Improving privacy protection in the area of behavioural targeting

Zuiderveen Borgesius, F.J.

Publication date
2014
Document Version
Final published version

8 Improving empowerment

To defend privacy in the area of behavioural targeting, this study argues for a combined approach of protecting and empowering people. This chapter discusses how the law could improve individual *empowerment*. The following chapter focuses on *protection* of the individual.[1481] The behavioural economics analysis in the previous chapter suggests that fostering individual control over personal data won't suffice to protect privacy in the behavioural targeting area.

Why still aim for empowerment? In theory, it might be possible to have a legal regime that strictly defines all data processing practices that are prohibited, or those practices that are allowed. In such a hypothetical regime, there would be no need to give choices to the data subject with an informed consent provision or opt-out possibilities. This study doesn't explore such a hypothetical regime, for several reasons.[1482]

First, it's not feasible that the EU would abolish data protection law and would start from scratch to develop a new privacy regime. And a data protection regime without a consent provision is unlikely, if only because the EU Charter of Fundamental Rights lists consent as a legal basis for processing.[1483] Second, it would be almost impossible to define all beneficial and all harmful data processing activities in advance.[1484] Third, people's tastes differ. Some people would approve of a certain practice, while others wouldn't. As noted, the privacy-as-control perspective, and regulation with a consent

---

[1481] As noted, this study distinguishes protection and empowerment rules to structure the discussion, but it's not suggested that there's a formal legal distinction (see chapter 4, section 5).
[1482] I'm not aware of any serious proposals for a legal privacy regime without any role for consent or opt-out procedures.
[1483] Article 8 of the EU Charter of Fundamental Rights.
[1484] See Solove 2013, p. 1895. In theory, a regime without consent might be possible. See chapter 6, section 5.

provision, has the advantage of respecting people's individual preferences.[1485] Taking away *all* privacy choices from the individual would probably make the legal regime unduly paternalistic.[1486] Indeed, several scholars that are extremely sceptical of informed consent as a privacy protection measure still say that a legal privacy regime without any role for informed consent is neither feasible nor desirable.[1487] The foregoing doesn't mean that the lawmaker should stay away from mandatory rules that limit people's choices. On the contrary, such mandatory rules are needed, and are discussed in the next chapter.

In sum, it's likely that there will always be many circumstances where relying on informed consent, in combination with data protection law's safeguards, is the appropriate legal approach. For those cases, transparency and consent should be taken seriously. And compared with the current situation of very limited individual control over personal information in the behavioural targeting area, some improvement must be possible.[1488]

This chapter is structured as follows. Section 8.1 discusses enforcement. Section 8.2 and 8.3 discuss measures to improve transparency and to make consent more meaningful. Section 8.4 gives suggestions to improve the consent requirement for the use of tracking technologies. Section 8.5 discusses the Do Not Track standard. Section 8.6 concludes.

8.1 Enforcement

It's difficult to quantify the effect of data protection law. "With data protection," notes Bennett, "it is not clear how one could measure or even observe success. Impact has to be evaluated according to complex changes in the treatment of a very

---

[1485] See chapter, 3, section 1.
[1486] See Solove 2013, p. 1894.
[1487] See e.g. Barocas & Nissenbaum 2009; Nissenbaum 2011; Solove 2013, p. 1899; Barocas & Nissenbaum 2014.
[1488] Data protection is only relevant as far as it applies to behavioural targeting. As noted, this study argues data protection law should generally apply to behavioural targeting (see chapter 5).

intangible, elusive, and ephemeral commodity – personal information."[1489] Even so, there's wide agreement that there's a compliance deficit with data protection law.[1490] In the area of behavioural targeting, non-compliance seems especially rampant. For instance, transparency regarding behavioural targeting often leaves something to be desired, and many firms fail to ask prior consent for using tracking technologies in compliance with the law. Hence, stricter enforcement of the law is needed to improve data subject control in the area of behavioural targeting.

Stricter enforcement is easier said than done. Data Protection Authorities are understaffed, and lack resources.[1491] Data protection law applies to the private and the public sector, and supervising the law for the private sector alone is an immense task.[1492] Enforcement is more difficult because many firms using behavioural targeting are based outside the EU. Even if the law applies, international investigations are costly. And until recently, behavioural targeting took place largely below the radar.[1493] Furthermore, many Data Protection Authorities lack effective enforcement powers.[1494] Some authorities can only impose low fines – in one member state the maximum fine is 290 Euro.[1495] In some countries, Data Protection Authorities can't impose firms penalties for many types of violations. Additionally, there are Data Protection Authorities that appear to prefer a light touch approach.[1496] For instance, the Irish Data

---

[1489] Bennett 1992, p. 238. See also Irion & Luchetta 2013, p. 23, p. 28.
[1490] See for instance Bennett 2011a, p. 493; Irion & Luchetta 2013, p. 50; Borghi et al. 2013. Empirical research seems to confirm a lack of compliance with data protection law (see e.g. Burghardt et al. 2010; Birnhack & Elkin-Koren 2010). In some member states, it's not the Data Protection Authority but another regulator that oversees compliance with article 5(3) of the e-Privacy Directive. For ease of reading, this study speaks of Data Protection Authorities.
[1491] Irion & Luchetta 2013, p. 28; European Agency for Fundamental Rights 2010, p. 8; European Agency for Fundamental Rights 2014a, p. 46-47.
[1492] Some parts of the public sector are outside the scope of the 1995 Data Protection Directive (see chapter 4, section 2).
[1493] Behavioural targeting hasn't been ignored earlier. For instance, the Article 29 Working Party discussed tracking and profiling since 1997 (see Article 29 Working Party 1997, WP 6; 1999, WP 17; WP 37, p. 16). In the US, the Federal Trade Commission has discussed online privacy since 1996 (see Federal Trade Commission 2012, appendix A).
[1494] Impact Assessment for the proposal for a Data Protection Regulation (2012), p. 17-18; annex 1, p. 36-38, annex 2, p. 41-44; European Agency for Fundamental Rights 2010, p. 8.
[1495] In Lithuania the maximum administrative fine is 290 euro (Impact Assessment for the proposal for a Data Protection Regulation (2012), annex 1, p. 37). See also European Data Protection Supervisor 2014, p. 16; European Agency for Fundamental Rights 2014a, p. 46-49.
[1496] Irion & Luchetta 2013, p. 29.

