Improving privacy protection in the area of behavioural targeting

Zuiderveen Borgesius, F.J.

Publication date
2014
Document Version
Final published version

9 Improving protection

How could the law protect, rather than empower, the individual? The protective data protection principles should be enforced more strictly. But this won't be enough to improve privacy protection in the area of behavioural targeting. In addition to data protection law, more specific rules regarding behavioural targeting are needed. If society is better off if certain behavioural targeting practices don't take place, the lawmaker should consider banning them.

Section 9.1 discusses the strengths and weaknesses of data protection law's general rules with open norms, compared to more specific rules. Section 9.2 argues that more attention to protecting the individual wouldn't necessarily make the law unduly paternalistic. Section 9.3 discusses the data minimisation principle. Section 9.4 shows that the transparency principle can be read as a prohibition of surreptitious data processing. Section 9.5 concerns sensitive data and chilling effects. Section 9.6 discusses data protection law's provision on automated decisions. A conclusion is provided in section 9.7.

9.1 General and specific rules

If fully complied with, the data protection principles could give reasonable privacy protection in the area of behavioural targeting.[1707] But there are at least two problems with data protection provisions that aim to protect the data subject. First, as discussed

[1707] As discussed in chapter 4, section 5 and chapter 6, section 5, data protection law contains many protective rules. See also Bygrave 2002, who discusses the implication of the data protection principles for profiling and behavioural targeting (p. 334-362).

in the last chapter, compliance and enforcement are lacking.[1708] Second, a common complaint is that the Data Protection Directive uses too many general rules with open norms. The open norms can help to explain the lack of compliance, as discussed below.

Because the Data Protection Directive lays down an omnibus regime and aims to cover many different situations, it contains many general rules with rather open norms.[1709] The strength of this regulatory strategy is that the law doesn't leave many gaps. Open norms can be applied to unforeseen situations, for instance, when new technologies are developed. Open norms also allow firms to decide how to achieve compliance. For example, firms can choose the best technical solution to comply with data protection law's security principle.[1710]

But open norms also have weaknesses. Opens norms can make the law hard to apply for firms, hard to understand for data subjects, and hard to enforce for Data Protection Authorities. Phrases such as "fairly", "necessary", and "not excessive" leave ample room for interpretation.[1711] Basic definitions of data protection law are subject to significant discussion.[1712] It has been said about data protection law that "the unclear definitions of legal terms are a major problem, potentially the greatest problem."[1713]

The distinction between specific rules and general rules with open norms is a matter of degree rather than kind. Lawyers can find ambiguity in the most detailed and specific rules. Hence, a rule is always relatively general or relatively specific.[1714] Besides, the complicated nature of data protection law shouldn't be exaggerated. Data protection law gives a relatively objective checklist for firms. Data protection law can

---

[1708] See chapter 8 section 1.
[1709] See chapter 4, section 2. See also ECJ, C-101/01, Lindqvist, 6 November 2003, par. 83; CJEU, C-468/10 and C-469/10, ASNEF, 24 November 2011, par. 35.
[1710] Article 17 of the Data Protection Directive. See on the security principle chapter 4, section 2 and the references there.
[1711] Article 6(1)(a), 6(1)(c), and 6(1)(c) of the Data Protection Directive.
[1712] See chapter 5: even the scope of "personal data", the key term of data protection law, is hotly debated. See also chapter 4, section 2.
[1713] Zwenne 2013, p. 37. See also Zwenne at al. 2007; Winter et al. 2008p. 161-162.
[1714] Hesselink 2011, p. 639. See also Sunstein 1995.

be applied without engaging in discussions about the scope and meaning of privacy.[1715] Notwithstanding, many data protection provisions are rather general.

Using a phrase from regulation studies, parts of data protection law can be characterised as principles-based regulation.[1716] "In principles-based regulation," explain Baldwin et al., "principles are used to outline regulatory objectives and values, and regulatees are left free to devise their own systems for serving such principles."[1717] Principles-based regulation "is a method of encouraging regulatees to think for themselves and assume responsible approaches."[1718] This approach works best for trustworthy firms. "Central to the success of PBR [principles-based regulation] is, accordingly, trust in the competence and responsibility of the regulatees."[1719]

Firms and regulators come from different backgrounds, and have different ideas. Therefore, firms may have genuinely different interpretations of what is meant by an open norm, according to Baldwin et al. "Firms and regulators are liable to interpret regulatory requirements in divergent ways because they see the world differently – even if the regulatees are well-disposed and highly capable."[1720] For example, if a firm saw incorrectly targeted ads as a problem, it might disagree with regulators when data processing is "excessive."[1721] Cultural differences between countries can also play a role when interpreting open norms.[1722] Furthermore, firms may see an open norm as an invitation for discussion, instead of as a rule they must follow, say Baldwin et al.

[1715] See chapter 4, section 2, and De Hert & Gutwirth 2006, p. 94.
[1716] See Busch 2010, p. 9. See on regulation studies chapter 8, section 1.
[1717] Baldwin et al. 2011, p. 302.
[1718] Baldwin et al. 2011, p. 303.
[1719] Baldwin et al. 2011, p. 303.
[1720] Baldwin et al. 2011, p. 306. This study calls such firms well-intentioned and (well-)informed. See on the appropriate enforcement strategies for different types of firms chapter 8, section 1.
[1721] See section 3 of this chapter.
[1722] For instance, US firms might not see privacy and data protection rights as fundamental rights.

> Even if there is general agreement on the governing principles for a regime, the relevant group of regulatory actors may treat those principles not as a statement of objectives but as starting points for debates on substantive aims – debates that they engage in with different conceptions of the game being participated in and different understandings regarding key aspects of that game (such as what constitutes "compliance" or a "reasonable practice").[1723]

Indeed, in the behavioural targeting area, some firms appear to see data protection rules as a starting point for discussion, rather than as rules they have to comply with.[1724] To illustrate, the Interactive Advertising Bureau UK (IAB) says the e-Privacy Directive's consent requirement for tracking technologies should be implemented in a way "that leaves space for innovative new business models to develop."[1725] The IAB suggests that it can be assumed that people consent to tracking cookies if they don't change their browsers' default settings. It appears the IAB sees the requirements for valid consent as open norms.

Specific rules are easier to follow and to enforce than general principles. To borrow an example from Sunstein, the rule "don't drive faster than 120", gives more guidance than "don't drive unreasonably fast", or "don't endanger other road users."[1726] Specific rules also provide more predictability regarding enforcement. Moreover, the *lex certa* principle requires the law to clearly describe which activities can lead to penalties.[1727] This would be especially relevant if Data Protection Authorities were

---

[1723] Baldwin et al. 2011, p. 304.
[1724] Some firms might simply not care about data protection law, for example because they don't expect it will be enforced (see chapter 8, section 1).
[1725] Interactive Advertising Bureau United Kingdom 2012, p. 2. See also Stringer 2013, on the Interactive Advertising Bureau arguing for a lighter regime for pseudonymous data.
[1726] The first two examples are taken from Sunstein, and slightly rephrased (Sunstein 1995, p. 959).
[1727] See on the foreseeability of rules ECtHR, Sunday Times v. The United Kingdom, No. 6538/74, 26 April 1979, par. 49. See also Zwenne 2013, p. 35.

given the authority to impose large penalties.[1728] In sum, there are good reasons for using more specific rules.

The main weakness of specific rules is that they're less flexible than more general norms. For instance, sometimes driving 140 mph is perfectly safe, and sometimes 60 mph is too fast. A maximum speed of 100 mph doesn't reflect such nuances. Another downside of specific rules is the possibility of "creative compliance."[1729] A firm could comply with the letter of the law, while breaching the spirit of the law. Creative compliance sometimes occurs in the field of tax law for example.[1730] Baldwin et al. suggest the lawmaker can mitigate the risk of creative compliance by ensuring that general principles apply in the background.[1731] To stay with the traffic law example, the law can generally prohibit endangering other road users, in addition to specific rules such as maximum speeds.[1732]

As far back as 1994 Simitis argued that the Data Protection Directive should be supplemented with sector specific rules. "Omnibus regulations of data processing are merely a first step. The more specific the processing issues are, the less general rules help. Although they may indicate the direction to be followed, they do not specify solutions appropriate for particular processing contexts."[1733] Simitis concludes the European Union "must complete the Directive with a series of regulations focusing on particular processing issues", for instance for "research and statistics, marketing, and credit agencies."[1734] The Data Protection Directive's preamble says its principles "may be supplemented or clarified, in particular as far as certain sectors are concerned, by

---

[1728] See chapter 8, section 1.
[1729] Baldwin et al. 2011, p. 306.
[1730] Baldwin et al. 2011, p. 232.
[1731] Baldwin et al. 2011, p 305-306. Arguably such a relationship exists between the e-Privacy Directive and the general Data Protection Directive.
[1732] See for instance article 5.1 of the Dutch Road Traffic Act: "It is an offence for any road user to act in such manner as to cause a hazard (or a potential hazard) on the public highway or to obstruct other road users in any way." And as noted in chapter 4, section 4, the good faith requirement in contract law can be used if more specific contract law provisions leave a gap.
[1733] Simitis 1994 p. 466. See also De Hert & Gutwirth 2006, p. 102.
[1734] Simitis 1994, p. 467. See also Blume 2012 (p. 32-34) who discusses whether the public and the private sector should be subject to different data protection regimes.

specific rules based on those principles."[1735] But with the e-Privacy Directive as the major exception, there hasn't been much activity on this front.[1736] That said, there are many norms, legal and non-legal, that protect privacy in addition to data protection law. For instance, the medical profession has its own norms, while some countries have specific rules for CCTV.[1737]

In conclusion, the Data Protection Directive open norms are flexible, but this flexibility comes at a cost for legal certainty and clarity. If specific rules were adopted for behavioural targeting, the general data protection principles should continue to apply as well, to ensure that the law doesn't leave any gaps.

9.2 Mandatory rules and paternalism

This section discusses factors that the lawmaker can take into account when deciding whether to use more protective rules in addition to data protection law. The section also considers, and rejects, the idea that using mandatory protective rules would make the law unduly paternalistic.

The behavioural economics analysis in previous chapters shows that more protective rules are needed to improve privacy protection in the area of behavioural targeting. Several scholars have hinted at the need for prohibitions in privacy law, because they lost faith in informed consent.[1738] But when should the lawmaker use prohibitions? De Hert & Gutwirth discuss five factors that the lawmaker can take into account when choosing between general data protection law and stricter "opacity tools." As discussed in chapter 4, De Hert & Gutwirth distinguish data protection law, a "transparency tool", from more prohibitive "opacity tools", such as the legal right to

---

[1735] Recital 68 of the Data Protection Directive.
[1736] See on the e-Privacy Directive chapter 5, section 6, chapter 6, section 4, and chapter 8, section 4.
[1737] See on CCTV Hempel & Töpfer 2004.
[1738] See e.g. Barocas & Nissenbaum 2009; Solove 2013; Radin 2013; Sloan & Warner 2013; Tene & Polonetsky 2012. See generally about mandatory rules regarding privacy Allen 2011. It must be noted that US scholars are critiquing the US "notice and consent" regime, which, unlike data protection law, doesn't include many mandatory rules.

privacy in the European Convention on Human Rights. Opacity tools aim "to guarantee non-interference in individual matters."[1739] Some of the suggestions for stricter rules and prohibitions that are given below in this chapter can be defended on the grounds suggested by de Hert & Gutwirth.[1740]

Opacity tools are appropriate in the following circumstances, according De Hert & Gutwirth.[1741] First, the sanctity of the home, not only in a literal sense, should be protected. "People need places where they can rest and come to terms with themselves in a sphere of trust and security (…)."[1742] Second, opacity tools are "required when other firmly rooted (in tradition or in law) human rights are at stake, such as the right to have correspondence and the content of communication protected."[1743] These first two reasons to choose opacity tools thus are reminiscent of the perspective of privacy as limited access, or as confidentiality.[1744]

Third, De Hert & Gutwirth note that the Data Protection Directive contains some opacity tools, rules of a more prohibitive nature. An example given by the authors is data protection law's stricter regime for "special categories" of data, such as data regarding health or political opinions.[1745] A second example is data protection law's in-principle prohibition of certain automated decisions with far-reaching effects for the individual (see section 6 of this chapter). The authors suggest that the stricter rules regarding automated decisions and special categories of data can be explained by the risk of unfair social sorting, or "discriminatory effects."[1746]

[1739] De Hert & Gutwirth 2006, p. 66. See chapter 4, section 3.
[1740] See section 3 and 5 of this chapter.
[1741] De Hert & Gutwirth 2006, p. 101.
[1742] De Hert & Gutwirth 2006, p. 101.
[1743] De Hert & Gutwirth 2006, p. 101.
[1744] Web browsing is a form of "communication" according to the legal definitions in the EU telecommunications framework (see chapter 6, section 4).
[1745] Article 8 of the Data Protection Directive.
[1746] De Hert & Gutwirth 2006, p. 102. See also Bennett 2011a, p. 490-491.

