a 2004 case, the Court took into account that paparazzi harassed the Princess of Monaco.[469] In sum, article 8 comprises privacy as limited access.

Privacy as control is also present in the case law of the European Court of Human Rights. The Court says "it would be too restrictive to limit the notion [of private life] to an 'inner circle' in which the individual may live his own personal life as he chooses and to exclude therefrom entirely the outside world not encompassed within that circle."[470] In several cases, the Court cites a Resolution of the Parliamentary Assembly of the Council of Europe on the right to privacy.[471] "In view of the new communication technologies which make it possible to store and use personal data, the right to control one's own data should be added to this definition."[472] In a case where a picture was taken without consent, the Court says it's a problem if "the person concerned would have no control over any subsequent use of the image."[473] Privacy as control can also be recognised in cases where the Court accepts a right for people to access[474] or to correct[475] personal data regarding them.

The Court has established that storing personal data can interfere with privacy, regardless of how those data are used.[476] "The mere storing of data relating to the private life of an individual amounts to an interference within the meaning of article 8

---

[469] ECtHR, Von Hannover v. Germany (I), No. 59320/00, 24 September 2004. In principle, offensive spam email interferes with privacy (ECtHR, Muscio v. Italy, No. 31358/03, 13 November 2007 (inadmissible)).

[470] ECtHR, Niemietz v. Germany, No. 13710/88, 16 December 1992, par. 29. The Court also stresses control over personal information in ECtHR, Von Hannover v. Germany (II), Nos. 40660/08 and 60641/08, 7 February 2012, par. 96.

[471] See e.g. ECtHR, Von Hannover v. Germany (I), No. 59320/00, 24 September 2004, par 72; ECtHR, Von Hannover v. Germany (II), Nos. 40660/08 and 60641/08, 7 February 2012, par. 71.

[472] Parliamentary Assembly, Resolution 1165 (1998), on the right to privacy.

[473] ECtHR, Reklos and Davourlis v. Greece, No. 1234/05, 15 January 2009, par 40. See also par. 42-43 for a control perspective on privacy. See also ECtHR, Von Hannover v. Germany (II), Nos. 40660/08 and 60641/08, 7 February 2012, par. 96.

[474] See e.g. ECtHR, Gaskin v. United Kingdom, Application no. 10454/83, 7 July 1989, par. 49; ECtHR, McMichael v. United Kingdom, No. 16424/90, 24 February 1995, par 92; ECtHR, Mcginley and Egan v. United Kingdom (10/1997/794/995-996), 9 June 1998. par 97.

[475] See e.g. ECtHR, Rotaru v. Romania, No. 28341/95, 4 May 2000, par. 46; Christine Goodwin v. United Kingdom, No. 28957/95, 11 July 2002, par. 93; ECtHR, Segerstedt-Wiberg and others v. Sweden, No. 62332/00, 6 June 2006, par. 99; ECtHR, Cemalettïn Canli v. Turkey, No. 22427/04, 18 November 2008, par 41-43; ECtHR, Ciubotaru V. Moldova, No. 27138/04, 27 April 2010, par. 51, par. 59.

[476] See e.g. ECtHR, Leander v. Sweden, No. 9248/81, 26 March 1987, par. 48; ECtHR, Amann v. Switzerland, No. 27798/95, 16 February 2000, par. 69; ECtHR, Copland v. United Kingdom, No. 62617/00, 3 April 2007, par. 43-44; ECtHR, S. and Marper v. United Kingdom, No. 30562/04 and 30566/04. 4 December 2008, par. 67, par 121.

(…). The subsequent use of the stored information has no bearing on that finding."[477] However, the Court said this in a case where the state stored personal data that are particularly sensitive (DNA data). In some cases where private parties store personal data, the Court also says that the mere storage interferes with privacy, but again the data were rather sensitive.[478] In some other cases the Court didn't see personal data processing as a privacy interference. Hence, for the Court some personal data processing activities don't interfere with privacy.[479] Sometimes the European Court of Human Rights also applies data protection principles (see the next chapter).[480] The Court has cited the Data Protection Convention,[481] and the Data Protection Directive.[482]

The other important European Court, the European Court of Justice, says that privacy is threatened by any personal data processing – and doesn't limit its remarks to sensitive data.[483] This is in line with the EU Charter of Fundamental Rights, which requires fair processing for any kind of personal data. The Court says about the right to privacy and data protection: "as a general rule, any processing of personal data by a third party may constitute a threat to those rights."[484] As the Data Protection Directive requires, the Court does differentiate between non-special personal data and "special

---

[477] ECtHR, S. and Marper v. United Kingdom, No. 30562/04 and 30566/04. 4 December 2008, par. 67 (capitalisaion adapted).

[478] In a case where a private party held photographic material, the mere retention of that personal information interfered with private life (ECtHR, Reklos and Davourlis v. Greece, No. 1234/05, 15 January 2009, par. 42). See along similar lines (regarding video surveillance by a private party) ECtHR, Köpke v. Germany, No. 420/07 (inadmissible), 5 October 2010.

[479] See e.g. ECtHR, Perry v. United Kingdom, No. 63737/00, 17 July 2003, par 40: "the normal use of security cameras *per se* whether in the public street or on premises, such as shopping centres or police stations where they serve a legitimate and foreseeable purpose, do not raise issues under Article 8 § 1 of the Convention." See De Hert & Gutwirth 2009, p. 24-26; Kranenborg 2007, p. 311-312; Kokott & Sobotta 2014, p. 223-224; González Fuster 2014, p. 101.

[480] See on the data protection principles chapter 4, section 2.

[481] See for an early case ECtHR, Z v. Finland, No. 22009/93, 25 February 1997, par. 95.

[482] Examples of cases where the Court mentions the Data protection Directive include ECtHR, Romet v. The Netherlands, No. 7094/06, 14 February 2012; ECtHR, M.M. v. United Kingdom, No. 24029/07, 13 November 2012; ECtHR, S. and Marper v. United Kingdom, No. 30562/04 and 30566/04. 4 December 2008; ECtHR, Mosley v. United Kingdom, 48009/08, 10 May 2011.

[483] CJEU, C-291/12, Schwartz v. Stadt Bochum, 17 October 2013, par. 25. See also the judgment on the Data Retention Directive CJEU, C-293/12 and C-594/12, Digital Rights Ireland Ltd, 8 April 2014, par. 29.