Protection Commissioner is criticised for not enforcing the law against Facebook.[1497] On the other hand, some Data Protection Authorities receive criticism for being too aggressive.[1498]

Another problem that relates to the enforcement deficit is that data protection law contains many general rules with rather open norms. For example, there's still discussion on the question of whether data protection law applies when firms don't tie a name to data they process for behavioural targeting.[1499] Some Data Protection Authorities may be hesitant to impose sanctions in cases that are likely to lead to discussion about the material scope of the law. And for data subjects it may be unclear what they can expect. The next chapter returns to the topic of data protection law's open norms.[1500]

Causal relationships are hard to prove, but data protection law does seem to have effect. For instance, while many European websites don't ask consent for using tracking cookies in compliance with the e-Privacy Directive, they do offer some information about cookies. The consent requirement for tracking technologies from the 2009 e-Privacy Directive has led many European website publishers to behave in a manner that complies with the 2002 e-Privacy Directive, which required transparency and an opt-out option for cookies.[1501] And the fact that many firms lobbied in Brussels to influence the proposals for a Data Protection Regulation suggests that they don't think data protection law can be ignored.[1502]

Sometimes Data Protection Authorities take action in the area of behavioural targeting. For instance, the Dutch Authority has investigated the use of tracking

---

[1497] Max Schrems from Austria is one of the most vocal critics of the Irish Data Protection Authority (see Europe versus Facebook 2014).
[1498] Bamberger & Mulligan 2013 report on criticism on the aggressive approach of the Spanish DPA (p. 1593-1616).
[1499] See chapter 5.
[1500] Chapter 9, section 1.
[1501] See chapter 6, section 4.
[1502] See on lobbying chapter 5, section 5, chapter 6, section 3, chapter 8, section 3, and chapter 9, section 6.

cookies on smart TV sets, and the use of cookies by a behavioural targeting firm.[1503] And Data Protection Authorities have examined Google's data processing practices. In 2012, Google consolidated most of its more than 60 privacy policies into one overarching policy that governs the majority of its services. The new policy allows Google to combine user data over its various services. Google embarked on a large-scale information campaign that alerted people to the changes, with banners on its search page and on other Google websites. The Working Party had asked Google to postpone introducing the new policy, so Data Protection Authorities could gather more information. Google refused.[1504]

The Working Party sent Google long questionnaires about the privacy policy changes, but Google didn't answer all the questions in detail. The Working Party summarised its preliminary findings in a letter to Google.[1505] Among other things, the Working Party complains that Google doesn't offer enough transparency and fails to properly aks for consent for combining the data.[1506] Furthermore, Google doesn't ask consent for cookies in accordance with the e-Privacy Directive.[1507] Several privacy authorities from outside Europe jointly wrote an open letter to express their support to the Working Party's conclusions.[1508] Data Protection Authorities in six member states continued the investigation. At the time of writing, Data Protection Authorities in Spain and France have imposed fines of 900,000 and 150,000 Euros.[1509]

Enforcement strategies

An important avenue for further research is how compliance with the data protection rules could be improved. While this isn't a study on enforcement, some preliminary

---

[1503] College bescherming persoonsgegevens 2013 (TP Vision); College bescherming persoonsgegevens 2014 (YD).
[1504] See for a summary of the events College bescherming persoonsgegevens (Dutch DPA) 2013 (Google), p. 7-11.
[1505] Along with the French CNIL, the DPAs from the following countries continued the investigation: Germany, Italy, the Netherlands, Spain and the United Kingdom. See the website of CNIL, with further references (CNIL 2012 (Google)).
[1506] Formally it's a letter signed by 28 national Data Protection Authorities.
[1507] See Article 29 Working Party 2013 (Google letter), appendix, p. 5. See also CNIL 2014 (Google), p. 17-20.
[1508] The signatories of the letter include authorities from Mexico, Hong Kong, and Australia (Asian Pacific Privacy Authorities 2012, Google letter).
[1509] See Agencia Española de Protección de Datos (Spanish Data Protection Authority) 2013; CNIL 2014 (Google).

remarks are made on the topic. In the field of regulation studies, much has been written on the best way to make firms comply with the law, for instance with environmental law.[1510] Adapting a categorisation by Baldwin et al., firms can be categorised by looking at their intentions and their know-how. Grossly simplifying, a firm could be well-intentioned or ill-intentioned, and could be informed or ignorant.[1511] This way, four types of firms can be distinguished. The categories are simplifications. In reality, a firm will have characteristics of several categories. The classification is meant to illustrate that for some firms hard enforcement is needed. For other firms, raising awareness of the legal requirements may be the most effective tool to make them comply with data protection law.

The first category of firms is informed and well-intentioned.[1512] An example might be a large firm with skilled technologists and data protection lawyers. The firm understands the law, wants to comply, and can comply. The lawyers know every detail of the law and can translate the data protection principles into practical guidelines for the technologists to implement. Generally speaking, large-scale privacy violations are not to be expected from firms in the first category. The firms in this category are aware of the legal requirements. Hence, raising awareness of data protection law isn't needed for such firms. And threatening with sanctions isn't needed, as these firms are well-intentioned and want to comply with the law.

Second, a firm can be ignorant and well-intentioned. Such firms want to comply with the law, but might break the law by accident. For instance, a website publisher might use social media buttons or a web analytics programme on its website, without realising these expose visitors to privacy-invasive tracking. Or a developer of smart phone apps might use an ad network's services to include ads in its app. The

---

[1510] Regulation studies can be described as follows: "a multi-disciplinary field, with substantial contributions to regulatory debates being made by political scientists, lawyers, sociologists, anthropologists, and others. Writings on regulation are well-represented across scholarly publication outlets and there has also been the inevitable arrival of a journal with the word regulation in its title, *Regulation and Governance*" (Baldwin et al. 2010).
[1511] Baldwin et al. 2010 speak of "ill-disposed" and "well-disposed" firms, and of "highly capable" firms and "low capacity" firms (p. 304-306).
[1512] Baldwin et al. 2010, p. 304.

developer might consciously include a snippet of code from the ad network in the app. An app developer might also unwittingly enable third party tracking, when using "libraries"; these are blocks of ready-made code. A library might include code that enables an ad network to track the activities of the app's users.[1513] And a firm that doesn't tie a name to the data it processes might not realise it processes personal data.[1514]

Unwillingness isn't the main problem for this second category of firms. The problem is ignorance. For well-intentioned but ignorant firms, awareness raising is likely to be the most effective way of ensuring that they comply with the law. If Data Protection Authorities wanted to do more to raise awareness regarding the law, there would be various ways to do so. For instance, the Working Party's opinions, although sometimes hard to read for non-specialists, also receive attention in the press, which could bring the legal requirements to the attention of firms. And Data Protection Authorities might speak at conferences and other events. But another approach is also possible. Strict enforcement with respect to ill-intentioned firms may raise awareness regarding the law, and incentivise firms to educate themselves. To illustrate, the Dutch Data Protection Authority decided in 2007 that it "will concentrate on carrying out investigations and enforcement actions – the core task of any independent supervisory authority – to ensure a more effective promotion of the awareness of standards, and a stronger, more efficient enforcement of the compliance with legislation."[1515]

Third, a firm can be informed and ill-intentioned. The firm is an "amoral calculator", aims for maximum profit, and sees the risk of fines as a business risk.[1516] This type of firm could also be described as fully rational in the economic sense.[1517] The firm will

---

[1513] See Article 29 Working Party 2013, WP 202. See also the firm Flurry, which was discussed in chapter 2, section 2 (Yahoo 2014 (Flurry)).
[1514] See chapter 5, section 2.
[1515] College bescherming persoonsgegevens, Annual report 2007, p. 69-70.
[1516] Baldwin et al. 2010, p. 305. See also Becker 1993.
[1517] See chapter 7, section 2.

choose to bend or break the rules, as long as the expected profit from breaking the rules is higher than the chance of being fined, multiplied with the expected fine. As Black notes, "when compliance becomes a matter of risk management, non-compliance becomes an option."[1518] For a firm with billions of profit, a fine of one million euro isn't a dissuasive threat. In the context of environmental law, Faure observes: "fining a polluter with a too low fine can have a perverse learning effect."[1519]

But high penalties alone aren't enough. To incentivise a firm to comply with the law, the firm must believe there's a considerable chance that it will get caught and will have to pay the penalty.[1520] Suppose the expected fine is one million euro, and there's a 1% probability that such a fine is imposed. The expected loss is thus 1% of one million euro = 10,000 euro. To ensure a credible chance of enforcement, Data Protection Authorities should receive sufficient funding.