Fourth, "a need for opacity can be drawn from the function of human rights in promoting and encouraging citizenship."[1747] The lawmaker should use opacity tools if data processing threatens the "formation of the free and equal citizen." This rationale could be extended: if data processing threatens values that are important for a democratic society, rules of a more prohibitive nature are needed. In general, De Hert & Gutwirth seem especially inclined to argue for opacity tools when, apart from individual interests, societal interests are at stake as well.[1748] Lastly, similar to Simitis, De Hert & Gutwirth call for opacity tools if data protection regulation leaves too much room for different interpretations.[1749] This mainly seems to be an argument for clear and specific rules, rather than for prohibitive rules.

If the data subject can override a rule by giving consent, this study doesn't see it as a prohibition. In the terminology of chapter 6, prohibitions are "mandatory", and rules that can be overridden with consent are "default rules."[1750] De Hert & Gutwirth don't limit their category of opacity tools to mandatory rules. For instance, the authors see the e-Privacy Directive's opt-in requirement for commercial email as an opacity tool, "which inherently implies the prohibition of unsolicited marketing mail unless the user makes an explicit request to receive it."[1751] Similarly, they see the data protection regime for special categories of data an opacity tool, even though in many member states the prohibition of processing can be overridden with explicit consent.[1752] This study classifies such opt-in requirements as default rules.

Paternalism

The previous chapter discussed ways to make consent more meaningful. If firms want to process personal data, and can't base the processing on the balancing provision or

---

[1747] De Hert & Gutwirth 2006, p. 102.
[1748] This line of reasoning is related to the economic concept of externalities (see chapter 7, section 3).
[1749] De Hert & Gutwirth 2006, p. 102.
[1750] See chapter 6, section 5.
[1751] De Hert & Gutwirth 2006, p. 95.
[1752] De Hert & Gutwirth 2006, p. 77. They note that the prohibition of processing special categories of data isn't absolute.

another legal basis, they must ask the data subject for consent. Hence, by default, certain data processing activities aren't allowed, but the data subject can change this default situation by consenting to processing.[1753] Such a default rule leaves the choice to the data subject. In contrast, mandatory rules can't be overridden with consent, and limit the data subject's contractual freedom. As discussed in chapter 6, paternalism involves, in short, limiting somebody's contractual freedom in order to protect that person.[1754] Therefore, unlike default rules, mandatory rules could be unduly paternalistic in some cases.[1755]

But using more mandatory rules that protect the data subject wouldn't necessarily make the law unduly paternalistic. A rule is purely paternalistic if it only aims at protecting people against themselves. But there are other rationales for legal privacy protection than protecting people against themselves. The right to privacy and the right to data protection aim to contribute to a fair society, which goes beyond individual interests.

Additionally, an economic argument can be made in favour of adopting mandatory rules in the area of behavioural targeting.[1756] As discussed, an economic analysis of informed consent to behavioural targeting suggests there are market failures, such as information asymmetry. It may be impossible to reduce the information asymmetry problem to manageable proportions.[1757] Reducing market failures has nothing to do with paternalism. Furthermore, using protective mandatory rules could be more efficient than giving people the choice to give or refuse consent. It would take people

---

[1753] Article 7(a) and 8(2)(a) of the Data Protection Directive. Data processing practices that aren't allowed without consent are, in short, those practices that can't be based on article 7(b)-7(f) of the Data Protection Directive.
[1754] See chapter 6, section 6.
[1755] Some scholars see default rules as mildly paternalistic (see for instance Sunstein & Thaler 2008).
[1756] See chapter 7, section 3 (on transaction costs).
[1757] See chapter 7 and 8.

several weeks a year to read all online privacy policies they encounter. The aggregate costs for society would be enormous.[1758]

Furthermore, the European Court of Human Rights requires protection of the right to private life that is "effective, not theoretical and illusory."[1759] Because behavioural research shows that data protection law's informed consent requirement is problematic in practice, more protective measures are needed to provide effective privacy protection.[1760] If informed consent requirements don't succeed in protecting privacy in the area of behavioural targeting, it's likely to affect millions of people.[1761] In addition, the current situation is that hundreds of millions of people are being tracked and profiled without being aware. As Hoofnagle et al. note, tracking millions of people without their consent could be seen as a unilateral intervention imposed by the marketing industry, without prior debate.[1762]

Moreover, bothering people dozens of times per day with choices that they don't understand doesn't empower them in any real sense. The time somebody spends on such choices can't be spent on pursuing other goals. "Time is limited," notes Sunstein, "and some issues are complex, boring, or both."[1763] In daily life, there are many decisions people don't have to worry about: "how best to clean tap water, or how to fly an airplane, or what safety equipment should be on trains."[1764] "If we did not benefit from an explicit or implicit delegation of choice-making authority, we would be far worse off, and in an important sense less autonomous, because we would have less time to chart our own course."[1765]

[1758] Expressed in money, in 2007 the cost of reading privacy policies would be around 781 billion dollars, while all online advertising income in the US was estimated to be 21 billion dollar. (Cranor & McDonald 2008).
[1759] ECtHR, Christine Goodwin v. the United Kingdom, No. 28957/95, July 11, 2002, par 74.
[1760] See chapter 7, section 3 - 6.
[1761] Radin suggests that the amount of people affected should be taken into account when regulating standard contract terms (Radin 2013, chapter 9).
[1762] Hoofnagle et al. 2012.
[1763] Sunstein 2013, p. 1884.
[1764] Sunstein 2013, p. 1884.
[1765] Sunstein 2013, p. 1884. See also Wagner 2010, p. 68.

Solove makes a similar point. "With the food we eat and the cars we drive, we have much choice in the products we buy, and we trust that these products will fall within certain reasonable parameters of safety. We do not have to become experts on cars or milk, and people do not necessarily want to become experts on privacy either."[1766] He adds: "many people do not want to micromanage their privacy. They want to know that someone is looking out for their privacy and that they will be protected from harmful uses."[1767]

It doesn't follow that we should outsource all our choices to the state.[1768] But the foregoing does suggest that, sometimes, prohibitions can give people more time to lead their lives. In sum, somewhat paradoxically, sometimes taking choices away from the individual with mandatory rules can foster real individual empowerment.[1769] It is, of course, necessary to arrange democratic legitimacy and sufficient checks and balances regarding the entity that sets the rules.[1770]

Nudging and using transaction costs strategically

Formally a mandatory rule can be distinguished from a non-mandatory default rule. But in practice the distinction isn't as hard as it may seem. Default rules can be "sticky", because many people stick with default options.[1771] As noted in the previous chapter, requiring opt-in consent for tracking could be seen as nudging.[1772] The lawmaker could also use an option in between mandatory and default rules: the strategic use of transaction costs.[1773]

[1766] Solove 2013, p. 1901.
[1767] Solove 2013, p. 1901.
[1768] To avoid misunderstandings: Solove and Sunstein don't suggest we outsource all our (privacy) decisions to the state. In fact, they seem more worried about legal paternalism than many European scholars (including me).
[1769] See along similar lines, in the context of contract law Mak 2008, p. 26.
[1770] As noted in chapter 1, section 4, a discussion of the democratic deficit of the EU falls outside the scope of this study.
[1771] Ayres 2012. See on the stickiness of defaults in the context of tracking Tene & Polonetsky 2012, p. 335.
[1772] Chapter 8, section 3.
[1773] Thanks for Oren Bar-Gill for suggesting this idea to me. See on the strategic use of transaction costs in the context of privacy and tracking Willis 2013a, especially p. 82-84, p. 122-128. See also Guibault, who suggests that

For example, the lawmaker could strengthen a nudge by adding transaction costs.[1774] Perhaps the lawmaker could require one mouse click for valid consent, if the consent concerns relatively innocuous types of tracking. The lawmaker could require three mouse clicks for more worrying practices. "Sticky defaults", says Ayres, "should be thought of as an intermediate category falling between ordinary defaults and traditional mandatory rules."[1775] Transaction costs could come in different shades, to introduce different degrees of stickiness for the default. In theory the law could require a thirty second waiting period, a phone call, or a letter by registered mail to opt in to certain practices.[1776]

The law does add friction to some decisions. For instance, formalities in contract law add transaction costs. Sometimes the law requires the involvement of a notary for a valid contract, for example when buying a house. And under Italian law, certain types of onerous contract clauses in standard contract terms must be signed separately.[1777] Data protection law requires "explicit" consent for the processing of special categories of personal data. About half of the member states require such explicit consent to be in writing.[1778] Some legally imposed transaction costs can be explained, at least in part, by the wish to reduce the chance of careless decisions. As noted, marketers are aware of the importance of transaction costs – and sometimes use them strategically. Opting out of behavioural targeting and other types of direct marketing

---

individually negotiated contracts regarding copyright involve more transaction costs than standard contracts, but could be regulated less strictly than standard contracts (Guibault 2002, p. 303).

[1774] If a nudge is made stronger by using transaction costs strategically, it might not count as a "nudge" anymore, since it's not "easy and cheap to avoid" (Sunstein & Thaler 2008, p. 6).

[1775] Ayres 2012, p. 2087 (including a helpful schedule).

[1776] See Ayres 2012, p. 2103. Ayres also gives more exotic examples. People could be required to answer a question before they can alter a default. "Will other corporations have the opportunity to purchase your mailing address and shopping information?" (p. 2077). See for a critique on the strategic use of transaction costs in the area of behavioural targeting Willis 2013a, p. 122-128.

[1777] Article 1341 of the Italian Civil Code (from 1942). See for a translation Gorla 1962, p. 2.

[1778] Article 8(2)(a) of the Data Protection Directive; Impact Assessment for the proposal for a Data Protection Regulation (2012), annex 2, p. 29. There are exceptions to the explicit consent requirement; see article 8(2)(b) - 8(5).

often takes more effort than opting in.[1779] In principle, the lawmaker could do something similar.

But caution is needed if the lawmaker considers adding friction to consent procedures in the area of behavioural targeting. A legal regime that adds transaction costs and allows firms to offer take-it-or-leave-it choices could lead to an unpleasant situation. Website publishers could use tracking walls, including if the lawmaker required three mouse clicks for consent.[1780] People would not enjoy clicking three times "I agree" if they want to visit a website, and accept they have to agree to tracking. With that caveat, the conclusion still stands: the distinction between mandatory rules and opt-in systems (default rules) isn't a black and white issue. In principle the lawmaker has a range of options.

To conclude, there are good reasons to supplement the general data protection regime with specific rules, or with prohibitions, in the area of behavioural targeting. Taking into account the limited potential of informed consent as a privacy protection measure, using mandatory rules doesn't imply undue paternalism.

9.3 Data minimisation

Many data protection provisions always apply, regardless of whether the data subject has consented to the processing. For instance, the data minimisation principle is mandatory. Several Data Protection Directive provisions express the data minimisation principle. For example, the amount of personal data must be "not excessive" in relation to the processing purposes. And firms must not keep data

---

[1779] See chapter 7, section 3.