[484] CJEU, C-291/12, Schwartz v. Stadt Bochum, 17 October 2013, par. 25. See also the judgment on the Data Retention Directive CJEU, C-293/12 and C-594/12, Digital Rights Ireland Ltd, 8 April 2014, par. 29.

categories of data", such as data regarding health, religion or race.[485] In sum, privacy as control can be recognised in the case law of the European Court of Human Rights and the European Court of Justice.[486]

The third privacy perspective, the freedom from unreasonable constraints on identity construction, can be recognised in the case law as well. For example, in a case regarding privacy infringements by the press, the Court emphasises privacy's function for the construction of one's personality. "As to respect for the individual's private life, the Court reiterates the fundamental importance of its protection in order to ensure the development of every human being's personality. That protection extends beyond the private family circle to include a social dimension."[487]

The Court says the right to private life should enable a person to "freely pursue the development and fulfilment of his personality."[488] The right to private life also includes a social dimension and "comprises the right to establish and develop relationships with other human beings."[489] In a 2012 judgment concerning Princess Caroline of Monaco, who complained about privacy violations by the press, the reasoning of the Court relates to the privacy as identity construction perspective.

> The Court reiterates that the concept of private life extends to aspects relating to personal identity, such as a person's name, photo, or physical and moral integrity; the guarantee afforded by article 8 of the Convention is primarily intended to ensure

---

[485] See e.g. CJEU, C-101/01, Lindqvist, 6 November 2003.
[486] The European Court of Justice isn't very explicit on the question of whether it sees privacy as control over personal information. However, the Court's reasoning does remind one of privacy as control sometimes. For instance, in the Data Retention case the Court says that the "fact that data are retained and subsequently used without the subscriber or registered user being informed", entails a "particularly serious" interference with the right to privacy (CJEU, C-293/12 and C-594/12, Digital Rights Ireland Ltd, 8 April 2014, par. 37). The Google Spain case, emphasising the right to request erasure of data (possibly too much), also fits the privacy as control perspective (CJEU, C-131/12, Google Spain, 13 May 2014).
[487] ECtHR, Biriuk v. Lithuania, No. 23373/03, 25 November 2008, par. 38.
[488] ECtHR, Shtukaturov v. Russia, No. 44009/05, 27 March 2008, par. 83.
[489] ECtHR, Amann v. Switzerland, No. 27798/95, 16 February 2000, par. 65; ECtHR, Perry v. United Kingdom, No. 63737/00, 17 July 2003, par. 65.

> the development, without outside interference, of the personality of each individual in his relations with other human beings.[490]

In conclusion, judges and lawmakers try to adapt the right to privacy to new developments and technologies. The right to privacy is laid down in the European Convention on Human Rights, and in the EU Charter of Fundamental Rights. The European Court of Human Rights interprets the right to privacy generously, and refuses to pin itself down to one definition. Each of the three privacy perspectives that was discussed in section 3.1 can be recognised in the case law of the European Court of Human Rights.

3.3 Privacy implications of behavioural targeting

There are many privacy problems with behavioural targeting.[491] This study focuses in particular on three problems. First, the massive collection of data about user behaviour can lead to chilling effects. A second problem is the lack of individual control over personal information. A third problem is social sorting and the risk of manipulation.[492] The problems are related and partly overlap.

Chilling effects relating to massive data collection on user behaviour

Many people find data collection for behavioural targeting creepy or invasive.[493] The tracking for behavioural targeting has often been compared with following somebody

---

[490] ECtHR, Von Hannover v. Germany (II), Nos. 40660/08 and 60641/08, 7 February 2012, par 95 (capitalisation adapted). See also ECtHR, Niemietz v. Germany, No. 13710/88, 16 December 1992, par 29. Arguably, the privacy as identity construction perspective could also be recognised in the Google Spain judgment of the European Court of Justice, although the Court based its reasoning mostly on data protection law. People could try to shape their identity by influencing search results regarding their name (CJEU, C-131/12, Google Spain, 13 May 2014).

[491] See generally on privacy (and related) problems regarding behavioural targeting Turow 2011; Castelluccia & Narayanan 2012; Federal Trade Commission 2012. See also Hildebrandt & Gutwirth (eds.) 2008, on profiling, and Richards 2013, on surveillance, and the references therein.

[492] Van Der Sloot gives a similar analysis of privacy problems resulting from data collection in the area of behavioural targeting. But he argues that the problems are better conceptualised as data protection problems, rather than as privacy problems (Van Der Sloot 2011).

on the streets.[494] People use the internet for many things, including things that they would prefer to keep confidential.[495] As Berners-Lee notes, browsing behaviour can reveal a lot about a person:

> The URLs which people use reveal a huge amount about their lives, loves, hates, and fears. This is extremely sensitive material. People use the web in crisis, when wondering whether they have STDs, or cancer, when wondering whether they are homosexual and whether to talk about it, to discuss political views which may to some may be abhorrent, and so on.[496]

For example, many websites about health problems allow third parties to track their visitors. People might search for information about unwanted pregnancies, drugs, suicidal tendencies, or HIV. Medical problems can be embarrassing or simply personal. People may have an individual privacy interest in keeping confidential that they read about such topics. But if a chilling effect occurred, the problem would go beyond individual interests. People with questions about health might refrain from looking for information if they fear being tracked.[497] It would be detrimental for society if a person failed to seek treatment for a contaguous disease.

People also use the internet to read about news and politics. Third party tracking happens on the websites of most newspapers. But people could feel uneasy when firms monitor their reading habits. A person's political opinion could be inferred from his or her reading habits. People may want to read a communist, Christian, or Muslim

---

[493] See chapter 7, section 1 for research on people's attitude regarding behavioural targeting.
[494] See e.g. Kang 1998, par 1198-1199; Kristol 2001, p. 180; Chester 2007, p. 134; International Working Group on Data Protection in Telecommunications (Berlin Group) 2013, p. 2-3.
[495] As Richards puts it, a record of somebody's browsing behaviour is "in a very real sense a partial transcript of the operation of a human mind" (Richards 2008, p. 436).
[496] Berners-Lee 2009. He discusses behavioural targeting that relies on deep packet inspection, but his remark is relevant for behavioural targeting in general.
[497] See United Nations High Commissioner for Human Rights 2014, p. 5; Castelluccia & Narayanan 2012, p. 9.

news site. And a political opinion that is uncontroversial now, could become suspicious in the future.[498] Many conclusions could be drawn from people's browsing behaviour – the right or the wrong conclusions.[499] Somebody might be looking for information about cancer for a friend. And somebody who reads about bombing airports isn't necessarily a terrorist.