There may be other reasons for firms to comply with the law than avoiding fines.[1521] For instance, some firms offer consumer services, and may fear that people will switch to another service. Fear of consumer backlash is mainly relevant for firms that also offer consumer services, such as a search engine, a social network site, or computer software.[1522] For such firms, naming and shaming by the press or by Data Protection Authorities may be a worse punishment than a fine. Some Data Protection Authorities already use the shaming approach. For instance, the French Data Protection Authority obliged Google to publish on its search homepage that it had violated French law.[1523] The lawmaker could consider introducing the possibility for data Protection Authorities to publish the names of firms that breach data protection

---

[1518] Black 2008, p. 454.
[1519] Faure 2010, p. 263.
[1520] Faure 2010. See for a similar conclusion Schneier 2012, chapter 9; chapter 13; p. 241.
[1521] Like individuals, firms are not fully "rational" in the economic sense. See Chang 2014, p. 176 and further.
[1522] However, switching to another service may be difficult for a consumer, for instance because of transaction costs or network effects. And there might not be any competitors with better privacy policies. See chapter 7, section 3 and 4.
[1523] See e.g. CNIL 2014 (Google). See generally on reputational sanctions Van Erp 2007.

law. For some firms naming and shaming is less worrisome. For example, it's hard for people to boycott an ad network, if they don't know which websites work with the ad network.[1524] In sum, for the third category, well-informed but ill-intentioned firms, dissuasive penalties and a credible threat of enforcement are needed. Raising awareness regarding the law won't help to make these firms in comply with the law.

This study doesn't suggest that some firms enjoy breaking the law, although the phrase "ill-intentioned" was used above. As noted in the last chapter, market forces may push firms towards exploiting information asymmetries and people's biases, and towards more privacy invasive tracking.[1525] If the trend towards centralisation in the online marketing industry continues, at some point perhaps a handful of well-informed large firms are responsible for the majority of behavioural targeting. It can't be ruled out that some of these firms would be ill-intentioned.

The fourth category of firms is ill-intentioned and ignorant. They're not aware of the law, but wouldn't mind breaking it anyway. For example, it would be difficult to make criminals operating spyware comply with European data protection law, especially if they're based in a far-away country. But sometimes the law could be enforced to other players. For example, a European website publisher could be held responsible if it allows third parties to distribute spyware.[1526]

In sum, the best methods of ensuring that firms comply depend on the intentions and the legal and technical know-how of the firm. For some firms dissuasive penalties and a credible threat of enforcement are needed. For others raising awareness of the law may be the best approach to foster compliance. Faure arrives at a similar conclusion about environmental law.

[1524] See Schneier 2012, p. 183. There might be an indirect effect: website publishers might be hesitant to work with an ad network that receives criticism from the public.
[1525] Chapter 7, section 3 and 4.
[1526] See Article 29 Working Party 2010, WP 171: publishers and ad networks are often joint controllers. See also Castelluccia & Narayanan 2012, p. 22.

> Deterrence may be the primary goal in case of intentionally violating perpetrators (…) (who could only be brought to compliance by threatening them with high penalties) whereas a softer compliance strategy (providing information leading towards following the law) may be the more appropriate strategy with firms that merely breach because of lacking information.[1527]

The European Commission has realised that Data Protection Authorities have insufficient powers. Therefore, the proposal for a Data Protection Regulation aims to strengthen their enforcement powers. For instance, the proposal would enable Data Protection Authorities, in some circumstances, to impose sanctions of up to 2% of a firm's annual worldwide turnover. The European Parliament has proposed to increase the maximum to 5%.[1528] The proposal also calls for adequate resources for Data Protection Authorities.[1529]

Enforcement by data subjects

In principle, enforcement could also come from data subjects. But people rarely go to court when their data protection rights are breached. Litigation is expensive, and people aren't likely to go to court if litigation costs outweigh the damages that can be won.[1530] This problem isn't unique for data protection law. For example, if a consumer buys a product for ten euro that doesn't function as promised, it's not worth suing the producer.[1531] But if millions of consumers lose ten euro, the aggregate costs for society can be enormous. Similarly, privacy violations can concern millions of

---

[1527] Faure 2010, p. 263.
[1528] Article 79 of the European Commission proposal for a Data Protection Regulation (2012); article 70(2a)(c) of the LIBE Compromise, proposal for a Data Protection Regulation (2013).
[1529] Article 47(5) of the European Commission proposal for a Data Protection Regulation (2012); article 47(5) the LIBE Compromise, proposal for a Data Protection Regulation (2013).
[1530] See Impact Assessment for the proposal for a Data Protection Regulation (2012), p. 38; European Agency for Fundamental Rights 2014a, p. 39-44.
[1531] Baldwin et al. 2011, p. 126-127.

individuals that each bear small costs, such as annoyance. Solove compares privacy violations to bee stings. One isn't a problem, but many together would be.[1532] The problem of mass harm situations provides an argument for enforcement by regulatory authorities, such as consumer protection agencies or Data Protection Authorities.

An option that could be explored is introducing collective action procedures in the area of data protection law.[1533] Collective action procedures should make it possible for people to sue a firm collectively. Like this, a firm can be held accountable when it imposes small costs to many people that amount to large costs in the aggregate. The Commission proposal for a Data Protection Regulation would allow organisations to take firms to court for breaching people's data protection rights.[1534]

The Commission has published a recommendation on collective redress, which could also have an impact on data protection practice.[1535] The recommendation aims to "facilitate access to justice, stop illegal practices and enable injured parties to obtain compensation in mass harm situations caused by violations of rights granted under Union law, while ensuring appropriate procedural safeguards to avoid abusive litigation."[1536] The preamble states that data protection law is an area where collective action could be important.[1537] The recommendation encourages, but doesn't require, member states to adapt their laws. It could take years before a legally binding instrument is adopted.[1538] Another problem with enforcement by data subjects is that winning compensation for non-monetary damages can be difficult. Hence, it would be

---

[1532] Solove 2013, p. 1891. See also Haggert & Ericson 2000, who speak of a "surveillant assemblage."
[1533] The Article 29 Working Party has also suggested the introduction of class action suits in data protection law (Article 29 Working Party 2010, WP 168, p. 16). See also European Agency for Fundamental Rights 2014a, p. 32; p. 53.
[1534] See article 73(2), 74, 75 and 76(1) of the European Commission proposal for a Data Protection Regulation (2012).
[1535] European Commission 2013 (Collective Redress Recommendation).
[1536] Article 1(1) of European Commission 2013 (Collective Redress Recommendation).
[1537] Recital 7 of European Commission 2013 (Collective Redress Recommendation).
[1538] Hodges 2013 argues that it would be very difficult to develop a Europe-wide collective redress system, because of the different national legal systems. See also par. 41 of the European Commission 2013 (Collective Redress Recommendation).

worthwhile to examine whether the law should enable people to claim compensation for non-monetary damages that result from data protection law violations.