[1780] Some website publishers impose transaction costs on visitors to improve advertising income. For instance, many websites cut articles in parts, so the reader has to click to reach the next part. Each click causes the website to refresh, which enables the website to display new ads.

"longer than is necessary" for the processing purposes.[1781] The European Data Protection Supervisor describes the data minimisation principle as follows.

> The principle of "data minimization" means that a data controller should limit the collection of personal information to what is directly relevant and necessary to accomplish a specified purpose. They should also retain the data only for as long as is necessary to fulfil that purpose. In other words, data controllers should collect only the personal data they really need, and should keep it only for as long as they need it.[1782]

Limiting the amount of data stored and shortening retention periods could mitigate some risks that are inherent to personal data processing. The vast scale of data processing for behavioural targeting aggravates chilling effects and the lack of individual control over personal information. And data storage brings risks, such as data breaches.[1783] Compliance with the data minimisation principle could mitigate such privacy problems.

Enforcing the data minimisation principle could also limit the amount of data that's available to construct predictive models.[1784] Predictive models based on the personal data of one group of people can be used to infer confidential information about people who weren't part of that group.[1785] Respect for the data minimisation principle limits the amount of information that firms can use for such practices. On the other hand, a lack of data can lead to incorrect predictive models, which in turn may cause unfair

---

[1781] Article 6(d) en article 6(e) of the Data Protection Directive. See for an overview of the data protection principles chapter 4, section 2.
[1782] European Data Protection Supervisor (Glossary). The Parliamentary Assembly of the Council of Europe stresses the importance of data minimisation in article 18(8) of its Resolution 1843 (2011) The protection of privacy and personal data on the Internet and online media, 7 October 2011.
[1783] See chapter 3, section 3.
[1784] See Hildebrandt et al. 2008, p. 245; Calo 2013, p. 44.
[1785] See chapter 2, section 5; chapter 7, section 3.

outcomes.[1786] For instance, an incorrect predictive model could say that a person is likely to default on credit, while more data might help to preclude such errors. This line of thought could lead to the conclusion that enough data should be available to create correct predictive models.[1787] But with behavioural targeting, the risks resulting from collecting too many personal data seem greater than the risks resulting from not having enough data to construct accurate predictive models. Besides, predictive models for behavioural targeting are rarely accurate. Accuracy in individual cases isn't the goal of behavioural targeting. A model can be useful for behavioural targeting if it correctly predicts that 0.5 % of the people who see an ad will click on it, if the click-through rate for untargeted ads is lower.[1788]

It follows from the structure of the Data Protection Directive that the data minimisation requirements from article 6 always apply, regardless of the legal basis for personal data processing in article 7 (such as consent or the balancing provision).[1789] In the words of the European Court of Justice: "all processing of personal data must comply, first, with the principles relating to data quality set out in article 6 of the directive and, secondly, with one of the criteria for making data processing legitimate listed in article 7 of the directive."[1790] A couple of national courts have ruled that data processing can be unlawful because it's disproportionate, even though the data subject has consented.[1791] As the Working Party puts it, "consent (…) is not a license for unfair and unlawful processing. If the purpose of the data processing is excessive and/or disproportionate, even if the user has consented, the [data controller] will not have a valid legal ground and would likely be in violation of

---

[1786] See Barocas 2014, chapter V.
[1787] See Schermer 2013, p. 147; Van Der Sloot 2013.
[1788] See chapter 2, section 5.
[1789] See on the relation between consent and the other data protection provisions chapter 6, section 5 and 6.
[1790] CJEU, C-131/12, Google Spain, 13 May 2014, par. 71 (capitalisation adapted). This could be different when an exception on the basis of article 13 of the Directive applies. See similarly ECJ, C-465/00, C-138/01 and C-139/01, Österreichischer Rundfunk, 20 May 2003, par, 65; CJEU, C-468/10 and C-469/10, ASNEF, 24 November 2011, par. 26.
[1791] Hoge Raad [Dutch Supreme Court], 9 September 2011, ECLI:NL:HR:2011:BQ8097 (Santander), English summary in Valgaeren & Gijrath 2011; Naczelny Sąd Administracyjny [Polish Supreme Administrative Court], 1 December 2009, I OSK 249/09 (Inspector General for Personal Data Protection), English translation: <www.giodo.gov.pl/417/id_art/649/j/en/> accessed 28 May 2014.

the Data Protection Directive."[1792] Scholars concur that consent can't legitimise disproportionate data processing.[1793]

A firm could try to argue it needs all the information it can get its hands on, because its processing purpose is targeting ads as precisely as possible. Or a firm could argue that collecting large amounts of data is "necessary" to build accurate predictive models. But it seems unlikely that judges or Data Protection Authorities would agree with such reasoning. Kuner has analysed how Data Protection Authorities apply the proportionality principle.[1794] He concludes that for data controllers, "the risk of legal problems caused by application of the proportionality principle can be particularly high" for some data processing practices. As an example he gives "the large-scale collection of data over the internet."[1795]

In its investigation of Google's 2012 privacy policy changes, the Working Party says that Google doesn't respect the data minimisation principle. "Google empowers itself to collect vast amounts of personal data about internet users, but Google has not demonstrated that this collection was proportionate to the purposes for which they are processed."[1796] The Working Party adds that "the Privacy policy suggests the absence of any limit concerning the scope of the collection and the potential uses of the personal data."[1797]

Few would probably argue that "excessive" personal data processing should be allowed. But when is data processing excessive? Acquisti argues for a strict interpretation of the data minimisation principle, although, being an economist rather than a data protection lawyer, he doesn't use the phrase data minimisation. According to Acquisti, firms should explain why they need personal data and why they can't

---

[1792] Article 29 Working Party 2013, WP 202, p. 16. See also Article 29 Working Party 2014, WP 217, p. 33.
[1793] Bygrave & Schartum 2009, p. 164; p. 166; Rouvroy & Poullet 2009, p. 73; Kosta 2013, p. 27; Gellert & Gutwirth 2013, 527; Dinant & Poullet 2006.
[1794] The principles of data minimization and proportionality are related. Kuner says "Proportionality has also led to creation of the concept of 'data minimisation' (Kuner 2008, p. 1618)
[1795] Kuner 2008, p. 1620 (capitalisation adapted).
[1796] Article 29 Working Party 2013 (Google letter), appendix, p. 7. See similarly CNIL 2014 (Google), p. 20-22.
[1797] Article 29 Working Party 2013 (Google letter), p. 1. See also the appendix, especially p. 4 and 7.

reach the same goal processing fewer data, for instance, by using privacy-preserving technologies. Like this, "the burden of proof for deciding whom and how should protect consumers privacy would go from *prove that the consumer is bearing a cost* when her privacy is not respected, to *prove that the firm cannot provide the same product*, in manners that are more protective of individual privacy."[1798] Acquisti concludes regulation may be needed to change the incentives for firms, to push them towards more privacy friendly practices.[1799]

A very strict interpretation of the data minimisation principle would imply that most data collection for behavioural targeting is prohibited. In principle, behavioural targeting would be possible without large-scale data collection, because behavioural targeting systems exist that don't involve sharing one's browsing behaviour with a firm. For example, a browser plug-in called Adnostic builds a profile based on the user's browsing behaviour, and uses that profile to target ads. Minimal information leaves the user's device, as the behavioural targeting happens in the browser. "The ad network remains agnostic to the user's interests."[1800] Mozilla is conducting research on a similar system for the Firefox browser.[1801] As behavioural targeting would be possible without large-scale data collection, it could be seen as "excessive" if firms collect large amounts of personal data for behavioural targeting. At present, the data minimisation principle is rarely interpreted as requiring such privacy-friendly behavioural targeting systems.

The lawmaker should consider making it more explicit, for instance in a recital, that consent can't legitimise disproportionate data processing. Such a recital could remind firms that the data subject's consent doesn't legitimise collecting personal data at will,

---

[1798] Acquisti 2010a, p. 43. See along similar lines Acquisti 2010b, p. 19-20.
[1799] Acquisti 2010b, p. 19-20; Acquisti 2010a, p. 43. Mayer & Narayanan 2013 arrive at a similar conclusion (p. 95-96).
[1800] Barocas et al. 2010. See also Castelluccia & Narayanan 2012, p. 16. See on privacy preserving analytics and click-fraud prevention Mayer & Narayanan (Donottrack.us website). See on click-fraud prevention also Soghoian 2011a.
[1801] Scott 2013.

and that Data Protection Authorities can intervene in the case of excessive data processing.

The European Commission proposal for a Data Protection Regulation makes the data minimisation principle more explicit. Personal data must be "limited to the minimum necessary in relation to the purposes for which they are processed; they shall only be processed if, and as long as, the purposes could not be fulfilled by processing information that does not involve personal data."[1802] This formulation allows for a stricter interpretation of the data minimisation principle. A proposal to modernise the Council of Europe's Data Protection Convention also provides inspiration. The proposal suggests adding the proportionality principle to the main principles of the Data Protection Convention, as follows: "[d]ata processing shall be proportionate in relation to the legitimate purpose pursued and reflect at all stages of the processing a fair balance between all interests concerned, be they public or private interests, and the rights and freedoms at stake."[1803]

Perhaps the law could prohibit storing data for behavioural targeting longer than a set period of, to give an example, two days. Such a hard and fast rule provides more legal certainty than general principles. Compared to estimating when the data minimisation principle requires deletion, complying with a maximum retention period of two days is easy. As noted, De Hert & Gutwirth call for specific rules if data protection regulation leaves too much room for different interpretations.[1804] However, limiting retention periods (phase 2) won't do much for people who think the tracking itself (phase 1) is the main problem, for instance, because of chilling effects. The most

---

[1802] Article 5(c) of the European Commission proposal for a Data Protection Regulation. Article 5(e) adds that data may not be kept longer than necessary. The LIBE Compromise text speaks of "data minimisation" and "storage minimisation" (article 5(c) and 5(e)). Article 6(1) the e-Privacy Directive is an example of a strict data minimisation requirement. Traffic data "must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication" (subject to exceptions).

[1803] Council of Europe, The Consultative Committee Of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data [ETS No. 108] 2012a, article 5(1). See on the proportionality principle chapter 4, section 2, and chapter 6, section 1 and 2.

[1804] See section 1 of this chapter.

effective way to reduce chilling effects is not collecting data (phase 1).[1805] As an aside, it's unclear whether storing tracking data for longer than a few days helps much to improve the click-through rate on ads.[1806]

9.4 Transparency

The transparency principle can be read as a prohibition of surreptitious data processing. Hence, while the last chapter discussed the transparency principle as a means to empower the individual, the principle could also be seen as more prohibitive. As the European Commission put it in 1992, the fair and lawful principle "excludes the use for example of concealed devices which allow data to be collected surreptitiously and without the knowledge of the data subject."[1807]

Data processing is only allowed if it's done in compliance with the transparency principle. Of course, firms are allowed to use sophisticated technology that's difficult to explain to people. A different interpretation of the transparency principle might make the whole internet illegal. But the Data Protection Directive requires the data controller to inform data subjects about its identity and about the processing purposes, and to give all other information that's necessary to guarantee fairness.[1808]

With some behavioural targeting practices, it would be hard for a website publisher to comply with the law's transparency requirements, even if it were to try its best. For example, some ad networks allow other ad networks to buy access to individuals (identified through cookies or other identifiers) by bidding on an automated auction.[1809] In such situations, the website publisher doesn't know in advance which ad networks will display ads on its site, and which ad networks will track its website

---

[1805] See along similar lines Diaz & Gürses 2012, p. 2-3.
[1806] See Strandburg 2013, p. 104-105.
[1807] European Commission amended proposal for a Data Protection Directive (1992), p. 15. See also European Agency for Fundamental Rights 2014, p. 76-78.
[1808] Article 10 and 11 of the Data Protection Directive (see chapter 4, section 3). Moreover, article 5(3) of the e-Privacy Directive requires "clear and comprehensive information" for the use of most tracking technologies (see chapter 6, section 4).
[1809] See on ad exchanges, real time bidding, and cookie synching chapter 2 section 6.

visitors. In data protection parlance: the publisher doesn't know who the joint data controllers are.[1810] Neither does the publisher know for which purposes the ad networks will use the data they collect.[1811] As noted, the Data Protection Directive obliges data controllers to provide a data subject information about their identity, the processing purpose, and all other information that's necessary to guarantee fair processing.[1812] Therefore, it's hard to see how the publisher could comply with the law's transparency requirements.