People have individual interests in keeping their reading habits confidential, but it's also in the interest of society that people don't fear surveillance. Frank La Rue, the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression for the United Nations, says privacy is essential in order to enjoy the right to seek and receive information.

> States cannot ensure that individuals are able to freely seek and receive information or express themselves without respecting, protecting and promoting their right to privacy. Privacy and freedom of expression are interlinked and mutually dependent; an infringement upon one can be both the cause and consequence of an infringement upon the other.[500]

Behavioural targeting could be seen as a form of surveillance, as defined by Lyon: "any collection and processing of personal data, whether identifiable or not, for the purposes of influencing or managing those whose data have been garnered."[501] The goal of data processing for behavioural targeting is influencing people with advertising. Lyon stresses that the word surveillance doesn't imply that a practice is sinister. But he adds that surveillance always implies "power relations."[502]

---

[498] Berners-Lee 2009 makes a similar point. See also Turow et al. 2012.
[499] Van Hoboken 2012, p. 323; Purtova 2011, p. 44-46.
[500] La Rue 2013, p. 20.
[501] Lyon 2001, p. 2. A United Nations report speaks of "communications surveillance" (La Rue 2013, p. 3).
[502] Lyon 2001, p. 16. See also Clarke, who speaks of dataveillance, "the systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons" (Clarke 1999).

The chilling effect of surveillance can be illustrated by the Panopticon, a circular prison designed by Bentham.[503] The prison has a watchtower in the middle, and the guards can watch the prisoners at all times. The prisoners can always see the watchtower, so they're reminded that they could be being watched at any given time. But the prisoners can't see whether they are being watched. Therefore, they will adapt their behaviour.[504]

Behavioural targeting fits Lyon's definition of surveillance, but there's no threat of punishment. However, as the German Bundesverfassungsgericht notes, not knowing how personal information will be used can cause a chilling effect as well. "If someone is uncertain whether deviant behaviour is noted down and stored permanently as information, or is applied or passed on, he will try not to attract attention by such behaviour." [505] Unfettered surveillance could lead to self-censorship. The Court adds that this threatens society as a whole. "This would not only impair [the individual's] chances of development but would also impair the common good, because self-determination is an elementary functional condition of a free democratic community based on its citizens' capacity to act and to cooperate."[506]

It has been suggested that online tracking doesn't merely influence people's behaviour, but also their thoughts. In the US, Richards argues that surveillance threatens the possibility to "develop ideas and beliefs away from the unwanted gaze or interference of others." Therefore, he says, the first amendment (that protects freedom of speech) should be interpreted in such a way that it safeguards intellectual privacy. "Intellectual privacy is protection from surveillance or interference when we

---

[503] Foucault 1977.

[504] It has been suggested that behavioural targeting is worse than a Panopticon, as firms can store all the information they gather (International Working Group on Data Protection in Telecommunications (Berlin Group) 2013).

[505] Bundesverfassungsgericht 25 March 1982, BGBl.I 369 (1982), (Volks-, Berufs-, Wohnungs- und Arbeitsstättenzählung (Volkszählungsgesetz)), translation by Riedel, E.H., Human Rights Law Journal 1984, vol. 5, no 1, p. 94, p. 100, paragraph II.

[506] Bundesverfassungsgericht 25 March 1982, BGBl.I 369 (1982), (Volks-, Berufs-, Wohnungs- und Arbeitsstättenzählung (Volkszählungsgesetz)), translation by Riedel, E.H., Human Rights Law Journal 1984, vol. 5, no 1, p. 94, p. 100, paragraph II.

are engaged in the processes of generating ideas – thinking, reading, and speaking with confidantes before our ideas are ready for public consumption."[507] Similarly, Cohen argues for a "right to read anonymously."[508]

In Europe, Van Hoboken suggests that privacy is necessary to enjoy the right to impart and receive information.

> It can be argued that the user's privacy is a precondition for the fundamental right to search, access and receive information and ideas freely. Free information-seeking behavior can be quite negatively affected if the main available options to find information online entail comprehensive surveillance and storage of end-users behavior without appropriate guarantees in view of intellectual freedom.[509]

The chilling effect could be greater if communications, such as email messages, are also monitored. The European Court of Human Rights says that the mere threat of surveillance threatens fundamental rights. In a case regarding a German law that empowered the authorities to inspect mail and to listen to telephone conversations, the Court warns that the "menace of surveillance can be claimed in itself to restrict free communication."[510] In another case, the Court states that such a "threat necessarily strikes at freedom of communication between users of the telecommunications services and thereby amounts in itself to an interference with the exercise of the

---

[507] Richards 2014. See Richards 2008; Richards 2013.
[508] Cohen 1995. See also Kang 1998, p. 1260.
[509] Van Hoboken 2012, p. 226, internal footnote omitted. While he discusses surveillance by search engines, his remarks are also relevant for behavioural targeting.
[510] ECtHR, Klass and others v. Germany, No. 5029/71, 6 September 1978, par. 37.

applicants' rights under article 8, irrespective of any measures actually taken against them."[511]

The European Court of Human Rights says that monitoring traffic data (sometimes called metadata), rather than the content of communications, also interferes with the right to privacy.[512] According to the Bundesverfassungsgericht, the retention of traffic data by telecommunications companies for law enforcement can invoke a "feeling of permanent control", because people feel a "diffuse threat."[513]

> [A] preventive general retention of all telecommunications traffic data (…) is, among other reasons, also to be considered as such a heavy infringement because it can evoke a sense of being watched permanently (…). The individual does not know which state official knows what about him or her, but the individual does know that it is very possible that the official does know a lot, possibly also highly intimate matters about him or her.[514]

Along the same lines, the European Court of Justice states that storing traffic data by telecommunications companies for law enforcement purposes "is likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance."[515] The cases concern surveillance for law enforcement, but similar conclusions can be drawn about behavioural targeting.[516] Once private parties