8.2 Transparency

The last chapter showed that information asymmetry is a problem in the area of behavioural targeting. For some information asymmetry problems data protection law already suggests an answer, but for others it doesn't. Information asymmetry is a problem from an economic perspective and from the perspective of privacy as control.[1539] But information asymmetry is also a problem under current law.

The main problem is many people don't know that their activities are monitored for behavioural targeting. At first glance, the answer is straightforward. The Data Protection Directive requires a firm to tell data subjects its identity and the processing purpose, and all other information that's necessary to guarantee fair processing.[1540] The Directive doesn't explicitly require firms to publish an easily accessible privacy policy, but it's general practice. The European Commission proposal for a Data Protection Regulation codifies this practice.[1541] And, as discussed in the next section, asking prior consent does more to alert people to tracking than offering an opt-out possibility.

A second category of information asymmetry is that people have scant idea about what firms do with their personal data. Again, at least the beginning of the answer is straightforward. Data protection law requires firms to disclose their processing purposes. And firms must clearly describe a specified purpose that isn't too vague or too general, and must not use personal data for unrelated purposes that the data

---

[1539] See on economics chapter 7, section 3. See on the privacy as control perspective chapter 3, section 1. Information asymmetry is also a problem from the privacy as identity construction perspective.
[1540] Article 10 and 11 of the Data Protection Directive. See on the information that should be provided when firms apply profiling techniques also: article 4 of the Council of Europe, Committee of Ministers, Recommendation (2010)13 to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling, 23 November 2010.
[1541] Article 11 of the European Commission proposal for a Data Protection Regulation (2012).

subject doesn't expect.[1542] Data Protection Authorities summarise that firms must aim for "surprise minimisation."[1543] As discussed in chapter 4, the purpose limitation principle isn't as strict as it might seem.[1544] Nevertheless, the principle could help to protect people against unexpected uses of their data. Transparency about data processing can only be meaningful if the purpose limitation principle is complied with.[1545]

The information asymmetry is partly caused by transaction costs, such as the time it would take people to inform themselves.[1546] Reading privacy policies would take too much time. They're often long and difficult to read and sometimes refer the reader to policies from other firms. According to the Article 29 Working Party, long privacy policies full of legalese aren't acceptable. "Internet companies should not develop privacy notices that are too complex, law-oriented or excessively long." [1547] Furthermore, privacy policies that obfuscate relevant information by pointing to other privacy policies are unlikely to comply with data protection law's transparency principle.

In its Google investigation, the Working Party complains that Google's privacy policy is too vague. "Google has not indicated what data is combined between which services."[1548] Furthermore, "Google gives incomplete or approximate information about the purposes and the categories of data collected. The privacy policy is a mix of particularly wide statements and of examples that mitigate these statements and mislead users on the exact extent of Google's actual practices."[1549] Indeed, while

---

[1542] Article 6(1)(b) of the data Protection Directive; Article 29 Working Party 2013, WP 203. See chapter 4, section 3.
[1543] Kohnstamm & Wiewiórowski 2013.
[1544] See chapter 7, section 3 and 4.
[1545] But see Moerel 2014, who suggests the purpose limitation principle should be deleted from the Data Protection Regulation (p. 55).
[1546] See chapter 7, section 3.
[1547] Article 29 Working Party 2013 (Google letter), p. 2. See also Article 29 Working Party 2004, WP 100, p. 5.
[1548] Article 29 Working Party 2013 (Google letter), appendix, p. 3.
[1549] Article 29 Working Party 2013 (Google letter), appendix, p. 2 (capitalisation adapted). For similar conclusions about earlier versions of Google's privacy policy, see Van Hoboken 2012, p. 329-333; Van Der Sloot & Zuiderveen Borgesius 2012, p. 102-108.

Google's privacy policy deserves praise for staying away from legalese, it uses confusing terms that leave the reader guessing which personal data are processed for which purposes. To illustrate, it's unclear which types of data Google sees as personal data.

The European Commission proposal for a Data Protection Regulation gives more detailed transparency rules.[1550] For instance, it requires firms to have "easily accessible policies (…) in an intelligible form, using clear and plain language, adapted to the data subject."[1551] The clear language requirement is in line with European consumer law, which requires firms to disclose "information in a clear and comprehensible manner."[1552] The preamble stresses the importance of clear information in the area of online advertising.[1553] Codifying the clear language requirement could discourage firms from using unreadable policies. And the requirement would make it easier for Data Protection Authorities to intervene when firms use vague policies or consent requests. The rule wouldn't be enough to ensure actual transparency, but it could help to lower the costs of reading privacy policies.

An important aspect of effectively informing people is not overwhelming them with information.[1554] Less is more. Therefore, making privacy policies simpler seems like a good idea. But privacy isn't simple.[1555] Describing complicated data processing practices accurately leads to a long text. If the text is too concise, it doesn't provide enough information. Reducing transaction costs by making privacy policies simpler is

---

[1550] Unlike the Data Protection Directive's article 11(c), the European Commission proposal's article 14(1)(h) doesn't mention "the categories of data" as an example of the information that firms must give to guarantee fair processing. See critically Korff 2012, p. 33.

[1551] Article 11 of the European Commission proposal for a Data Protection Regulation (2012). See generally chapter III, section 1 of the proposal, "Transparency and modalities."

[1552] For instance, the Consumer Rights Directive requires firms to disclose "information in a clear and comprehensible manner (article 6(1)), and in "plain and intelligible language" (article 7(1); article 8(1)). The preamble discusses traders that supply digital content, such as apps or software. Such firms must inform consumers in particular about "the ways in which digital content can be used, for instance for the tracking of consumer behaviour (recital 19)."

[1553] Recital 46 of the European Commission proposal for a Data Protection Regulation (2012). See also Impact Assessment for the proposal for a Data Protection Regulation (2012), annex 2, p. 31.

[1554] Helberger 2013a, p. 34.