Some websites use phrases along the following lines in their privacy policies. "We or other companies may use cookies to suggest and deliver content which we believe may interest you."[1813] The Working Party doesn't accept such vague information: "[s]tatements such as 'advertisers and other third parties may also use their own cookies or action tags' are clearly not sufficient."[1814] Furthermore, a user's consent can't be specific and informed if a website can't explain to visitors for which ad networks it asks consent.[1815]

If it's indeed impossible for firms to comply with data protection law's transparency requirements, only one conclusion seems possible: the processing isn't allowed. As Blume notes, "it must be considered whether a lack of transparency should have consequences and maybe imply that data processing cannot take place."[1816] The lawmaker should consider making it more explicit that processing is prohibited, unless firms can comply with the transparency principle.

[1810] The Working Party says ad networks and website publishers are often joint data controllers, as they jointly determine the purposes and means of the processing. See Article 29 Working Party 2010, WP 171, p 11.
[1811] In principle, it's the firm operating the cookie (such as an ad network) that must obtain consent. But the Working Party says that a website publisher that allows third parties to place cookies shares the responsibility for information and consent. See chapter 6, section 4.
[1812] Art 10 and 11 of the Data Protection Directive (see chapter 4, section 3, and chapter 8, section 2). See also article 5(3) of the e-Privacy Directive.
[1813] This phrase is taken from the privacy policy of the Guardian (Guardian, privacy policy).
[1814] Article 29 Working Party 2010, WP 171, p. 18.
[1815] See on the requirements for valid consent chapter 6, section 3 and 4, and chapter 8, section 3 and 4.
[1816] Blume 2012, p. 32.

The transparency principle could also limit what firms can lawfully do with personal data. As noted, transparency about data processing can only be meaningful if the purpose limitation principle is complied with. The purpose limitation principle prohibits firms from using data for goals that the data subject can't expect, unless an exception applies.[1817] Some online marketing practices, such as selling copies of data to other firms, seem hard to reconcile with the purpose limitation principle. It would be difficult for the seller to ensure that the buyer doesn't use the data for unexpected purposes.

Transparency isn't only important to make personal data processing controllable for the individual. Transparency can also help to make data processing controllable for Data Protection Authorities and the lawmaker. Data protection law's transparency requirements can help to uncover problems that might call for regulatory intervention.[1818] Hence, also in cases when hard prohibitions are a better approach than data protection law, data protection law could still be useful in bringing problems to light that need the attention of policymakers.

9.5 Sensitive data

The mere collection of data about people's behaviour can have a chilling effect. For example, if people fear surveillance, they might refrain from looking for medical information on the web.[1819] Research confirms that people don't like it when information regarding their health is used for behavioural targeting.[1820] Many marketers seem to realise people's uneasiness with such practices, as some self-regulatory codes for behavioural targeting have stricter rules for data regarding health.[1821]

[1817] See chapter 4, section 3; chapter 8, section 2.
[1818] See chapter 4, section 3. See also Bennett 2011a, p. 491.
[1819] Behavioural targeting can be seen as a type of surveillance; see chapter 3, section 3.
[1820] See chapter 7, section 1, and Leon et al 2013. See on chilling effects chapter 3 section 3.
[1821] See for instance Direct Marketing Association (United States) 2014.

There's a long tradition of protecting personal data regarding health, as illustrated by the Hippocratic oath that requires doctors to keep patient information confidential. Medical secrecy protects individual privacy interests of patients, and a public interest: the trust in medical services.[1822] The European Court of Justice confirms that the right to privacy "includes in particular a person's right to keep his state of health secret"[1823] The Court adds that protecting health data is important for the individual, and for society's trust in health services.[1824] The European Court of Human Rights uses similar reasoning:

> The protection of personal data, in particular medical data, is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life as guaranteed by Article 8 of the Convention. Respecting the confidentiality of health data is a vital principle in the legal systems of all the Contracting Parties to the Convention. It is crucial not only to respect the sense of privacy of a patient but also to preserve his or her confidence in the medical profession and in the health services in general.[1825]

Furthermore, processing special categories of data can lead to unfair treatment. If a cookie representing somebody says that person is in the "lesbian, gay, bisexual, and transgender" category,[1826] or the "handicapped" category,[1827] the person could be

---

[1822] Ploem 2004, p. 129-133.
[1823] European Union Civil Service Tribunal, Civil Service Tribunal Decision F-46/095, V & EDPS v. European Parliament, 5 July 2011, par. 163.
[1824] European Union Civil Service Tribunal, Civil Service Tribunal Decision F-46/095, V & EDPS v. European Parliament, 5 July 2011, par 123.
[1825] I. v. Finland, App. No. 25011/03, 17 Jul. 2008, par. 38. See along similar lines Z v. Finland (9/1996/627/811) 25 February 1997, par. 95.
[1826] Flurry (audiences). Flurry is firm offering analytics and advertising for mobile devices. Among the demographic data that advertisers can select, Flurry lists "race" (Flurry, factual).
[1827] Rocket Fuel, Health Related Segments 2014.

discriminated against on this basis, even if no name is tied the cookie.[1828] Likewise, a cookie profile could be used for unfair discriminatory practices, if the profile says somebody is poor, rich, or from a certain neighbourhood, and decisions are based on that profile.[1829] And if a name is tied to the information, it could lead to embarrassment or worse if the information leaks.[1830]

Does data protection law's regime for health-related personal data (a "special category of data") apply to behavioural targeting?[1831] As discussed in chapter 5, many firms operate in a grey area. Much depends on the type of behaviour that firms track, and how they use that information.[1832] An ad network that tracks daily visits to website with kosher recipes could conclude that somebody is Jewish. Ad networks don't have an interest in harming people on the basis of sensitive information. Ad networks aim to increase the click-through rate on ads. For an ad network the topic of the website that somebody visits is of little relevance, as long as a correlation can be found between a visit to that website and clicking on certain ads.[1833] On the other hand, there are ad networks that enable advertisers to advertise to people based on special categories of data.[1834] Some ad networks use interest categories such as "arthritis", or "cardiovascular general health."[1835]

Case law suggests that the phrase "special categories of data" must be given a wide interpretation.[1836] Hence, tracking on websites with medical information should probably be seen as the processing of "data concerning health or sex life." Such

---

[1828] It appears an US data broker also sold addresses of people in the "rape victims" category (Hill 2013a).
[1829] Non-discrimination law might apply to some discriminatory practices. See section 6 below.
[1830] See on data breaches regarding health related data I. v. Finland, App. No. 25011/03, 17 Jul. 2008, par. 38.
[1831] See article 8 of the Data protection Directive.
[1832] See chapter 5, section 6.
[1833] See Van Hoboken 2012, who arrives at a similar conclusion regarding search engines (p. 332).
[1834] Assuming that behavioural targeting entails personal data processing.
[1835] Yahoo! Privacy. See also the interest category "lesbian, gay, bisexual, and transgender" highlighted previously in this section.
[1836] ECJ, C-101/01, Lindqvist, 6 November 2003, par. 50: "the expression 'data concerning health' (…) must be given a wide interpretation." This suggests that special categories of data generally must be interpreted generously (see Bygrave 2014, p. 167). The Office of the Privacy Commissioner of Canada, applying PIPEDA, the Canadian equivalent of data protection law, concluded that "Google is delivering tailored ads in respect of a sensitive category, in this case, health" (Office of the Privacy Commissioner of Canada (Google) 2014).

tracking is thus prohibited, or only allowed after obtaining the data subject's explicit consent.[1837] The privacy risks involved in using health data for behavioural targeting outweigh the possible societal benefits in allowing such practices. Therefore, the EU lawmaker should consider prohibiting the use of any data regarding health for behavioural targeting, whether the data subject gives consent or not.[1838]

Data protection law's regime for special categories of data can be criticised for being too data-centred. As Nissenbaum notes, sensitivity often depends on the context, rather than on the type of data.[1839] Say a website offers information about diseases. The website publisher allows an ad network to track the website visitors. In theory, the ad network could only record that a person (or the cookie with ID *xyz*) visited a website in the Netherlands, and disregard it's a website about health problems. But even if the ad network doesn't collect or infer special categories of data, a chilling effect could occur if people expect that visits to health websites are tracked.

Therefore, the lawmaker should consider whether prohibitions are needed in certain contexts. Such prohibitions have been suggested. For instance, the European Consumers' Organisation says tracking on health related websites should be prohibited.[1840] A difficult question would be how to phrase such prohibitions in a way that doesn't make them over or under inclusive. How to define "health related websites"? Is it enough if the website presents itself as a health related website, for instance by including a picture of a doctor in a white coat? And would a prohibition of using any "health data" for behavioural targeting also cover tracking of daily visits to a website with gluten free recipes? And which rules should cover smart health apps? Furthermore, legal limits on the use of health related data shouldn't unnecessarily hamper socially beneficial processing practices. For instance, rules shouldn't unduly

---

[1837] See article 8 of the Data Protection Directive.
[1838] See for a similar idea Turow 2011, p. 200. As noted, some member states have chosen not to allow people to override the prohibition of processing special categories of data with explicit consent. See chapter 5, section 6.
[1839] Nissenbaum 2010. See in detail on sensitive data (from a US perspective) Ohm 2014.
[1840] European Consumer Organisation BEUC 2013, p. 8. See also Willis 2013a, p. 87.

hinder medical practice or scientific research. In sum, drafting and agreeing on prohibitions would be hard. But that shouldn't be a reason to ignore this legal tool.

Politics

A second example of chilling effects that can result from behavioural targeting concerns reading about politics online.[1841] People might refrain from reading about certain political opinions or topics if they fear surveillance. People may have an individual interest in keeping their political views confidential, and in not having others drawing the wrong conclusions about their political opinions. Somebody might visit a website about communism or extreme right wing ideas out of curiosity, or because of strong disagreement. There's also a societal interest in respecting the confidentiality of political opinions. In a democratic society people are expected to vote, and arguably they should be able to inform themselves without fear of surveillance. It's widely accepted that information about people's political opinions deserves protection.[1842]

The freedom to receive and impart information protects individual interests and the common good. Article 10 of the European Convention on Human Rights says the right to freedom of expression includes the freedom to receive information and ideas without interference by public authority. The Court emphasises the role of freedom of expression for a democratic society. "Freedom of expression constitutes one of the essential foundations of such a society, one of the basic conditions for its progress and for the development of every man."[1843] Furthermore, "the public has a right to receive information of general interest"[1844] and "the internet plays an important role in enhancing the public's access to news and facilitating the sharing and dissemination

---

[1841] See chapter 2, section 5, and chapter 3, section 1 and 3.
[1842] See on the processing of personal data regarding one's political opinion ECtHR, Rotaru v. Romania, No. 28341/95, 4 May 2000. There's also a tradition of secret voting. See Jacobs 2011.
[1843] ECtHR, Handyside v. the United Kingdom, No. 5493/72, 7 December 1976, par. 49. See on the function of freedom of expression also Van Hoboken 2012, chapter 4.
[1844] ECtHR, Társaság a Szabadságjogokért v. Hungary, No. 37374/05, 14 April 2009, par. 26. See for an overview of case law on the right to receive information (with a different focus than this study) Herr 2011; Hins & Voorhoof 2007.

of information generally (…)."[1845] Article 10 doesn't merely require states to refrain from interfering with the right to freedom of expression. States may have to take action: "the genuine and effective exercise of freedom of expression under Article 10 may require positive measures of protection, even in the sphere of relations between individuals."[1846] The International Covenant on Civil and Political Rights is phrased in stronger terms than the European Convention on Human Rights, and also protects the right to "seek" information.[1847]

News services

Neither article 10 of the Convention, nor the related case law, grants a right not to have one's browsing behaviour monitored. But arguably the values underlying freedom of expression imply that people should be able to read the news without fear of undue surveillance.[1848] Helberger emphasises the value of news services for a democratic society, and questions whether tracking walls on such services are acceptable.