---

[511] ECtHR, Liberty and others v. United Kingdom, No. 58243/00, 1 July 2008, par. 56. See also par. 104-105. See similarly United Nations High Commissioner for Human Rights 2014, p. 7.
[512] ECtHR, Malone v. United Kingdom, No. 8691/79, 2 August 1984, par. 83-84; ECtHR, Copland v. United Kingdom, No. 62617/00, 3 April 2007. See also CJEU, C-293/12 and C-594/12, Digital Rights Ireland Ltd, 8 April 2014.
[513] Traffic data are, in short, data processed for the purpose of the conveyance of a communication (see article 2(b) of the e-Privacy Directive). See chapter 5, section 6.
[514] Bundesverfassungsgericht 2 March 2010, BvR 256/08 vom 2.3.2010, Absatz-Nr. (1 - 345), (Vorratsdatenspeicherung) [Data Retention]. Translation by Bellanova et al. 2011, p. 10.
[515] CJEU, C-293/12 and C-594/12, Digital Rights Ireland Ltd, 8 April 2014, par. 37.
[516] See Article 20 Working Party 2014, WP 217, p. 37.

hold personal data, law enforcement bodies can, and indeed often do, access those data. In a case regarding monitoring internet traffic by a private party, the Advocate General of the European Court of Justice states that such monitoring "constitutes, by its very nature, a 'restriction' (…) on the freedom of communication enshrined in article 11(1) of the Charter (…)."[517]

The early history of the right to confidentiality of communications illustrates the connection between that right and the right to freedom of expression. Nowadays the right to confidentiality of communications is regarded as a privacy-related right.[518] But when it was developed in the late eighteenth century, confidentiality of correspondence was seen as an auxiliary right to safeguard freedom of expression.[519] The right to confidentiality of communications in the e-Privacy Directive also applies to web browsing behaviour.[520]

Behavioural targeting firms collect information about people's online activities, which can include information that people don't want to disclose. Privacy as limited access captures this. Moreover, some tracking practices invades people's private sphere. For instance, a smart phone's location data could disclose where a person's house is, or where that person sleeps. Tracking that involves accessing information on people's devices can also interfere with privacy as limited access. The e-Privacy Directive's preamble discusses tracking technologies such as adware and cookies, and says that people's devices are private: "[t]erminal equipment of users of electronic communications networks and any information stored on such equipment are part of the private sphere of the users requiring protection under the European Convention for the Protection of Human Rights and Fundamental Freedoms."[521] Similarly, the

---

[517] Opinion AG Cruz Villalón, 14 April 2011, par 73 (for CJEU, C-70/10, Scarlet v. Sabam, 24 November 2011, Scarlet Sabam AG) (capitalisation adapted). The Advocate General is an independent advisor to the European Court of Justice (see article 252 of the consolidated version of the Treaty on the functioning of the EU).
[518] See for instance article 7 of the EU Charter of Fundamental Rights.
[519] Ruiz 1997, p. 67. See also ECtHR, Autronic AG v. Switzerland, No. 12726/87, 22 May 1990, par. 47.
[520] See chapter 6, section 4.
[521] Recital 24 of the e-Privacy Directive.

German Bundesverfassungsgericht says people have a "right to the guarantee of the confidentiality and integrity of information technology systems."[522]

Privacy as control and privacy as identity construction are also relevant when discussing chilling effects. For instance, the lack of individual control over data processed for behavioural targeting could aggravate the chilling effect. And if surveillance indeed influenced people's thoughts, it could constrain the development of their identity.[523] Regardless of how data are used at later stages, tracking people's behaviour (phase 1 of behavioural targeting) can cause a chilling effect. But data processing in later phases can worsen the chilling effect. For instance, a firm could find new information about a person by analysing the collected data.[524]

Lack of individual control over personal information

A second privacy problem regarding behavioural targeting is that people lack control over information regarding them. One aspect of the lack of individual control is information asymmetry. The online behaviour of hundreds of millions of people is tracked, without them being aware.[525] A visit to a website can lead to receiving dozens of tracking cookies from firms that people have never heard about. As Cranor notes, "it is nearly impossible for website visitors to determine where their data flows, let alone exert any control over it."[526]

Furthermore, people have scant knowledge about what firms do with data about them, and what the consequences could be. Personal data is auctioned off, shared and combined, without people being aware. "Users, more often than not, do not understand the degree to which they are a commodity in each level of this

---

[522] Bundesverfassungsgericht, 27 February 2008, decisions, vol. 120, p. 274-350 (Online Durchsuchung).
[523] Diaz & Gürses 2012.
[524] Schermer 2007, p. 136-137; Schermer 2013, p. 139.
[525] Hoofnagle et al. 2012, p. 291.
[526] Cranor 2012, p. 1.

marketplace."[527] If people don't even know who holds information about them, it's clear they can't exercise control over that information.

Firms rarely explain clearly what they do with people's data. Privacy policies often use ambiguous language, and don't help to make the complicated data flows behind behavioural targeting transparent. It's rare for people to have consented in a meaningful way to behavioural targeting. As discussed in more detail in chapter 7, people don't know enough about the complex data flows behind behavioural targeting to understand what they are being asked to consent to. And if firms ask consent, they often make using a service conditional on consent to tracking. Many people feel they must consent to behavioural targeting when encountering such take-it-or-leave-it choices.

Behavioural targeting can lead to experienced harms.[528] Data could be used in ways that harm people. For instance, a profile could be used to charge higher prices to a person. A health insurer might learn that somebody was reading about certain diseases, or about alcohol addiction. Furthermore, storing information about people is inherently risky. Data can leak, to insiders or outsiders. For instance, an employee might access the information stored by a firm. In one case, an internet firm's employee accessed information in user accounts, such as messages and contact lists.[529] Or a hacker or another outsider might obtain the data. 32 million user passwords were accessed at a firm that develops social media apps and runs an ad network.[530] And in the US, data brokers accidentally sold personal data to criminals.[531] A data breach could lead to spam, embarrassment, identity fraud, or other unpleasant surprises.[532]

---

[527] White House (Podesta J et al.) 2014, p. 41.
[528] See on experienced harms and expected harms Gürses 2010, p. 87-89; Calo 2011. See also section 3 of this chapter.
[529] Checn 2010.
[530] See about this data breach at RockYou: Hoffman 2011.
[531] For instance, US data broker Acxiom sold personal data about thousands of people to a criminal gang (Van der Meulen 2010, p. 76-77; 206-209). Experian also sold personal information to criminals (Krebs 2013).
[532] The harms can be diverse. In one case, a US data broker sold information to a stalker that used the information to locate and murder a woman (Remsburg v. Docusearch, Inc. 816 A.2d (N.H. 2003)).