[1555] Daniel Solove used a similar phrase during the Symposium 2012: Privacy & Technology, 9 November 2012, Harvard University, Boston (<www.harvardlawreview.org/privacy-symposium.php> accessed 15 August 2013).

hard to reconcile with reducing information asymmetry.[1556] And reading privacy policies, even short ones, takes time. Many short notices together still add up to a lot of information. And each day, people have to deal with more information than only privacy policies. For instance, consumer law requires firms to disclose information on many products.[1557]

Some improvement must be possible over the current situation, as now privacy policies are often long, unreadable texts.[1558] The Working Party suggests using layered privacy policies. A firm should explain in a few sentences what it wants to do with personal data. People should be given the chance to click through to more detailed information.[1559] However, research shows it's questionable whether people would ever read the second and third layer. In any case, we shouldn't hope for too much when aiming to make people read privacy statements, simplified or not. Research suggests that "even the most readable policies are too difficult for most people to understand and even the best policies are confusing."[1560]

Maybe icons could be useful to communicate the data processing practices of firms. The Working Party and the European Commission encourage the use of icons,[1561] and the European Parliament has proposed to require firms to use icons to inform people about data processing practices.[1562] There are self-regulatory bodies that give seals,

---

[1556] See Nissenbaum 2011, p. 36; Solove 2013, p. 1885; Bar-Gill 2012, p. 37.
[1557] See about the cumulative effect of legal transparency requirements Ben-Shahar & Schneider 2011.
[1558] See for an overview of research on the comprehensibility of texts: Lentz et al, Knowledge Base Comprehensible Text. Some lawmakers adopted detailed rules regarding the readability of information. For example, in Brazil the law requires a minimum font of at least size 12 in standard terms for consumer contracts (article 54(3) of the Federal law n. 8.078, of September 11th, 1990). In Florida, the law has strict requirements regarding the presentation of insurance policies. "Every policy shall be readable as required by this section. (…) An insurance "policy is deemed readable if (…) [t]he text achieves a minimum score of 45 on the Flesch reading ease test (…) or an equivalent score on any other test comparable in result and approved by the office" (Florida Statutes: Insurance Rates and Contracts, Title XXXVII, chapter 627, Insurance Rates and Contracts, article 627.4145**,** par. 1(a).)
[1559] Article 29 Working Party 2004, WP 100.
[1560] Mcdonald et al. 2009, p. 50.
[1561] European Commission 2007 (PETs), par. 4.3.2.
[1562] See article 13(a), and the annex, of the LIBE Compromise, proposal for a Data Protection Regulation (2013). I have to admit that to me, the proposed six icons don't seem very clear. But it's possible that after a while, people would start to recognise the icons.

but such seals don't always imply that a website has high standards.[1563] Some providers have awarded seals to any firm, without a prior check. One paper found that websites with a seal from a particular organisation were generally less trustworthy than websites without that seal.[1564]

In the field of consumer law, scholars have suggested the introduction of intermediaries that help people to benefit from information.[1565] Regulators could audit intermediaries to ensure honesty. A similar approach could be considered for personal data processing practices. For instance, firms could be required to disclose their data processing practices to intermediaries that give ratings or seals. An organisation could make "white lists" or "block lists" for cookies that people can install in their browsers. Researchers at Stanford University are working on such a project.[1566] The European Parliament's LIBE Compromise enables firms to request a Data Protection Authority, for a reasonable fee, to certify that the personal data processing is performed in compliance with the Regulation.[1567]

In view of the limited effect that privacy policies have in informing people, more research is needed on alternative ways of presenting information. The current "failure of mandated disclosure" doesn't prove that legal transparency requirements will always fail.[1568] Calo argues that we shouldn't forget about transparency and informed consent, before better ways of presenting information have been tried.[1569] There's

---

[1563] See Rodrigues et al. 2013, p. 52-54; Tschofenig et al. 2013, p. 7-8. See also Schneier 2012, p. 183. Under the Unfair Commercial Practices Directive, one of the practices that's always unfair is: "Displaying a trust mark, quality mark or equivalent without having obtained the necessary authorisation" (Annex I (2)).
[1564] Edelman 2011. In 2014, the organisation in question, TRUSTe, agreed to settle Federal Trade Commission charges that it deceived consumers about its recertification program (Federal Trade Commission 2014a). See generally on trust marks and European law: Balboni 2008.
[1565] For instance, an intermediary could offer a website where people can easily compare cell phone contracts, adapted to their own usage. See for ideas along these lines Bar-Gill 2010, p. 41-42; Luth 2010, p. 243-247.
[1566] Cookie Clearinghouse 2014.
[1567] Article 39 of the LIBE Compromise, proposal for a Data Protection Regulation (2013). The Working Party is critical about the idea as it is phrased in the LIBE Compromise (Article 29 Working Party 2013 (draft LIBE comments, p. 4-5).
[1568] Calo 2011a. The phrase "failure of mandated disclosure" is taken from Ben-Shahar & Schneider 2011.
[1569] Calo 2011a.

research on better ways of presenting privacy policies.[1570] Cooperation between disciplines is needed, such as technology design, computer interface design, and psychology.[1571] There are firms that experiment with novel ways of presenting information about privacy.[1572] Some smart phone apps show that it's possible to communicate basic information in an intuitive way on small screens. But it appears firms put more effort in communicating the functions of an app than communicating their privacy policies.[1573]

But even if effective ways to present privacy policies could be developed, it might be difficult to make firms use them, because incentives are lacking. A firm that wants to distract people from information has many ways to do so, for instance by giving more information than needed, by using ambiguous language, or by framing information.[1574] "Click here for more relevant advertising" doesn't have the same ring to it as "Click here for continuous surveillance." But as long as information isn't misleading, the Data Protection Directive doesn't seem to have an answer to framing. In some cases, consumer law could be applied by analogy to framing. For example, it's unfair to present rights given to consumers in law as a distinctive feature of the trader's offer.[1575] In this light, a privacy policy raises questions if it presents people's data protection rights, such as the right to access, as a favour. Perhaps standardised privacy policies could help.[1576] The European Commission proposal for a Data Protection Regulation would make it possible to require firms to use a standard form to communicate their privacy policies.[1577]

[1570] See in the privacy field for instance Calo & Vroom 2012. Calo argues that the difference between effective information and nudges is a matter of degree rather than kind (Calo 2013a).
[1571] See in this context the work of the interdisciplinary research projects SPION (Security and privacy in online social networks), <www.spion.me/publications>, and USEMP (User Empowerment for Enhanced Online Management), <www.usemp-project.eu> accessed 28 May 2014.
[1572] For instance, Google publishes videos about cookies (Google (How Google uses cookies)).
[1573] See Helberger 2013a.
[1574] See Ben-Shahar & Schneider 2011; Willis 2013.
[1575] Annex 1 (10) of the Unfair Commercial Practices Directive. See on fairness in consumer law and data protection law chapter 4, section 4.
[1576] Verhelst 2012, p. 222-225; Kelley et al. 2010; Helberger 2013a, p. 30.
[1577] Article 14(8) of the European Commission proposal for a Data Protection Regulation (2012).