> [T]here might be situations in which policymakers might decide that the acceptance of profiling and targeting is not an acceptable price at all, comparable e.g. to the existing prohibition on the sponsoring on news or religious programs. Taking e.g. into account the particular importance that news content has for political participation and democratic life, and argument could be made that in order to avoid chilling effects

---

[1845] ECtHR, Fredrik Neij and Peter Sunde Kolmisoppi (The Pirate Bay) v. Sweden, No. 40397/12, 19 February 2013 (inadmissible), capitalisation adapted.
[1846] ECtHR, Khurshid Mustafa v. Sweden, No. 23883/06 16 March 2009, par. 32.
[1847] Article 19(2) of the International Covenant on Civil and Political Rights.
[1848] Richards makes a similar point in the US context (Richards 2008, p. 428).

> people should never been required to accept tracking of their news consumption.[1849]

Furthermore, if somebody wants to read one source (website A), another source (website B) may not be a valid alternative for that person. As Helberger puts it, "media is speech, and when consuming media content it does matter who the speaker is. Accordingly, turning away and/or listening to another speaker is not necessarily an option."[1850]

The Audiovisual Media Services Directive prohibits sponsoring for news programmes.[1851] That prohibition only applies to television broadcasting and comparable moving images, so it doesn't apply to news websites with only text and pictures.[1852] Nevertheless, the rule shows that specific regulation for marketing in the context of news services wouldn't be a novelty. As De Hert & Gutwirth suggest, prohibitive rules are an appropriate response when data processing threatens important values for a democratic society.[1853] A chilling effect is hard to prove empirically.[1854] But if a chilling effect occurred in relation to reading about politics, it would threaten the democratic society.[1855] Furthermore, processing information about people's medical conditions or political opinions brings the risk of discrimination.

A full prohibition of any third party tracking on news services may be too blunt an instrument. For instance, it would be hard to define the scope of the ban. Would the ban apply to political blogs and to online newspapers that only gossip about

---

[1849] Helberger 2013, p. 18.
[1850] Helberger 2013, p. 12.
[1851] Article 10(4) of the Audio Visual Media Services Directive. "News and current affairs programmes shall not be sponsored." See along similar lines article 18(3) of the European Convention on Transfrontier Television. See for commentary Kabel 2008, p. 640.
[1852] Recital 28 of the Audio Visual Media Services Directive.
[1853] De Hert & Gutwirth 2006, p. 101-102. See section 2 of this chapter.
[1854] A survey by Cranor & McDonald 2010 suggests behavioural targeting has a chilling effect, but the research concerns declared (not revealed) preferences. A survey among 520 writers in the US finds many writers self-censor their work because they fear surveillance by intelligence agencies (PEN America 2013). Another study analysed Google search results, and suggests people "were less likely to search using search terms that they believed might get them in trouble with the U. S. government" (Marthews & Tucker 2014).
[1855] See chapter 3, section 3.

celebrities? And such a ban could lower the advertising income for news websites, at least in the short term. It wouldn't make sense if a rule that aims to ensure that people feel free to read about politics causes news services to go bankrupt. However, as discussed, in the long run behavioural targeting might decrease ad revenues for some website publishers.[1856]

The lawmaker should consider separate rules for tracking on websites of public service media, such as public broadcasters. The Council of Europe says public service media should promote democratic values, and should offer "universal access."[1857] In many European countries public service broadcasters receive public funding.[1858] Some public service broadcasters expose website visitors to third party tracking. For example, people could only access the website of the Dutch public broadcaster if they "consented" to tracking by various third parties. According to the Dutch Data Protection Authority, the universal access requirement implies that the broadcaster shouldn't make website visitors "pay" again with their personal data.[1859] Helberger concurs:

> It is (…) at least questionable whether in a situation in which access to the website is made conditional upon the acceptance of cookies, the website is still accessible for everyone. Very much will depend on whether users will find this too high are price, taking also into account that these contents have already been financed with public money.[1860]

[1856] See chapter 2, section 1 and 6, and chapter 7, section 2.
[1857] 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. See on public service media McGonagle 2011, chapter 4.
[1858] See on this topic European Commission 2009 (State Aid).
[1859] College bescherming persoonsgegevens (Dutch DPA) 2013 (NPO). See also chapter 6, section 3 and 4, and chapter 8, section 3 and 5. See on "paying" with personal data chapter 7, section 2.
[1860] Helberger 2013, p. 20 (internal reference omitted).

This study agrees with this line of reasoning. The lawmaker should prohibit public service broadcasters to make the use of their services dependent on consent to third party tracking. Such a prohibition shouldn't be limited to websites. For instance, certain types of digital television also enable tracking for behavioural targeting.[1861] The lawmaker should consider banning all personal data collection for behavioural targeting and similar purposes on public service media – at least when third parties collect the data.[1862]

Public sector websites

More generally, people should be able to visit important government websites without exposing themselves to tracking by third parties. As noted, under current law tracking walls and similar take-it-or-leave-it choices are prohibited if people must use a website, because the consent wouldn't be "free."[1863] For instance, say people are required to file their taxes online. If the tax website had a tracking wall that imposes third party tracking, people's consent to tracking wouldn't be voluntary. The EU lawmaker should consider make it explicit that public sector websites shouldn't offer visitors take-it-or-leave-it choices regarding commercial tracking.[1864]

Apart from the question of whether people are required to use a website, it's questionable whether it's appropriate for public sector bodies to allow third party tracking for commercial purposes on their websites – even if people consent. If a website is funded by the state, people paid for that website through taxes. It's hard to see why the state should facilitate tracking for commercial purposes on public sector websites. In practice, public sector websites might use third party widgets such as

---

[1861] See College bescherming persoonsgegevens (Dutch DPA) 2013 (TP Vision); Hessische Datenschutzbeauftragte (Data Protection Authority Hesse, Germany) 2014.
[1862] Data use by third parties tends to be riskier and less transparent than data use by the website publisher.
[1863] See chapter 6, section 3 and 4, and chapter 8, section 3 and 5.
[1864] For instance, the EU lawmaker could state that in a recital regarding consent in data protection law, or regarding (the successor of) article 5(3) of the e-Privacy Directive. Data analytics for fraud prevention may be necessary for some public sector websites.

social media buttons.[1865] The website publisher might not realise that the inclusion of such code exposes visitors to privacy-invasive tracking.[1866] The lawmaker could consider banning any third party tracking for commercial purposes on public sector websites. The exact scope of such a ban would require further debate.[1867] At the time of writing, in the Netherlands a bill to amend the implementation law of the e-Privacy Directive is being discussed, that contains, in short, a prohibition of tracking walls on public sector websites.[1868]

Traffic and location data

For traffic data and for location data, the e-Privacy Directive has specific rules, which resemble the rules for special categories of data in the Data Protection Directive.[1869] But the rules on traffic and location data only apply to providers of publicly available electronic communications services, such as internet access providers or phone operators – telecommunication providers for short.[1870] Telecommunication providers may only process traffic and location data with the user's consent, unless a specified exception applies.[1871] Hence, telecommunication providers can't rely on the balancing provision for processing such data.[1872] But many firms, such as ad networks and providers of smart phone apps, process more traffic and location data than telecommunication providers. The scope of the regime for traffic and location data

---

[1865] To illustrate: Van Der Velden found third party tracking on 60% of a set of Dutch governmental websites she examined (Van Der Velden 2014).
[1866] Using the taxonomy of chapter 8, section 1, the website publisher may be well-intentioned but ignorant. As an aside: websites can include "greyed out" buttons, which don't track people unless people click on the button to activate the button, for instance to "like" a page (see Schmidt 2011; Schneier 2013b).
[1867] For instance, what to do about organisations that are partly funded by the state? And some (first party) tracking could be necessary for website security purposes.
[1868] Proposal to amend the Telecommunicatiewet (Telecommunications Act): Eerste Kamer, vergaderjaar 2014–2015, 33 902, A <www.eerstekamer.nl/wetsvoorstel/33902_wijziging_artikel_11_7a> accessed 17 November 2014.
[1869] See for traffic data article 5 and article 6, and for location data article 9 of the e-Privacy Directive. See chapter 5, section 6.
[1870] An "electronic communications service" is, in short, a service that consists wholly or mainly in the conveyance of signals on electronic communications networks (article 2(c) of the Framework Directive 2002/21/EC (amended in 2009)). It's thus a transmission service.
[1871] See article 5(1) and 6 (traffic data) and article 9 (location data) of the e-privacy Directive. The e-Privacy Directive distinguishes users from subscribers. This distinction isn't further explored in this study.
[1872] See on article 7(f) of the Data Protection Directive, the balancing provision chapter 6, section 2.

must probably be broadened. Traffic and location data are sensitive, and deserve extra protection – also when they are processed by firms other than telecommunication providers.

The lawmaker should consider introducing specific rules for using traffic and location data for behavioural targeting. Hence, such rules would focus more on the processing purpose than on the type of firm.[1873] Some scholars suggest that using traffic and location data shouldn't be allowed at all in some situations: "location-based services should not even offer the option (to minors) to share their location with third parties and/or use it for behavioural tracking purposes."[1874] As these authors note, specific rules regarding tracking children may be needed.[1875]

In conclusion, strictly enforcing the existing rules on special categories of data could reduce privacy problems such as chilling effects. For instance, if they fear surveillance people might be hesitant to look for medical information on the web, or to read about politics on the web. As chilling effects can result from the collection context, the lawmaker should consider additional rules that focus on the context, rather than on the data type. For example, the lawmaker should consider banning third party tracking for behavioural targeting on public service media.

9.6 Automated decisions

"Data processing may provide an aid to decision-making, but it cannot be the end of the matter; human judgment must have its place," said the European Commission in 1992.[1876] This is the rationale for article 15 of the Data Protection Directive, the provision on automated decisions. Article 15 is based on the French Data Protection Act from 1978, which prohibits automated court decisions. The French Act also

---

[1873] It could be called a functional approach if the lawmaker focuses on the purpose of behavioural targeting, rather than on certain types of firms (see, in a different context Arnbak 2013a).
[1874] Ausloos et al. 2012, p. 25. See also Turow 2011, p. 200.
[1875] As noted in chapter 1, section 4, the question of whether special privacy rules are needed for children falls outside this study's scope. See on such issues Van Der Hof et al. 2014.
[1876] European Commission amended proposal for a Data Protection Directive (1992), p. 26.

prohibits other automated decisions with legal effect for the individual, unless a specified exception applies.[1877] Article 15 of the Data Protection Directive, sometimes called the Kafka provision, could be seen as an in-principle prohibition of certain fully automated decisions with far-reaching effects. The analysis below mainly relies on literature, because the provision hasn't been applied much in practice.[1878]

The Directive's provision on automated decisions applies to data processing by firms, and by the state. Within the private sector, the provision applies to a wide range of activities, such as credit scoring.[1879] The provision doesn't concern the legal basis for collecting data. Hence, in principle firms that gather personal data to use for automated decisions, could base such collection on various legal bases, including consent and the balancing provision.[1880] The main rule of the Directive's provision on automated decisions is as follows:

> Member States shall grant the right to every person not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc.[1881]

In short, people may not be subjected to certain automated decisions with far-reaching effects. The Directive says a person has "the right not to be subject to" certain

---

[1877] Article 10, Loi Informatique Et Libertes [Act on Information Technology, Data Files and Civil Liberties] (Act N°78-17 Of 6 January 1978), last amended 17 March 2014: "No court decision involving the assessment of an individual's behaviour may be based on an automatic processing of personal data intended to assess some aspects of his personality." See Korff 2010b, p. 24-27; Kabel 1999, p. 281-282.
[1878] See Korff 2012, p. 26.
[1879] See European Agency for Fundamental Rights 2014, p. 117. Certain public sector activities are outside the Directive's scope. See chapter 4, section 2.
[1880] See on the legal basis requirement for data processing chapter 6.
[1881] Article 15(1) of the Data Protection Directive.

decisions.[1882] But literature suggests this implies an in-principle prohibition of such decisions.[1883] Several countries emphasise the prohibitive character of the provision in their implementation laws. For instance, the Austrian act says that "nobody shall be subjected to" such decisions.[1884] Other countries phrased it less strictly.[1885]

Does article 15 apply to behavioural targeting? Four conditions must be met for the provision to apply, says Bygrave. Slightly rephrased, the conditions are as follows: (i) There must be a decision, (ii) that decision is based solely on automated processing of data, (iii) the data used for the decision are intended to evaluate certain personal aspects of the person concerned, and (iv) the decision must have legal or other significant effects for the person.[1886] With behavioural targeting, an algorithm decides to show the right ad at the right time to the right person, based on analysing that person's behaviour. Data processed for behavioural targeting are "intended to evaluate certain personal aspects" about a person. Therefore, the first three conditions are met.[1887] The fourth condition requires the decision to have "legal effects", or to "significantly" affect the person.