Identity fraud can be costly for the victim, and for society as a whole – even without taking privacy interests into account.[533]

A general risk resulting from data storage is function creep: using data for other purposes than the original collection purpose.[534] For instance, commercial databases tend to attract the attention of law enforcement bodies.[535] People would protest a law requiring everyone to provide the police with lists of all of the websites they visit daily. But many behavioural targeting firms collect such data. And when the data are there, the police can demand access.[536] Firms like Facebook and Google, both using behavioural targeting, get many demands for police access.[537] Moreover, intelligence agencies could access data held by firms.[538] Schneier summarises: "[t]he primary business model of the Internet is built on mass surveillance, and our government's intelligence-gathering agencies have become addicted to that data."[539] The data that have been gathered for behavioural targeting can thus be used for new purposes. But also the technologies that have been developed for behavioural targeting could be used for new purposes. For instance, the National Security Agency (US) appears to have used tracking cookies of behavioural targeting firms to unmask users of the Tor anonymity service.[540] Using surveillance technologies for new purposes could be called "surveillance creep."[541]

---

[533] Van Den Hoven 1997. See on identity fraud ECtHR, Romet v. The Netherlands, No. 7094/06, 14 February 2012.
[534] Function creep can be seen as a breach of data protection law's purpose limitation principle (see chapter 4, section 3). See Dahl & Sætnan 2009.
[535] See the Data Retention Directive. See also Van Hoboken 2012, p. 324-325. Haggerty & Ericson 2000.
[536] Or, to take an example by Schneier "[i]magine the government passed a law requiring all citizens to carry a tracking device. Such a law would immediately be found unconstitutional. Yet we all carry mobile phones" (Schneier 2013a).
[537] See Google Transparency Report 2014; Facebook Government Requests Report 2014.
[538] See on state access to commercial data Soghoian 2012 (regarding the US); Brown 2012; Arnbak et al. 2013; Koning 2013. See also the special issue on systematic government access to private-sector data of the journal International Data Privacy Law, volume 4, issue 1, February 2014.
[539] Schneier 2013a. He's from the US, but his remarks are relevant for Europe too.
[540] See Reisman et al. 2014, with further references.
[541] See Marx 2005.

Apart from experienced harms, the lack of individual control over personal information can lead to the expectation of harm, or subjective harm.[542] People may vaguely realise that organisations hold data about them. Many people fear their information will be used, without their knowledge, for unexpected purposes.[543] A majority of Europeans doesn't trust internet companies such as search engines and social networks sites to protect their personal information.[544] The lack of control problem has an individual and a societal dimension. Information based harms, such as identity fraud, are costly both for victims and society as a whole.[545] For instance, the European Commission suggests that consumers' privacy anxieties hinder online business.[546]

In sum, transparency and individual control are lacking during every behavioural targeting phase. The ideal of privacy as individual control over personal information doesn't seem close to materialising in the area of behavioural targeting.

Social sorting

A third privacy risk resulting from behavioural targeting concerns social sorting and the risk of manipulation. Behavioural targeting enables what surveillance scholars refer to as social sorting.[547] In Lyon's words, social sorting involves "obtain[ing] personal and group data in order to classify people and populations according to varying criteria, to determine who should be targeted for special treatment, suspicion, eligibility, inclusion, access, and so on."[548] For example, an advertiser could use discounts to lure affluent people to become regular customers. But the advertiser might want to avoid poor people because they're less profitable. Or advertisers could

---

[542] Gürses 2010, p. 87-89; Calo 2011. See also section 3 of this chapter. The expectation of harm that results from a lack of individual control over personal data could also be called a chilling effect.
[543] European Commission 2011 (Eurobarometer), p. 146.
[544] European Commission 2011 (Eurobarometer), p. 138.
[545] The phrase "information based harms" is borrowed from Van Den Hoven 1997.
[546] European Commission proposal for a Data Protection Regulation (2012), p. 1. See also recital 5 of the e-Privacy Directive. From an economic perspective, information asymmetry is a societal problem because it's a type of market failure (see chapter 7, section 3).
[547] See chapter 1, section 3, for a description of surveillance studies.
[548] Lyon 2002a, p. 20. See on surveillance and marketing Pridmore & Lyon 2011.

target poor people with offers for certain products, such as predatory lending schemes.[549] Legal scholars tend to speak of discrimination when discussing social sorting.[550]

Firms classify people as "targets" or "waste", says Turow. "Marketers justify these activities as encouraging *relevance*. But the unrequested nature of the new media-buying routines and the directions these activities are taking suggest that *narrowed options* and *social discrimination* might be better terms to describe what media-buyers are actually casting."[551] The Dutch Data Protection Authority expresses similar concerns: "profiling can lead to stigmatisation and discrimination and to a society in which free choice has become illusory."[552] European Data Protection Authorities add that "[t]his may perpetuate existing prejudices and stereotypes, and aggravate the problems of social exclusion and stratification."[553]

Social sorting isn't a new phenomenon. By placing billboards for expensive cars in wealthy neighbourhoods, firms can target population segments based on location. Since the 1980s database marketing allows for segmentation on the individual level.[554] A book on database marketing explains that firms shouldn't treat all customers the same:

> Successful relationship marketing forces us to look at a new marketing fact of life. The buyer-seller relationship is not a democracy. All customers are not created equal. All customers are not entitled to the same inalienable rights, privileges, and

---

[549] To illustrate, one US firm sells an "Online Ad Network Direct Response Buyers Mailing List": "These responsive buyers have also expressed an interest in additional promotions, and 60% of these impulse buyers had their bank cards declined. (…) This self reported age 18+, third party verified database is perfect for subprime financial or credit repair offers. Gender, DOB, homeowner, marital status, income and a variety of other demographics are also available" (Mailing List Finder 2014).
[550] See Richards 2013, p. 1957-58.
[551] Turow 2011, p. 89. See also Dixon & Gellman 2014; White House (Podesta J et al.) 2014, p. 53; Barocas 2014.
[552] College bescherming persoonsgegevens, Annual report 2011, p. 2.
[553] Article 29 Working Party 2013, WP 203, p. 45.
[554] Gandy speaks of the "panoptic sort" (Gandy 1993).