For some types of information asymmetry, current data protection law simply doesn't have an answer. It's impossible for people to predict the possible consequences of future uses of personal data. Education about privacy risks seems to be the appropriate answer. In some other contexts, the law requires information about risks, such as on cigarette warnings. Thus, perhaps firms could be required to disclose information about privacy risks.[1578]

Furthermore, it's hard to make an informed decision whether to disclose personal data in exchange for the use of a "free" service, because people don't know the value of their data. Data protection law doesn't have an answer here either. But the transparency principle could provide inspiration. It has been suggested in literature that firms should be required to tell the data subject how much profit they'll make with his or her personal data.[1579] Consumer law prohibits firms from advertising a product as "free" if there are hidden costs.[1580] By analogy, this makes some privacy policies suspicious if the firm captures personal data by way of "payment." In this light, Facebook's claim that "it's free and always will be" deserves scepticism.[1581]

Risk of manipulation

Some fear that personalised ads and other content could surreptitiously steer people's behaviour. In short, behavioural targeting could be used to manipulate people. As noted, it's an open question how serious the threat is at present. But in some contexts, such as political advertising, undue influence would be more worrying than in

---

[1578] Such information could include, for instance, the number of data breaches that have occurred the year before. Thanks to Oren Bar-Gill for this suggestion.
[1579] Traung 2012, p. 42.
[1580] Annex 1 (20) of the Unfair Commercial Practices Directive. "Commercial practices which are in all circumstances considered unfair (…) [include:] Describing a product as 'gratis', 'free', 'without charge' or similar if the consumer has to pay anything other than the unavoidable cost of responding to the commercial practice and collecting or paying for delivery of the item."
[1581] "It's free and always will be", says Facebook on the page where people can register for an account (<www.facebook.com> accessed 28 May 2014). See on framing chapter 7, section 4.

others.[1582] As in some cases personalisation could become a problem, scholars and policymakers should keep a close eye on the developments.

Data protection law can help to keep track of developments and perhaps to lessen some risks. The transparency principle also applies if a firm processes personal data to personalise ads or services. The law requires firms to tell data subjects the processing purpose and to give all information that's necessary to guarantee fair data processing.[1583] This suggests a firm must say so if the processing purpose is personalising content. For example, the firm could explain it uses people's browsing behaviour to personalise content.[1584]

If the lawmaker wanted to preclude problems related to surreptitious personalisation, the law could require an icon to accompany personalised content.[1585] A requirement to distinguish certain content wouldn't be a novelty. EU law requires advertising to be clearly labelled as such.[1586] Furthermore, data protection law can be interpreted as generally requiring an option to opt out of personalisation. If personal data processing for personalisation is based on the legal basis consent, people can withdraw their consent. If the processing is based on the balancing provision or on a contract, people have the right to object on compelling legitimate grounds. If the processing concerns personalised advertising, people have an absolute right to object: the right to stop the

---

[1582] See chapter 2, section 7, and chapter 3, section 3.
[1583] Article 10 and 11 of the Data Protection Directive. When a firm applies a predictive model to an individual (phase 5 of the behavioural targeting process), the firm processes personal data, and data protection law applies (see chapter 5, section 2). Therefore, the firm has to inform the data subject about the processing purpose.
[1584] See also Bozdag & Timmersmans 2011, who call for transparency to mitigate the risk of filter bubbles.
[1585] See Helberger 2011; Koops 2008, p. 336; Oostveen 2012. An icon to accompany personalised content wouldn't be a complete novelty. When Google started to personalise search results in 2009, for a while it included a link that could alert people that the results were personalised (Horling 2009).
[1586] Article 9(1)(a) and 19 of the Audiovisual Media Services Directive; Article 6 of the E-Commerce Directive, Unfair Commercial Practice Directive, Annex I (11). See Helberger 2013, p. 8. The effectiveness of icons is an open question. Whether an icon alerts people to personalisation would have to be assessed in behavioural studies.

processing.[1587] The lawmaker could consider explicitly codifying a requirement for firms to offer people the possibility to stop or pause personalisation.[1588]

Data protection law is silent on the lawfulness of price discrimination and personalised prices.[1589] But if an online shop personalises prices, for instance, on the basis of a cookie representing a customer, it singles out a person and processes personal data. Data protection law requires the data controller to disclose the processing purposes to the data subject.[1590] Therefore, a firm is also obliged to disclose the purpose if the purpose is personalising prices.[1591] Apart from that, data protection law has a specific provision for certain automated decisions, which may be relevant for personalised pricing as well. This provision is discussed in the next chapter.[1592]

Regarding the transparency principle, there's a potential loophole in the Data Protection Directive. Article 11 states which information firms must disclose "where the data have not been obtained from the data subject." This provision applies, for instance, when a data controller obtains data without the individual's consent. But the second paragraph could be interpreted as softening the transparency requirement in case of predictive modelling. "Paragraph 1 shall not apply where, in particular for processing for statistical purposes or for the purposes of historical or scientific research, the provision of such information proves impossible or would involve a disproportionate effort (…)."[1593] Firms could use statistical data to construct predictive models. A firm could try to argue that informing people about its plans to build a predictive model on the basis of their personal data would take "disproportionate

---

[1587] Article 14(a) and 14(b) of the Data Protection Directive. See on opting out chapter 6, section 2; on withdrawing consent chapter 6, section 3.
[1588] A requirement to offer people the chance to pause processing wouldn't be a novelty. Article 9(2) of the e-Privacy Directive requires firms to offer people the possibility to temporarily refuse the processing of location data. Turow proposes an alternative: firms should be required to offer people the chance to see which ads somebody with another cookie profile would see (Turow 2011, p. 198-199).
[1589] See on personalised pricing chapter 2, section 7 and the references there.
[1590] Article 10 and 11 of the Data Protection Directive.
[1591] See on price discrimination chapter 2, section 7 and the references there. See also chapter 9, section 7.
[1592] Article 15 of the Data Protection Directive. See Chapter 9, section 6.
[1593] Article 11(2) of the Data Protection Directive. See also recital 38-40.

effort."[1594] Following that reasoning, the firm wouldn't have to inform the people whose data it uses for building the predictive model. Therefore, the lawmaker could consider stating in a recital that this provision doesn't legitimise building predictive models without transparency for the people from whom the input data were collected. On the other hand, such a rule could hamper scientific or medical research. This suggests the lawmaker should consider drafting separate rules for behavioural targeting or for electronic direct marketing. (The next chapter returns tot this idea.[1595])

Access rights

To foster transparency, data protection law requires more from firms than privacy policies and consent requests. For instance, people have the right to access data concerning them.[1596] Again, this calls for enforcement of existing rules and for the development of user-friendly solutions. There's work in this area. For example, Google lets a person see the interest categories that Google tied to the cookie that represents the person. A person can rectify the categories Google has associated with the cookie.[1597] However, Google doesn't show people all information it has on them, and Google doesn't explain how it inferred the interest categories.[1598] Notwithstanding, the interest manager shows that creative solutions to enable access rights are possible.

Access rights to cookie-based profiles could have drawbacks. An ad network could design a system where a user could inspect all data that an ad network has attached to his or her cookie, such as his or her browsing history. But such a system would also

---

[1594] Aggregating personal data to construct a predictive model could be seen as the destruction of personal data, if the personal data are deleted. The destruction of personal data is included in the definition of processing. Hence, in principle a data controller should be transparent about this purpose. See Article 29 Working Party 2014, WP 216, p. 7.