An automated court decision would be an example of a decision with legal effect. The Belgian Data Protection Authority suggests that a targeted ad that includes "a reduction and therefore a price offer" has legal effect as well.[1888] Presumably, the Authority sees a price offer as an invitation to enter an agreement, which could indeed be seen as having a legal effect. This interpretation would make article 15 applicable

---

[1882] Article 15 uses the phrase "every person", rather than "data subject." Some suggest article 15 also applies if a firm can't identify a person about whom it makes an automated decision. See Konarski et al. 2012, p. 34.
[1883] Korff 2012 (p. 26) and De Hert & Gutwirth 2008 (p. 283) see article 15 as an in-principle prohibition. But see Bygrave 2001, who suggests that the provision might allow the automated decisions if the data subject doesn't object. See also Hildebrandt 2012, p. 50.
[1884] Article 49(1) of the Datenschutzgesetz of Austria. See also article 17(1) of the Personal Data Protection Act in Estonia, and article 12bis of the Data Protection Act in Belgium.
[1885] See for instance the Data Protection Act in Portugal (article 13), in Spain (article 13), and in Norway (article 22 and 25).
[1886] Bygrave 2002, p. 320. See for a similar analysis with three conditions: European Commission amended proposal for a Data Protection Directive (1992), p. 26.
[1887] Bygrave 2002, p. 320. See also International Working Group on Data Protection in Telecommunications (Berlin Group) 2013, p. 6.
[1888] Commission for the Protection of Privacy Belgium 2012, par. 80. See also Vermeulen 2013, p. 12.

to certain types of price discrimination.[1889] From here on, this chapter focuses on decisions that "significantly" affect people, rather than on decisions with "legal effects."

The Data Protection Directive doesn't explain when a decision "significantly" affects a person. But it seems questionable whether one targeted ad falls within the scope of an automated decision that "significantly affects" a person within the meaning of article 15. However, Bygrave argues that in some cases behavioural targeting – "cybermarketing" as he referred to it in 2002 – can have significant effects, for example if a firms charges higher prices to somebody, or denies somebody access to a service:[1890]

> For instance, a cybermarketing process could be plausibly said to have a significant (significantly adverse) effect on the persons concerned if it involves unfair discrimination in one or other form of "weblining" (e.g., the person visiting the website is offered products or services at a higher price than other, assumedly more valuable customers have to pay, or the person is denied an opportunity of purchasing products/services that are made available to others).[1891]

It's dubious whether one targeted ad should generally be seen as an automated decision with significant effects in the sense of article 15. Somebody might not even notice the ad. In many cases, receiving one single targeted ad probably doesn't lead to

---

[1889] See on price discrimination chapter 2, section 7, chapter 8, section 2, and chapter 9, section 7.
[1890] Bygrave 2002, p. 323-324. Church & Millard note: "[t]here is no further definition of a "significant effect", though it is very unlikely that this would be limited to decisions having a pecuniary effect" (Church & Millard 2010, p. 84). See on the vagueness of "significant effect" also Article 29 Working Party 2012, WP 191, p. 14.
[1891] Bygrave 2002, p. 323-324 (punctuation adapted, internal footnote omitted). The word "weblining" refers to "redlining", where city areas are used as a proxy to discriminate people based on race (Stepanek 2000). See critically on that phrase Zarsky 2002, p. 35.

an effect for the individual that should be regarded as "significant" in the sense of article 15.

Behaviourally targeting as a *practice* does have significant effects for society and for individuals. For instance, large-scale data collection can lead to chilling effects, and people lack control over what happens to their data. Furthermore, the very point of advertising is to change views, attitudes, actions, and behaviours over time.[1892] Thus, in aggregate, behavioural targeting may well significantly affect someone.

It could also be argued that one targeted ad should generally be seen as a decision that "significantly affects" somebody in the sense of article 15. One could focus less on the effects of one automated decision on the individual, and more on the effects of automated decisions generally on individuals and society. Following that line of reasoning, article 15 can be triggered *because* behavioural targeting as a practice has significant effects.[1893]

In sum, the text of article 15 seems to suggest that the provision only applies if one specific automated decision significantly affects an individual. The correct interpretation of the provision must come from the courts. But, as noted, so far the provision hasn't been applied much in practice.

Exceptions to the in-principle prohibition

For this study, there are two relevant exceptions to the in principle prohibition of automated decisions with significant effects, which are summarised now.[1894] First, an automated decision is allowed when it "is taken in the course of the entering into or performance of a contract, provided the request for the entering into or the

---

[1892] See on the privacy implications of behavioural targeting chapter 3.
[1893] See generally Hildebrandt 2012.
[1894] A third exception isn't discussed here, because of its limited relevance for behavioural targeting. An automated decision is allowed if it's authorised by a law that includes measures to safeguard the data subject's legitimate interests (article 15(2)(b) of the Data Protection Directive).

performance of the contract, lodged by the data subject, has been satisfied."[1895] For instance, an insurance firm might use software to decide whether or not it will offer people an insurance contract. The provision allows such an automated decision if it leads to offering somebody a contract, because the person's request to enter a contract has been met.[1896]

Second, firms are allowed to automatically refuse to enter a contract with somebody, if "there are suitable measures to safeguard his legitimate interests, such as arrangements allowing him to put his point of view."[1897] Hence, a firm that uses software to automatically deny somebody an insurance contract could ensure that the person can ask a human to reconsider the decision. This makes it trivial for a firm, such as an insurance company, to comply with the provision.[1898] It might be enough if the insurance company included a phone number on the website, where people can ask a human to reconsider the automated decision to deny the insurance contract.

For many types of unfair social sorting the provision offers little help.[1899] Suppose an ad network refrains from showing certain ads to people who visited a price comparison website, or to people whose IP address suggests that they are from a poor neighbourhood. Those people may not realise the ad network excludes them from the campaign. Therefore, it's difficult to challenge the decision. Likewise, the provision doesn't help much to reduce the risk of filter bubbles and manipulation.[1900] One automated decision to personalise a website might not "significantly" affect a person within the meaning of article 15; and therefore the decision may remain outside the provision's scope.[1901] However, as noted in the previous chapter, data protection law could help to make personalisation more transparent – including if article 15 doesn't

---

[1895] Article 15(2)(a) of the Data Protection Directive.
[1896] In any case, somebody probably wouldn't object to an automated decision, if the decision were in the person's favour. See Kabel 1996, p. 281. But see Bygrave 2002, p. 327.
[1897] Article 15(2)(a) of the Data Protection Directive.
[1898] Article 15 doesn't require the firm to amend the criteria for the decision. Bygrave 2002, p. 324; Rubinstein 2013, p. 6.
[1899] See on social sorting chapter 3, section 3.
[1900] See on filter bubbles chapter 3, section 3.
[1901] Article 15(1) of the Data Protection Directive.

apply. After all, firms are required to disclose the processing purpose, and this requirement also applies when the purpose is personalising content.[1902]

The Data Protection Directive grants the data subject the right to learn the underlying logic of an automated decision with significant effects.[1903] Hence, an insurance firm that denies somebody a contract based on an automated decision must explain the logic behind that decision, if the person who was denied the contract requests so. For instance, the firm could explain why the software denied the insurance contract, and which factors were taken into account. In some cases the right to ask for the decision's logic could help the data subject, but there are several reasons not to expect too much from this right.

First, the provision on automated decisions is hardly ever applied in practice. Second, the person has to ask for the information. Hence, if somebody isn't aware of an automated decision, the provision is of little help. For instance, if an ad network only shows an offer to certain people, a person who doesn't receive the offer is probably unaware of being excluded. Third, the Directive's recital 41 limits the right to learn the logic behind the automated decision. The right "must not adversely affect trade secrets or intellectual property."[1904] A firm might claim it can't fully explain an automated decision, because that would disclose too much about the software it uses. However, the recital doesn't allow the firm to refuse all information: "these considerations must not (…) result in the data subject being refused all information."[1905] The issue isn't merely theoretical. Facebook has invoked the recital to limit information it gives to people who exercised their right to access.[1906]

[1902] Article 10 and 11 of the Data Protection Directive. See chapter 4, section 3, and chapter 8, section 2.
[1903] Article 12(a) of the Data protection Directive. The right to ask the logic behind an automated decision can be characterised as a rule that aims to empower the data subject by granting her a right. But the rule is discussed in this chapter, because of its relevance for the automated decisions provision.
[1904] Recital 41 of the Data Protection Directive. See about the legal effect of recitals chapter 6, section 4.
[1905] Recital 41 of the Data Protection Directive.
[1906] Facebook invoked article 4(12) of the Irish Data Protection Act, which is based on recital 41. See Hildebrandt 2011, p. 3-4; Europe versus Facebook 2014.

Data Protection Regulation proposals

The European Commission proposal for a Data Protection regulation amends the provision on automated decisions. Article 20 of the proposal is called "measures based on profiling."[1907] The main rule is similar to the one in the Data Protection Directive: in principle a person should not be subjected to measures based on profiling that significantly affect him or her:

> Every natural person shall have the right not to be subject to a measure which produces legal effects concerning this natural person or significantly affects this natural person, and which is based solely on automated processing intended to evaluate certain personal aspects relating to this natural person or to analyse or predict in particular the natural person's performance at work, economic situation, location, health, personal preferences, reliability or behaviour.[1908]

The provision's second paragraph says profiling measures with significant effects are only allowed if an exception applies. The exceptions are similar to those in the Data Protection Directive. But a new exception is introduced. A profiling measure with significant effects is allowed if people give their consent, and if there are suitable safeguards.[1909] The proposal thus introduces yet another default rule that can be overridden with consent.[1910]

It's unclear to what extent the proposed provision applies to behavioural targeting. As the Belgian Data Protection Authority notes, it's "not easy to determine whether

---

[1907] Article 20 of the European Commission proposal for a Data Protection Regulation.
[1908] Article 20(1) of the European Commission proposal for a Data Protection Regulation (2012).
[1909] Article 20(2)(c) of the European Commission proposal for a Data Protection Regulation (2012). The text of article 20(2)(c) isn't very clear. The European Commission might mean that *consent* is subject to suitable safeguards. But presumably the Commission means suitable safeguards to protect the data subject's interests.
[1910] See on the distinction between default rules and mandatory rules chapter 6, section 5.

profiling for direct marketing purposes in the form of specific advertising messages is part of the scope of this article."[1911] The Authority adds that the provision ought to apply: "this kind of profiling should be subject to the specific conditions set out in article 20."[1912]