> benefits. (…) That means some customers must earn "better treatment" than others, whatever that means. If you can't accept this undemocratic fact, quit reading and close the book, right now. Database relationship marketing is not for you.[555]

With behavioural targeting, marketers don't need people's names to classify them.[556] For instance, an advertiser that seeks wealthy customers could avoid a person whose cookie profile shows that he or she visits websites about credit card debt problems, or whose IP address shows that he or she is from a poor neighbourhood. And if a cookie shows that a peerson often hunts for bargains at price comparison sites, an advertiser might conclude the person is too careful with money to be a profitable customer. An advertiser could exclude that person from campaigns. Or advertisers could target people with more money. For instance, a firm called Bluekai offers an "auction marketplace for all audience data", where marketers can buy access to pseudonymous profiles of "high spenders."[557] Behavioural targeting makes social sorting easier and more effective: firms can categorise people as targets and waste, and treat them accordingly.

Manipulation

Some fear that behavioural targeting could be used to manipulate people. Broadly speaking, this study summarises two risks under the heading manipulation. First, personalised advertising could become so effective that advertisers have an unfair advantage over consumers. Second, there could be a risk of "filter bubbles" or "information cocoons", especially when behavioural targeting is used to personalise not only ads, but also other content and services.[558] In brief, the idea is that

---

[555] Newell 1997, p. 136.
[556] Turow 2011, chapter 4.
[557] Marketers can buy access to "high spenders", "suburban spenders" or "big spenders" (Bluekai 2010, p. 6-8). Bluekai says the profiles are "anonymous" (see e.g. Bluekai 2012). In 2014, BlueKai was acquired by Oracle (Oracle 2014).
[558] The phrases are from Pariser 2011 and Sunstein 2006.

personalised advertising and other content could surreptitiously steer people's choices.

Personalised ads could be used to exploit people's weaknesses or to charge people higher prices. Calo worries that in the future, firms could find people's weaknesses by analysing massive amounts of information about their behaviour: "digital market manipulation." With modern personalised marketing techniques, "firms can not only take advantage of a general understanding of cognitive limitations, but can uncover and even trigger consumer frailty at an individual level."[559] For example, a firm could target ads to somebody when he or she is tired, or easy to persuade for another reason. Firms could tailor messages for maximum effect. In short, firms could obtain an unfair advantage over people.[560]

Following the definition quoted in the last chapter, advertising is "designed to persuade the receiver to take some action."[561] Hence, advertising always aims to persuade or influence people. Persuading people could become unfair when targeted ads influence people too much. Zarsky gives an example of somebody who might become a vegetarian. The example is slightly adapted here. Suppose an ad network tracks the behaviour of Alice. The ad network analyses Alice's browsing behaviour, and applies a predictive model. Alice has never thought about becoming a vegetarian, but the model suggests that the person behind ID *xyz* (Alice) is statistically likely to become a vegetarian within 2 years. One firm starts targeting Alice with ads for steak restaurants. Another firm targets Alice with ads about the advantages of a vegetarian diet. Hence, firms could steer Alice's behaviour, while Alice isn't even aware of

---

[559] Calo 2013, p. 1. See also chapter 2, section 5.
[560] See on fairness chapter 4, section 4.
[561] Curran & Richards 2002. See chapter 2, section 7.

being influenced.[562] Scholars from various disciplines say that profiling changes the power balance between firms and individuals.[563] Data Protection Authorities agree.[564]

Behavioural targeting could be used for purposes beyond advertising. The risk of manipulation is greater when firms personalise not only advertising, but also other content and services. However, as noted, the line between advertising and other content is fuzzy on the web.[565] Zarsky speaks of the autonomy trap, "the ability of content providers to influence the opinions and conceptions of individuals by providing them with tailored content based on the provider's agenda and the individual's personal traits."[566] Zarsky argues that the autonomy trap is one of the main threats resulting from data mining. He calls it "a scary concept, portraying a frightening picture of a dysfunctional society."[567] However, in 2004 he didn't think behavioural targeting practices already brought this risk.[568]

In his book "Republic.com", Sunstein discusses risks from too much customised content.[569] He's mainly concerned about people locking themselves into "information cocoons" or "echo chambers", by only reading like-minded opinions.[570] He worries about user-driven personalisation (customisation) and not about media-driven personalisation (which happens without people's deliberate input).[571] But in later work Sunstein expresses similar worries about software personalising content

---

[562] Zarsky 2002, p. 40.
[563] See e.g. Schwartz & Solove 2009, p. 2; Gürses 2010, p. 51; Acquisti 2010a, p. 11; Purtova 2011, p. 42-43; Richards & King 2013. As noted above (under chilling effects), Lyon says surveillance always implies power relationships (Lyon 2001, p. 16).
[564] International Working Group on Data Protection in Telecommunications (Berlin Group) 2013, p. 7 (capitalisation adapted).
[565] See chapter 2 section 7. See about the distinction between editorial content and advertising Van Hoboken 2012 (chapter 10, section 3).
[566] Zarsky 2004, p. 30 (original footnote omitted). Zarsky borrows the phrase from Schwartz, but Zarsky defines it differently (see Schwartz 2002, p. 821-828).
[567] Zarsky 2002, p. 42. See on data mining chapter 2, section 5.
[568] Zarsky 2004, p. 46.
[569] Sunstein 2002.
[570] He describes "information cocoons" as "communication universes in which we hear only what we choose and only what comfort sus and pleases us" (Sunstein 2006, p. 9).
[571] The phrases user- and media-driven personalisation are used by Helberger 2013, p. 5-6. User-driven personalisation can be called customisation, and media-driven personalisation can be called personalisation (Treiblmaier et al 2004).

automatically.[572] He discusses two risks. First, citizens in a democratic society need to come across opinions that differ from their own opinions to fully develop themselves. People might drift towards more extreme viewpoints if they don't encounter opposing viewpoints. "Unplanned, unanticipated encounters are central to democracy itself."[573] Second, if everyone locked themselves in their own information cocoons, people might have fewer common experiences. But Sunstein says a diverse democratic society needs shared experiences as "social glue."[574] Along similar lines, the Council of Europe says public service media should promote "social cohesion and integration of all individuals, groups and communities."[575]

Pariser speaks of a filter bubble, "a unique universe of information for each of us."[576] Say a search engine personalises search results. The search engine's software learns that people who click on links to website X, are likely to click on links to website Y. Therefore, the software recommends website Y to people who click on links to website X. As a result, the search engine could mainly provide links to conservative news sites to somebody whose profile suggests that he or she is conservative. And the search engine could offer mostly results from left-leaning websites to a person categorised as progressive. If people think they see a neutral or complete picture, the search engine could narrow their horizon, without them being aware. Adverse effects of too much personalisation can occur accidentally. Hence, a filter bubble can occur when a firm doesn't aim to manipulate a person. Many authors share at least some of the concerns about filter bubbles and information cocoons.[577]