[1595] Chapter 9, section 2 and section 7.

[1596] Article 12 of the Data Protection Directive; article 8(2) of the EU Charter of Fundamental Rights.

[1597] The "Ads Preferences Manager (…) lets you view, delete, or add interest categories associated with your browser so that you can receive ads that are more interesting to you" (Google 2009). See <www.google.com/settings/ads>. See also Van Der Sloot & Zuiderveen Borgesius 2012, p. 102-108.

[1598] "To some extent," notes Van Hoboken, "the control and transparency is merely a façade, behind which a (for the end-user) opaque sophisticated data processing architecture is doing the real work" (Van Hoboken 2009).

create a privacy risk. If Eve found Alice's device, he could see all the websites she visited by inspecting her cookie-profile. If this problem is indeed unsolvable, it could be argued that cookie-based profiling by ad networks is unlawful, as ad networks can't comply with data protection law's access rights. On the other hand, if Eve found Alice's device, it's likely he could also access other information on the device. So perhaps the fact that Eve can inspect her browsing history isn't Alice's main problem.

The European Commission approaches the problem of access rights to pseudonymous data differently in its proposal for a Data Protection Regulation. "If the data processed by a controller do not permit the controller to identify a natural person, the controller shall not be obliged to acquire additional information in order to identify the data subject for the sole purpose of complying with any provision of this Regulation."[1599] This provision could have unfortunate effects. A firm could invoke the provision to deny a data subject access to the browsing history in a cookie-based profile, if the firm can't establish whether the access request comes from the person whose browsing history is stored. If this rule were combined with a provision that allows behavioural targeting on an opt-out basis, people could be tracked and profiled without consent, and wouldn't even be able to exercise their access rights.[1600] Transparency and data subject control would be almost completely absent. Furthermore, not enabling data subject access to personal data seems hard to reconcile with the EU Charter of Fundamental Rights, which states: "[e]veryone has the right of access to data which has been collected concerning him or her."[1601]

Caveat and conclusion

As previously mentioned, one policy instrument to reduce information asymmetry is educating the public. Many people lack basic knowledge of internet technology and of

---

[1599] Article 10 of the European Commission proposal for a Data Protection Regulation (2012). The LIBE Compromise confirms this approach (article 10(1) of the LIBE Compromise, proposal for a Data Protection Regulation (2013)). See also article 15(2) of the LIBE Compromise.
[1600] See chapter 6, section 2.
[1601] Article 8(2) of the EU Charter of Fundamental Rights

security and privacy risks. As Cranor & McDonald put it, "consumers cannot protect themselves from risks they do not understand."[1602] However, learning takes time. It seems people are only vaguely aware of behavioural targeting, although it has been happening since the mid 1990s.[1603] And it's questionable whether education could keep up with the pace of the developments in the online marketing industry. Nevertheless, some knowledge is better than none. But the law shouldn't put unreasonable burdens on people's shoulders. In the European legal system, the state has positive obligations to protect people's privacy.[1604] Hence, empowerment shouldn't turn into responsibilisation.[1605] This term describes "the process whereby subjects are rendered individually responsible for a task which previously would have been the duty of another – usually a state agency – or would not have been recognized as a responsibility at all."[1606] While this caveat should be borne in mind, education could help.

In conclusion, stricter enforcement of data protection law, at least how it's interpreted by the Working Party, could help to reduce the information asymmetry. But there's room for refinement of the current legal framework. More transparency could give people a bit more control over information concerning them. Interdisciplinary research is needed to develop better ways to communicate privacy policies. But without a credible threat of enforcement and dissuasive sanctions, firms may lack incentives to make behavioural targeting transparent.

8.3 Consent for personal data processing processing processing

EvenEven though the last chapter showed that expectations of informed consent as a privacy protection measure shouldn't be too high, some improvement over the current

---

[1602] Cranor & McDonald 2010, p. 27. Castelluccia & Narayanan 2012 also call for education (p. 18-19).
[1603] As noted in chapter 2, section 2, cookies have been used for tracking since at least 1996.
[1604] See for instance ECtHR, Z v. Finland, No. 22009/93, 25 February 1997, par. 36. See chapter 3, section 2.
[1605] See Gürses 2010, p. 97. See also Acquisti et al. 2013, p. 2.
[1606] Wakefiel & Flemicg 2009, p. 276. See on responsibilisation in the privacy field the research project SPION, Security and Privacy for Online Social Networks, <www.spion.me> accessed 26 May 2014. Thanks to Seda Gürses for pointing out this concept to me.

situation must be possible. As noted, unambiguous consent is generally the only available legal basis for personal data processing for behavioural targeting, and the e-Privacy Directive requires consent for most tracking technologies.[1607]

It's sometimes suggested that firms can obtain the data subject's consent for personal data processing through their terms and conditions. But the Working Party doesn't accept this. "Consent must be specific. (…) Rather than inserting the information in the general conditions of the contract, this calls for the use of specific consent clauses, separated from the general terms and conditions"[1608] Case law of the European Court of Justice also suggests a consent request shouldn't be hidden in terms and conditions.[1609] Furthermore, obtaining consent by quietly changing a privacy policy isn't possible under data protection law, as there wouldn't be an expression of will by the data subject.[1610] A data subject thus shouldn't have to keep checking a privacy policy to see whether he or she accidentally consents to a new practice by continuing to use a service.

In its Google investigation, the Working Party says that "passive users" weren't informed, and weren't asked for consent. In brief, passive users are people who are tracked by Google on non-Google websites, for instance through its DoubleClick ad network.[1611] Such "users are generally not informed that Google is processing personal data, such as IP addresses and cookies."[1612] The Working Party adds that Google doesn't ask consent for using tracking cookies, as the e-Privacy Directive requires.[1613]

The European Commission proposal for a Data Protection Regulation reaffirms that mere inactivity doesn't signal consent. The proposal requires consent to be "explicit."

[1607] Chapter 6.
[1608] Article 29 Working Party, WP 187, p. 33-35. "The information must be provided directly to individuals. It is not enough for it to be merely available somewhere" (p. 35).
[1609] CJEU, C-92/09 and C-93/09, 9 November 2010, Volker und Markus Schecke and Eifert.
[1610] See chapter 6, section 3.
[1611] Article 29 Working Party 2013 (Google letter), appendix, p. 2, footnote 2. Passive users are "users who does not directly request a Google service but from whom data is still collected, typically through third party ad platforms, analytics or +1 buttons."
[1612] Article 29 Working Party 2013 (Google letter), appendix, p. 3.
[1613] Article 29 Working Party 2013 (Google letter), appendix, p. 5.