The European Commission proposal prohibits profiling measures that are based only on special categories of data. "Automated processing of personal data intended to evaluate certain personal aspects relating to a natural person shall not be based solely on the special categories of personal data."[1913] This prohibition also applies to profiling measures that don't "significantly affect" a person.[1914] But the prohibition has a narrow scope, as it concerns measures that are based "solely" on special categories of data. Some firms use special categories of data for behavioural targeting.[1915] However, the prohibition doesn't apply as long as a firm also uses non-special personal data. This is generally the case, so the rule seems to be a dead letter. Regardless of whether the profiling provision applies, a firm needs the data subject's explicit consent for processing special categories of data for behavioural targeting.[1916]

Presumably the aim of preventing unfair discrimination is one of the rationales for the prohibition of profiling measures based solely on special categories of data. But the prohibition fails to take into account that measures based on profiling could also lead to unfair discrimination if no special categories of data are used. For instance, non-special personal data could be used to generate special categories of data. Or non-special personal data could end up being used as a proxy for special categories of

---

[1911] Commission for the Protection of Privacy Belgium 2012, par. 80. See also Information Commissioner's Office 2013; Federation of European Direct and Interactive Marketing (FEDMA) 2013, p. 3.
[1912] Commission for the Protection of Privacy Belgium 2012, par. 80.
[1913] Article 20(3) of the European Commission proposal for a Data Protection Regulation (2012).
[1914] Article 20(3) doesn't mention "significant effects", and doesn't refer to another article that mentions "significant effects."
[1915] See section 5 of this chapter and chapter 5, section 6.
[1916] Like the 1995 Directive, the European Commission proposal for a Data Protection Regulation (2012) allows member states to decide that special categories of data can't be processed on the basis of explicit consent (article 9(1) and 9(2)(a)).

data. As Korff notes, automated decisions could "reinforce societal inequality" and have discriminatory effects, even if only prima facie innocuous data are used.[1917]

> Crucially, this discrimination-by-computer does not rest on the use of overtly discriminatory criteria, such as race, ethnicity or gender. Rather, discrimination of members of racial, ethnic, national or religious minorities, or of women, creeps into the algorithms in much more insidious ways, generally unintentionally and even unbeknown to the programmers. But it is no less discriminatory for all that.[1918]

For example, a bank could use software to deny credit to people who live in a particular neighbourhood, because many people in that neighbourhood don't repay their debts. If primarily immigrants live in that neighbourhood, such profiling measures might discriminate against immigrants, by accident or on purpose. But such practices wouldn't be covered by the prohibition of profiling measures based solely on special categories of data. Similarly, the software could deny credit to somebody who lives in a poor neighbourhood, even though that person always repays his or her debts.

Following a suggestion by Korff and several civil rights organisations, the European Parliament proposes to prohibit profiling measures that have the effect of discriminating on the basis of special categories of data, intentional or not.[1919] "Profiling that has the effect of discriminating against individuals on the basis of race or ethnic origin, political opinions, religion or beliefs, trade union membership, sexual

---

[1917] Korff 2012, p. 18.
[1918] Korff 2012, p. 22-23 (emphasis original, enter omitted). See also White House (Podesta J et al.) 2014, p. 45-47; p. 51-53; Article 29 Working Party 2013, WP 203, p. 47; p. 59; p. 61; Siegel 2013, p. 62-65; Calders & Žliobaitė 2013. See in detail on data mining (and profiling) and discrimination Barocas 2014.
[1919] Korff 2012, p. 37; Bits of Freedom 2012; EDRi (European Digital Rights) 2014 (less explicitly).

orientation or gender identity, or that results in measures which have such effect, shall be prohibited. (…)"[1920]

A topic for further research is where non-discrimination law and data protection law overlap, and where the two fields could usefully supplement each other.[1921] One important difference is that data protection law applies as soon as personal data are collected or otherwise processed. In contrast, non-discrimination law becomes relevant in later phases: when there's a difference in treatment of a person or a group.[1922] Furthermore, many non-discrimination rules only apply to certain protected grounds, such as sex, sexual orientation, disability, age, race, ethnic origin, national origin, and religion or belief.[1923] Hence, non-discrimination law may be less effective to combat discrimination against, for instance, people who live in poor neighbourhoods.[1924]

The profiling provision in the European Commission proposal adds a new transparency requirement to data protection law's general transparency requirements. In short, a firm must tell the person concerned that it takes a profiling measure with significant effect, and must inform the person about the measure's envisaged effects.[1925] This rule obliges a firm to inform the data subject about profiling measures, including if the person hasn't asked for it.[1926] This is an improvement in comparison with the Data Protection Directive's provision, which only requires firms

---

[1920] Article 20(3) of the LIBE Compromise, proposal for a Data Protection Regulation (2013). In his draft report, Rapporteur Albrecht had proposed to prohibit all profiling that includes or generates special categories of data (Draft Albrecht report, amendment 162, article 20(3)).

[1921] As noted, non-discrimination law falls outside the scope of this study. There are still many open questions regarding the interplay of data protection law and non-discrimination law. See on this topic Hildebrandt et al. 2008; De Vries et al. 2013. See generally on discriminatory effects of profiling Zarsky et al. 2013; Barocas 2014. See generally on non-discrimination law in Europe: European Agency for Fundamental Rights 2010a.

[1922] Using the five phases of data processing that were distinguished in chapter 2, non-discrimination law would apply to phase (5), but not to earlier phases.

[1923] Hildebrandt et al. 2008; De Vries et al. 2013.

[1924] See chapter 2, section 5. It's possible, for instance, to infer whether people are likely to default on credit based on their shopping behaviour.

[1925] Article 20(4) of the European Commission proposal for a Data Protection Regulation (2012).

[1926] Article 20(4) refers to article 14, and article 14 suggests a requirement of proactive transparency. Nevertheless, there's some debate on the question of whether a firm must proactively provide this information, or whether it only has to provide information upon request (Hildebrandt 2012, p. 51; Rubinstein 2013, p. 7).

to give information about automated decisions upon request.[1927] But it's only a minor improvement. The main problem is that the new transparency requirement only applies to profiling measures that "significantly affect" a person.[1928] Hence, the new transparency requirement probably wouldn't apply to most targeted ads, or to personalised websites.[1929] Furthermore, the new transparency obligation doesn't require firms to provide information about the logic involved in the profiling measure.[1930] And as discussed, merely ensuring that firms offer transparency isn't enough to empower people in any real sense.

Like the Data Protection Directive, the European Commission proposal contains a general right of access. Data subjects have the right to obtain information about the processing of their data from a firm.[1931] In the proposal such information must include "the significance and envisaged consequences of such processing, at least in the case of measures [based on profiling] referred to in article 20."[1932] Unlike the Directive, the European Commission proposal doesn't grant people the right to ask for the logic involved in the profiling measure.[1933]

The new transparency requirement should be amended, to improve privacy protection. A firm should inform people about profiling measures, also when no legal or

---

[1927] Article 12(a) of the Data Protection Directive. The Directive does have a general transparency requirement in article 10 and 11.

[1928] Article 20(4), containing the transparency requirement, refers to "the cases referred to in paragraph 2." Paragraph 2 refers to "measures of the kind referred to in paragraph 1." Paragraph 1 speaks of "a measure which produces legal effects concerning this natural person or significantly affects this natural person (…)." Korff is critical of the new transparency provision (Korff 2012, p. 33).

[1929] But see the discussion of article 15 of the Data Protection Directive above in this section.

[1930] See article 12(a) of the Data Protection Directive.

[1931] Article 15 of the European Commission proposal for a Data Protection Regulation (2012).

[1932] Article 15(1) (h) of the European Commission proposal for a Data Protection Regulation (2012). It's unclear what the European Commission means by the "significance" of profiling measures. (Korff 2012, p. 33.)

[1933] Recital 51 of the European Commission proposal for a Data Protection Regulation (2012) suggests that data subjects have the right to learn the logic behind profiling measures, but the recital is oddly phrased, as it speaks of a right to know "the logic of the data that are undergoing the processing" (see Korff 2012, p. 33). There are more references to profiling in the proposal. For instance, firms must carry out a data protection impact assessment if profiling is "systematic and extensive" (article 33(2)(a)). The preamble suggests that children shouldn't be subjected to measures based on profiling (recital 58). The Commission can adopt delegated acts regarding the suitable measures to safeguard the data subject's interests (article 20(5)).

significant effects are foreseen.[1934] The provided information should include an explanation of the logic behind profiling measures. The requirement could be coupled with a reasonable, and not too broadly phrased, exception for trade secrets etc.[1935] Such transparency requirements could reduce the risk of filter bubbles or manipulative practices enabled by behavioural targeting.[1936] A firm that personalises ads or other content should be transparent about the personalisation. For instance, a website could include a button that leads to an explanation of why and how a website is personalised. While transparency requirements are not a panacea to protect privacy and fairness, such requirements could be helpful.[1937]

Scholars call for the development of TETs, transparency-enhancing technologies, to enable meaningful transparency regarding profiling.[1938] Such technologies should "aim at making information flows more transparent through feedback and awareness thus enabling individuals as well as collectives to better understand how information is collected, aggregated, analyzed, and used for decision-making."[1939]

The European Commission proposal's profiling provision "was not warmly welcomed by representatives from the direct marketing and the online advertising industry."[1940] The American Chamber of Commerce, a business lobbying organisation, says it would be best to get rid of the rules on profiling.[1941] "At minimum, the Regulation should make clear that the restrictions on profiling do not extend to beneficial activities such as fraud prevention, service improvement, and marketing/content customization."[1942] The Interactive Advertising Bureau UK and the Federation of

---

[1934] This is required in article 14(1)(ga) of the LIBE Compromise, proposal for a Data Protection Regulation (2013).
[1935] See Korff 2012, p. 33-34; Bits of Freedom 2012.
[1936] See on the risk of manipulation resulting from behavioural targeting chapter 3, section 3.
[1937] Apart from helping data subjects, legal transparency requirements can help regulators and policymakers to assess industry practices. See chapter 4, section 3.
[1938] See for instance Hildebrandt & Gutwirth (eds.) 2008; Hildebrandt 2012. See also Bozdag & Timmersmans 2011.
[1939] Diaz & Gürses 2012, p. 3-4.
[1940] Vermeulen 2013, p. 12.
[1941] International Chamber of Commerce 2013, p. 2.
[1942] International Chamber of Commerce 2013, p. 2.

European Direct and Interactive Marketing (FEDMA) say profiling measures should be allowed on an opt-out basis, similar to the regime of the balancing provision.[1943]

While data protection rules regarding profiling could protect people against some forms of unfair social sorting, other social sorting practices remain outside the ambit of data protection law.[1944] For example, advertising that isn't targeted at individuals can have an effect that resembles social sorting through behavioural targeting. Predatory lending schemes or junk food could be advertised on a website that's visited primarily by poor people. If ads are adapted to the website rather than to individuals, it concerns a form of contextual advertising rather than behavioural targeting.[1945] Data protection law doesn't apply if people aren't singled out or otherwise identified. If social sorting through contextual ads is – or becomes – a problem, the lawmaker will have to seek a solution outside data protection law.

9.7 Conclusion

This chapter discussed how the law could improve protection of the individual, rather than empowerment. To start with, better enforcement of the current rules is needed. Many data protection provisions are mandatory; they always apply, regardless of whether the data subject has consented to the processing. If the data protection principles were fully complied with, they could give reasonable privacy protection in the area of behavioural targeting.

For example, it follows from the Data Protection Directive that excessive data processing isn't allowed, not even after the data subject's consent. Other data protection principles can defend privacy interests as well, also after somebody

---

[1943] Interactive Advertising Bureau United Kingdom 2012a; Federation of European Direct and Interactive Marketing (FEDMA) 2013, p. 4-5. As noted in chapter 6, section 2, the LIBE Compromise, proposal for a Data Protection Regulation (2013), allows, under certain circumstances, profiling based on the balancing provision. But the LIBE Compromise requires consent for profiling that has legal effects or significantly affects a person, unless a specified exception applies.
[1944] See Gürses 2010, p. 49; p. 55.
[1945] See chapter 2, section 1 and 3.

consents to processing. For instance, the purpose limitation principle and the security principle always apply. However, many provisions of the Data Protection Directive are rather general, and leave ample room for discussion. It's thus useful that the European Commission proposal for a Data Protection Regulation phrases some data protection principles more explicitly. But enforcing and tightening the data protection principles won't suffice to protect privacy in the behavioural targeting area. Additional rules are needed.