However, others are sceptical about the risks of personalisation.[578] The fear for filter bubbles leads to several questions. First, how much personalisation goes on? Research

---

[572] Sunstein 2013.
[573] Sunstein 2002, p. 9. See also Sunstein 2006.
[574] Sunstein 2002, p. 9.
[575] Council of Europe, Committee of Ministers, Recommendation CM/Rec(2007)3 of the Committee of Ministers to member states on the remit of public service media in the information society, 31 January 2007, article I.1(a).
[576] Pariser 2011, p. 9.
[577] See for instance Hildebrandt 2008a; Bozdag & Timmersmans 2011; Castelluccia & Narayanan 2012, p. 14; Oostveen 2012; Angwin 2014, p. 14-15; Lessig 2006 (chapter 11).
[578] See for instance McGonagle 2011, p. 198; Hoboken 2012, p. 286-287; p. 301; Jenkins 2008.

finds only limited personalisation in Google's search results.[579] Likewise, personalisation on news websites seems to be in its infancy.[580] But search engines do adapt search results to regions.[581] And one paper finds that watching extreme right videos on YouTube is likely to lead to recommendations for other extreme right videos.[582]

A second and more difficult question concerns the long-term effects of personalisation. Does personalised content really influence people and does it really harm our democracy? So far, there's little empirical evidence.[583] However, firms can influence people's emotions. For instance, Facebook published results of an experiment, which involved manipulating the user messages ("posts") that 689,003 users saw in their news feeds. "When positive expressions were reduced, people produced fewer positive posts and more negative posts; when negative expressions were reduced, the opposite pattern occurred."[584] Hence, Facebook succeeded in influencing the emotions of users.

Third, assuming that personalisation could deeply influence people, wouldn't the many possibilities to broaden one's horizon outweigh the effects of personalisation? For example, the web offers many kinds of unexpected content. In other words: how likely is it that the possible harm materialises? It appears that people do encounter information outside their own comfort zones.[585] And before the web became popular, people could lock themselves in their own echo chambers, by only choosing newspapers and radio stations that reinforced their existing opinions. In sum, it's unclear how much we should worry about filter bubbles at present. But problems

---

[579] Hannak et al. 2013.
[580] Thurman & Schifferes 2012; Turow 2011, p. 195. Moreover, as discussed in chapter 2, section 5, a predictive model for behavioural targeting might predict a click-through rate of 0.1 % to 0.5 %. Such models don't seem to enable very accurate personalisation.
[581] Hoboken 2012, p. 188.
[582] O'Callaghan et al. 2013.
[583] Van Hoboken 2012, p. 286; p. 301-302.
[584] Kramer et al. 2014.
[585] See e.g. Gentzkow & Shapiro 2011; LaCour 2014.

could arise in the future, whith further technological developments.[586] As previously noted, behavioural targeting could be seen as an early example of ambient intelligence: technology that senses and anticipates people's behaviour in order to adapt the environment to their inferred needs.[587]

In some contexts, undue influence would be more worrying than in others. The societal impact might be limited if behavioural targeting makes somebody buy a different brand of laundry detergent. But behavioural targeting in the context of elections raises more serious concerns. In the US, politicians use behavioural targeting. In principle, behavioural targeting would enable a political party to present each individual a personalised ad. In practice, it would make more sense to work less granularly. A political party could present itself as a one-issue party to each individual: "rhetorical redlining."[588]

By way of illustration, say a politician has a profile of Alice, identified by ID *xyz* in a cookie on her device. A predictive model says that the person behind ID *xyz* (Alice) probably dislikes immigrants. The politician shows Alice personalised ads, in which the politician promises to curtail immigration. The politician has a cookie-profile of Bob that suggests that Bob has more progressive views. The ad targeted to Bob says that the politician will fight discrimination of immigrants in the job market. The ad doesn't mention the politician's plan to limit immigration. Similarly, in ads targeted at jobless people, the politician mentions plans to increase the amount of money people on welfare receive every month. People whose profile suggests that their main concern is paying less tax, receive an ad stating that the politician will limit the maximum welfare period to six months. Hence, without technically lying, the politician could say something different to each individual. This doesn't seem to be a recipe for a healthy democracy.

---

[586] See Oostveen 2012.
[587] Hildebrandt 2010. See chapter 2, section 7.
[588] Turow et al. 2012, p. 7. See generally on behavioural targeting and profiling by politicians Barocas 2012; Bennett 2013; Kreiss 2012.

"Voter surveillance" is widespread in the US, says Bennett. He suggests that this can be partly explained by the absence of a general data protection law, and by the strong right to freedom of speech in the US. In Europe, data protection law limits the legal possibilities to obtain personal data.[589] However, it appears political parties in Europe look to the US practices: "candidates and political parties elsewhere have reportedly looked with great envy on the activities of their US counterparts and longed for similar abilities to find and target potential supporters and to ensure that they vote."[590]

The problems of unfair discrimination and manipulation surface in phase 5. A firm decides – or has software automatically decide – to show personalised ads or other content to a specific individual.[591] Other people are excluded because their profile suggests they won't become profitable customers. As long as the data aren't applied to an individual (phase 5), the sorting doesn't happen. But data analysis (phase 3) is a crucial step. For instance, a firm might discover that people who buy certain accessories for their cars are likely to default on payments. That model could be applied in phase 5, to deny someone credit.[592] Targeted advertising wouldn't be possible without collecting data. However, a firm could use data about one group of people to construct a predictive model, to apply that model to a person who isn't part of the group. Hence, while social sorting often involves processing vast amounts of information, a firm doesn't always need much information on the person to whom it applies the model.[593]

The perspective of privacy as the freedom from unreasonable constraints on identity construction fits well when discussing the risk of unfair social sorting and

---

[589] The Data Protection Directive provides for separate rules for political parties, which are less strict than for other data controllers (article 8(2)(d); recital 30 and 36). Nevertheless, the data protection regime probably reduces the amount of personal information that is available for political parties to obtain. See generally on data protection law chapter 4, section 2 and 3, and on personal data regarding political opinions chapter 5, section 7, and chapter 9, section 6.
[590] Bennett 2013.
[591] The Data Protection Directive has a separate provision for certain types of automated decisions (article 15) see chapter 9, section 6.
[592] See chapter 2, section 6.
[593] See chapter 2, section 3 and 5 on predictive modelling. See also chapter 5, section 3, and chapter 7, section 4 (on externalities).

manipulation. If personalised ads unreasonably influenced a person's choices, that person could be constrained in building his or her personality, or constructing his or her identity. And if an ad network compiles a profile of Alice, the ad network constructs an identity of Alice (her individual profile). Hence, it's not Alice who constructs that aspect of her identity. This could be seen as a constraint on Alice's freedom to construct her identity – and possibly an unreasonable constraint.[594]

The privacy as control perspective is also relevant for discrimination and manipulation. With fully transparent data processing and perfect individual control over behavioural targeting data, the risk of manipulation would be reduced. And some might find targeted ads more difficult to ignore than contextual advertising, and therefore more intrusive. If that were true, targeted ads could interfere with privacy as limited access.[595]

Social sorting as a privacy issue

People often use the word privacy to express unease about unfair treatment involving the use of personal data.[596] "Like it or not," says Bennett, "privacy frames the way that most ordinary people see the contemporary surveillance issues."[597] Some argue that social sorting and manipulation (in phase 5 of behavioural targeting) shouldn't be conceptualised as privacy problems. Koops says it's more a question of fairness: "why not call a spade a spade and say that in this respect, it is not so much privacy that is at stake, but fair judgement and equal treatment?"[598] Likewise, surveillance scholars often suggest that privacy isn't the right frame to discuss social sorting.[599]

---

[594] Diaz & Gürses categorise the problem of discrimination under privacy as identity construction (Diaz & Gürses 2012). See also Roosendaal 2013, p. 195; International Working Group on Data Protection in Telecommunications (Berlin Group) 2013, p. 5.
[595] See Füster et al. 2010. The Council of Europe also says intrusive online direct marketing advertising interferes with privacy (Committee of Ministers, Recommendation CM/Rec(2007)16 of the Committee of Ministers to member states on measures to promote the public service value of the Internet, V, 7 November 2007).
[596] See Bennett 2011a.
[597] Bennett 2011a, p. 495. See also Richards 2014a, p. 12, p. 28.
[598] Koops 2008, p. 329-330.
[599] See Lyon 2002a. See also Van Der Sloot 2011.

For this study it's not necessary to take sides in the debate on whether social sorting and manipulation should be discussed under the topic of privacy.[600] As noted, this study includes social sorting and the risk of manipulation in the category of privacy problems. But this study doesn't argue that such problems should *always* be categorised as privacy problems. In any case, the question "is this a privacy issue?" is a different question than "is this a serious threat?" Somebody might take the risk of unfair social sorting seriously, but not see it as a privacy problem. Apart from all that, the next chapter shows that while data protection aims to protect privacy interests, it also aims for fairness more generally when personal data are processed.[601]

3.4 Conclusion

This chapter discussed the privacy implications of behavioural targeting. Many people dislike behavioural targeting, because they find it creepy or privacy-invasive (see chapter 7).[602] This study classifies privacy perspectives into three groups: privacy as limited access, privacy as control over personal information, and privacy as the freedom from unreasonable constraints on identity construction. The three perspectives partly overlap, and highlight different aspects of privacy.

Privacy as limited access concerns a personal sphere, where people can be free from interference. The limited access perspective is similar to approaches of privacy as confidentiality, seclusion, or a right to be let alone. This perspective implies that too much access to a person interferes with privacy. For instance, if somebody wants to keep a website visit confidential, there's a privacy interference if others learn about the visit.

A second privacy perspective focuses on the control people should have over information concerning them. The privacy as control perspective is common since the

---

[600] See on this debate Bennett 2011a, and the reactions to that article in the Surveillance & Society journal.
[601] See chapter 4, section 3 and 4. See also chapter 9, section 6.
[602] See chapter 7, section 1.

1960s, when state bodies and other large organisations started to amass increasing amounts of information about people, often using computers. The control perspective has deeply influenced data protection law (see the next chapter).

Third, privacy can be seen as the freedom from unreasonable constraints on identity construction. This privacy as identity construction perspective highlights a concern regarding modern data processing practices in the digital environment such as profiling and behavioural targeting. There could be an interference with privacy if the environment manipulates somebody. The environment can include technology.

Each of three privacy perspectives can be recognised in the case law of the European Court of Human Rights. The Court interprets the right to privacy from the European Convention on Human Rights generously, and refuses to define the scope of the right. This living instrument doctrine allows the Court to apply the right to privacy in unforeseen situations and to new developments. The Court has held that monitoring somebody's internet usage interferes with privacy.

In the area of behavioural targeting, three of the main privacy problems are chilling effects, a lack of individual control over personal information, and the risk of unfair discrimination and manipulation. First, the massive data collection on user behaviour can cause chilling effects. Data collection can cause a chilling effect, regardless of how the data are used in later phases. People may adapt their behaviour if they suspect their activities are being monitored. For example, somebody who fears surveillance might hesitate to look for medical information, or to read about certain political topics.

Second, people lack control over information concerning them, and in the area of behavioural targeting individual control over personal information is almost completely lacking. As discussed in more detail in chapter 7, people don't know what information about them is collected, how it's used, and with whom it's shared. The feeling of lost control is a privacy problem. Apart from that, large-scale personal data

storage brings quantifiable risks. For instance, a data breach could occur, or data could be used for unexpected purposes, such as identity fraud.

Third, there's a risk of unfair discrimination and manipulation. Behavioural targeting enables social sorting: firms can classify people as "targets" and "waste", and treat them accordingly.[603] And some fear that behavioural targeting could be manipulative. Personalised advertising could become so effective that advertisers will have an unfair advantage over consumers. And there could be a risk of "filter bubbles" or "information cocoons", especially when behavioural targeting is used to personalise not only ads, but also other content and services.[604] The idea is that behavioural targeting could surreptitiously steer people's choices.

In sum, behavioural targeting raises privacy concerns from each of the three privacy perspectives. The next chapter turns to data protection law, the main legal instrument in the EU to protect privacy and related interests in the context of digital data processing.

* * *

[603] Turow 2011.
[604] The phrases are from Pariser 2011 and Sunstein 2006.