Article 5(3) of the e-Privacy Directive could be seen as a sector-specific rule for behavioural targeting, which supplements the general data protection regime.[1946] But article 5(3) requires too much, and at the same time, doesn't require much. On the one hand, article 5(3) is too blunt. The provision is over inclusive, as it also requires consent for certain innocuous types of cookies that pose few privacy threats. On the other hand, article 5(3) isn't very strict, as it merely obliges firms to obtain the individual's informed consent for the use of tracking cookies and similar technologies. Article 5(3) doesn't say much about the processing that takes place after a firm obtained consent for storing or accessing information on a user's device. Hence, the provision is mainly relevant for phase 1 of the behavioural targeting process (data collection). But, as far as personal data are processed, data protection law does regulate the processing after consent for the use of tracking technologies.

As noted in the previous chapter, it might be better if the lawmaker phrased the consent requirement for behavioural targeting in a more technology neutral way than article 5(3) of the e-Privacy Directive. The law could require consent for processing personal data, including pseudonymous data, for behavioural targeting and similar purposes – regardless of the technology that's used.

One option that could be explored is whether a separate legal instrument is needed for behavioural targeting. This study doesn't aim to propose a detailed sector-specific

---

[1946] See on article 5(3) chapter 6, section 4; chapter 8, section 4.

regime for behavioural targeting. Rather, some starting points for the discussion are given. In principle, specific rules could address different behavioural targeting phases: (1) data collection, (2) data storage, (3) data analysis, (4) data disclosure, and (5) the use of data for targeted advertising.[1947]

The most effective way to reduce chilling effects is not collecting data (phase 1).[1948] This could be partially achieved by applying and enforcing data protection law's regime for special categories of data, such as data regarding medical conditions, or political opinions. In a few EU member states, using special categories of personal data for direct marketing is prohibited; in many member states it is only allowed with the data subject's explicit consent. Because the privacy risks involved in using health data for behavioural targeting outweigh the possible societal benefits of allowing such practices, the EU lawmaker should consider prohibiting the use of any data regarding health for behavioural targeting, whether the data subject gives consent or not.

In many cases, sensitivity depends on the context, rather than on the types of data. Therefore, it should be considered whether data collection for behavioural targeting should be restricted or prohibited in certain contexts. For each situation where the lawmaker could consider banning certain practices, it could also opt for a lighter measure: banning tracking walls and similar take-it-or-leave-it choices.

To illustrate the possibility of regulating the collection context rather than a data type: for health related websites and services, the lawmaker should consider a ban on third party tracking for behavioural targeting. Specific rules should be considered as well for public sector services and websites. For instance, because of the special task of public service media, a chilling effect should be prevented. The lawmaker should consider banning all personal data collection for behavioural targeting and similar purposes on public service media – at least when third parties collect the data.

[1947] See on the five phases of behavioural targeting chapter 2.
[1948] See Diaz & Gürses 2012, p. 2-3.

As noted, under current law, a tracking wall could make consent involuntary if people must use a website. For many public sector websites, it could be the case that people are required to use them. Hence, if such public sector websites allow third party tracking, people should be able to use the website without consenting to such tracking. The lawmaker should consider making more explicit, for instance in a recital, that tracking walls and comparative take-it-or-leave-it choices are generally prohibited for public sector websites.

More generally, it doesn't seem appropriate for public sector websites to allow third party tracking for commercial purposes. Even if website visitors consent to tracking, it's far from evident why the state should facilitate firms to track people's behaviour for commercial purposes. Therefore, the lawmaker should consider a ban on third party tracking for commercial purposes on public sector websites.[1949]

Rules could also focus on phase 2 of the behavioural targeting process: data storage. For example, the data minimisation principle could be supplemented with more specific rules, in the form of maximum retention periods. The vast scale of data processing for behavioural targeting aggravates the chilling effects and the lack of individual control over personal information. Many risks would be reduced if fewer data were stored. With shorter retention periods, there would simply be fewer data that could be used for unexpected purposes. Shortening retention periods could mitigate some of the chilling effects.[1950] And restricting data collection in phase 1, or limiting retention periods in phase 2, would reduce the amount of information that's available to construct predictive models in phase 3.

Strict data minimisation requirements wouldn't be a novelty. The e-Privacy Directive says, in short, that traffic and location data must be erased when they're no longer

---

[1949] If such a ban were considered, many details, such as the scope of the ban, need further attention. For instance, what to do about organisations that are partly funded by the state?

[1950] See on empirical research on whether retention periods matter to users Leon et al. 2013: "participants who were told that data would be retained only for one day were significantly more willing to disclose browsing information" (p. 6).

required for conveying a communication or for billing, unless the user has given consent for another use. However, the e-Privacy Directive's rules for traffic and location data only apply to a narrow category of firms: providers of publicly available electronic communications services, such as internet access providers or phone operators – telecommunication providers for short.[1951] But many firms, such as ad networks and providers of smart phone apps, process more information of a more sensitive nature than telecommunication providers. This asymmetric situation calls for reconsideration.

Phase 3 concerns data analysis. Predictive models are outside the scope of data protection law.[1952] But as long as the data in phase 3 are (still) personal data, data protection law applies. Data protection law's transparency requirements can help to make personal data processing controllable for policymakers, as transparency can help to bring problems to light that might call for regulatory intervention.

Regulation could also focus on phase 4, data disclosure. In phase 4, firms make data available to advertisers or other firms. For example, an ad network can sell copies of data to other firms, or can enable advertisers to target specific persons with ads. This phase illustrates the importance of the purpose limitation principle. Maybe, in addition to the purpose limitation principle, data trade should be banned or restricted in certain contexts. It's not evident, for instance, that insurance companies should be allowed to obtain behavioural targeting data for the purpose of conducting risk calculations. And arguably, because of their special position, banks shouldn't be allowed to monetise their client's payment history through behavioural targeting.[1953]

The e-Privacy Directive prescribes an opt-in regime for using traffic and location data for direct marketing, but these rules only apply to telecommunications providers. The lawmaker should consider specific rules for traffic and location data for behavioural

---

[1951] It could be argued that the rules on traffic data (as far as they are included in article 5(1)) also apply to other types of firms. See chapter 6, section 4, and chapter 5, section 6.
[1952] See chapter 5, section 2 (and on predictive models chapter 2, section 5).
[1953] See Van Eijk 2014.

targeting. Such rules shouldn't only apply to telecommunications providers, but also to firms such as ad networks and providers of smart phone apps. In some contexts, collecting or using traffic and location data may have to be restricted or prohibited.

Sometimes, website publishers don't know in advance who will display ads on their websites, and who will track their website visitors. But if a publisher can't give data subjects the information that's required by the Data Protection Directive, the processing isn't allowed – and shouldn't be allowed. The transparency principle could thus limit what firms can lawfully do in phase 4. The lawmaker should consider making it more explicit that processing is prohibited, unless firms can comply with the transparency principle.

Phase 5 concerns the use of data for personalised advertising (or other purposes), and rules could focus on this phase as well. As far as the Data Protection Directive's provision on automated decisions applies at all to behavioural targeting, it applies to this phase. The provision could protect people against some forms of unfair social sorting. It follows from the provision that somebody may not be subjected to certain fully automated decisions that "significantly" affect her, unless a specified exception applies.[1954] But for behavioural targeting the relevance of the provision seems limited, because it's unclear whether one targeted ad "significantly" affects somebody in the sense of the provision. Furthermore, if an ad network only shows an offer to some people, somebody who doesn't receive the offer is probably unaware of being excluded.

The successor of the automated decisions provision in the European Commission proposal is called "measures based on profiling."[1955] The new provision obliges a firm to tell the person concerned that a profiling measure with significant effect is taken, and to inform the person about the measure's envisaged effects. The lawmaker should amend this provision, and prohibit profiling measures that have the effect of

---

[1954] Article 15 of the Data Protection Directive.
[1955] Article 20 of the European Commission proposal for a Data Protection Regulation.

discriminating on the basis of special categories of data, intentional or not. Such a prohibition would also apply if a firm used non-special data as a proxy for special categories of data. And firms should inform people about profiling measures and their underlying logic, and not only about profiling measures with significant effects. Interdisciplinary research is needed to develop tools to make profiling transparent in a meaningful way.

Usually non-discrimination law doesn't apply to the earlier phases of personal data processing, but it could apply to phase 5. Other rules that focus on phase 5 could also be envisaged. For example, it appears that a substantial part of the population would advocate a ban on personalised pricing, or a ban on personalised pricing in certain contexts.[1956] In any case, as noted in the previous chapter, data protection law requires transparency regarding personalised pricing. The data controller must disclose the processing purpose; this also applies if the purpose is personalising prices.[1957]

This study strongly argues against only focusing on data use (in phase 5) and leaving collection unregulated.[1958] Many privacy problems occur prior to phase 5. Apart from that, a regime that leaves collection unregulated would be difficult to reconcile with fundamental rights case law in Europe, and with the European Union Charter of Fundamental Rights.[1959]

As noted, a specific legal instrument for behavioural targeting, or for electronic direct marketing, would be one option to consider. In such a sector-specific regime, it would be easier to draft relatively specific rules that don't impose unreasonable burdens on

---

[1956] For instance, in a nationally representative survey in the US, Turow et al. 2005 "found that they [US adults] overwhelmingly object to most forms of behavioral targeting and all forms of price discrimination as ethically wrong" (p. 4). Whether personalised pricing is a good thing or not, and under which circumstances, is a complicated topic, which falls outside the scope of this study. See on personalised pricing chapter 2, section 8 and the references there.

[1957] Article 10 and 11 of the Data protection Directive. See chapter 8, section 2.

[1958] See for suggestions to regulators to focus (mainly or only) on use White House (Holdren JP et al.) 2014; Mayer-Schönberger & Cukier 2013. See for an argument against only regulating use (in phase 5): Hoofnagle 2014.

[1959] The European Court of Human Rights says the mere storage of data can interfere with privacy (see chapter 3, section 2). Furthermore, article 8 of the EU Charter of Fundamental Rights concerns personal data "processing", and processing includes collection (article 2(b) of the Data Protection Directive). See Irion & Luchetta 2013, p. 58.

other sectors. To illustrate, the legal regime for health related data shouldn't unduly hamper socially beneficial processing practices, such as research in the medical field or other scientific research.

Another option would be to include specific rules in other legal instruments. For example, rules for tracking on public service media could be included in media law. Other rules could be included in consumer law. Perhaps a black list could be drawn up of prohibited behavioural targeting practices.[1960] And the lawmaker could consider drawing up a list of circumstances to take into account in order to assess the voluntariness of consent.[1961]

In conclusion, enforcing and tightening the data protection principles could help to protect privacy in the area of behavioural targeting, even if people agree to consent requests. But additional rules are needed. The lawmaker shouldn't be afraid of prohibitions in the area of behavioural targeting. Taking into account the practical problems with informed consent to behavioural targeting, protecting the data subject with specific prohibitions or other mandatory rules wouldn't imply undue paternalism. True, it would be difficult to define prohibitions in such a way that they're not over or under inclusive. And banning certain practices implies that the lawmaker must make difficult normative choices. In an informed consent regime, such choices largely fall on the shoulders of the individual. Agreeing on prohibitions would be difficult, but that shouldn't be a reason to ignore the possibility.

* * *

[1960] See for instance the Unfair Commercial Practices Directive. The black list could be supplemented with a grey list, with practices that are presumed to be unfair. Hence, the "grey" practices are considered unfair, unless a firm can prove that the practice isn't unfair. (See on grey lists Centre for the Study of European Contract Law (CSECL) & Institute for Information Law (IViR) 2011, p. 228). The lists may have to be updated regularly.
[1961] See for a list of circumstances that could serve as a starting point for discussions chapter 6, section 4.