Consent requires a "statement" or "a clear affirmative action."[1614] "Silence or inactivity should (…) not constitute consent," adds the preamble.[1615] Furthermore, the proposal prohibits hiding a consent request in terms and conditions. "If the data subject's consent is to be given in the context of a written declaration which also concerns another matter, the requirement to give consent must be presented distinguishable in its appearance from this other matter."[1616] Just like in the early 1990s, when the Commission presented its proposal for a Data Protection Directive, many firms reacted to the 2012 proposal by lobbying to soften the requirements for consent.[1617]

Nudging and take-it-or-leave-it choices

The status quo bias suggests that requiring opt-in consent could lead to people disclosing fewer data. Requiring opt-in consent could be seen as a kind of "nudging", a phrase coined by Thaler & Sunstein.[1618] A lawmaker nudges when it uses insights from behavioural economics to gently push people's behaviour in a certain direction, without actually limiting their freedom of choice.[1619] Setting defaults is a classic example of nudging. Furthermore, a regime that requires affirmative action for consent (in line with legal doctrine) does more to alert people to data processing than a regime that accepts mere silence as "implied" or "opt-out" consent.

[1614] Article 4(8) of the European Commission proposal for a Data Protection Regulation (2012).
[1615] Recital 25 of the European Commission proposal for a Data Protection Regulation (2012). Facebook doesn't agree: "We (…) propose that the reference that consent must be given 'explicitly' and 'silence and inactivity should not constitute consent' should be deleted from Recital 25" (Facebook proposed amendments 2013).
[1616] Article 7(2) European Commission proposal for a Data Protection Regulation (2012).
[1617] See Facebook proposed amendments 2013, p. 23; Amazon proposed amendments (article 4(1)(8); International Chamber of Commerce 2013, p. 3; eBay proposed amendments 2012. See on the 1990s chapter 6, section 3.
[1618] Sunstein gives an opt-in requirement for tracking as an example of a nudge (Sunstein 2013a, p. 38; Sunstein 2013b, p. 13). See on nudging also chapter 9, section 2.
[1619] They describe nudging as follows: "A nudge, as we will use the term, is any aspect of the choice architecture that alters people's behavior in a predictable way without forbidding any options or significantly changing their economic incentives. To count as a mere nudge, the intervention must be easy and cheap to avoid. Nudges are not mandates. Putting the fruit at eye level counts as a nudge. Banning junk food does not" (Sunstein & Thaler 2008, p. 6). If the lawmaker aims to use default settings to keep people in the default setting, some speak of "policy defaults" (Ayres & Gertner 1989, Willis 2013a).

However, Willis warns that it's hard for a lawmaker to make firms use nudges, if those firms don't want to nudge people in the same direction as the lawmaker. Firms have many ways to entice people to opt in.[1620] As Sunstein puts it, "if regulated institutions are strongly opposed to a default rule and have easy access to their customers, they may well be able to use a variety of strategies, including behavioral ones, to encourage people to move in the direction the institutions prefer."[1621] For instance, firms can offer take-it-or-leave-it choices, such as tracking walls on websites. Hence, even if firms offered transparency and asked prior consent for behavioural targeting, people might still feel they have to consent.[1622]

The European Commission proposal for a Data Protection Regulation retains the requirement that consent must be free. The preamble adds: "consent does not provide a valid legal ground where the individual has no genuine and free choice and is subsequently not able to refuse or withdraw consent without detriment."[1623] This recital could be applied to tracking walls, but it doesn't give much more guidance than the existing requirement that consent must be "free."

The LIBE Compromise contains a provision that can be read as a prohibition of tracking walls under certain circumstances: "[t]he execution of a contract or the provision of a service shall not be made conditional on the consent to the processing of data that is not necessary for the execution of the contract or the provision of the service pursuant to article 6(1), point (b)."[1624] That latter provision concerns the legal basis that applies when the processing is necessary to perform a contract with the data subject. However, the LIBE Compromise would also allow firms to rely on the balancing provision for some behavioural targeting practices with pseudonymous

---

[1620] Willis 2013; Willis 2013a.
[1621] Sunstein 2013a, p. 119. See also Solove 2013, p. 1898. See in detail about the strategies firms can use to make people agree to tracking Willis 2013a, especially p. 111 and further.
[1622] See European Commission 2011 (Eurobarometer), p. 27.
[1623] Recital 33 of the European Commission proposal for a Data Protection Regulation (2012). Facebook has proposed an amendment that says: "a data controller may legitimately make consent to the processing a condition of access to a service, particularly when the service is free of charge to the data subject" (Facebook proposed amendments 2013, p. 27, amendment to recital 34).
[1624] Article 7(4) of the LIBE Compromise (capitalisation adapted).

data. Hence, for many behavioural targeting practices the practical effect of this prohibition of tracking walls would seem to be limited.[1625]

Should the law do anything about take-it-or-leave-it choices regarding the enjoyment of privacy when using websites and other internet services? This is a hard question that invokes discussions on how much legal paternalism is justified. Some authors suggest tracking walls should be prohibited.[1626] (A few suggest tracking walls are already prohibited under the Data Protection Directive.[1627]) A blanket prohibition of take-it-or-leave-it choices would prohibit people from disclosing their personal information in exchange for using a service. As far as protecting the data subject is the main rationale for the ban, a ban on tracking walls would fall within the paternalism definition used in this study.[1628] It doesn't follow that banning tracking walls would be *unduly* paternalistic. That said, some take-it-or-leave-it choices might concern relatively innocuous data processing practices, and it isn't evident that such choices should be prohibited.

The principle of contractual freedom can be applied by analogy to consent to tracking, but contractual freedom isn't absolute. And while insights from contract law can be applied by analogy to consent in data protection law, the two legal fields are different. Furthermore, if a ban on tracking walls would protect the data subject's interests and societal interests at the same time, it wouldn't be purely paternalistic. The next chapter discusses whether there are circumstances in which tracking walls should be prohibited, apart from the general rule that consent must be "free" to be valid.[1629]

[1625] See article 2(a), article 6(f), and recitals 38 and 58a of the LIBE Compromise, proposal for a Data Protection Regulation (2013). See chapter 6, section 2.
[1626] See for instance Irion & Luchetta 2013, p. 78; Brussels declaration 2011 (I am one of the signatories). At least one country prohibits take-it-or-leave-it choices. Article 16(2) of the Personal Information Protection Act of South Korea says: "The personal information processor shall not deny the provision of goods or services to the data subjects on ground that they would not consent to the collection of personal information exceeding minimum requirement." See also Strandburg 2013, p. 88.
[1627] Roosendaal 2013, p. 186. In contrast, I think current data protection law often allows take-it-or-leave-it choices (see chapter 6, section 3 and 4).
[1628] See chapter 6, section 6.
[1629] Chapter 9, section 5 and 7.

Some have suggested the law could require firms to offer a tracking-free version of their service, which has to be paid for with money.[1630] Such a rule would enable people to compare the prices of websites. Now the "price" of a website is usually hidden because people don't know what information about them is captured, nor how it will be used.[1631] Some commentators suggest the price of a tracking-free version shouldn't be left to the market alone.[1632] There are precedents for legal intervention in the prices of media. For instance, EU law limits the amount of advertising that can be shown on television.[1633] As Helberger notes, such an advertising maximum could be seen as a price cap, as the time people spend watching advertising on TV could be seen as payment for content.[1634]

A requirement for firms to offer a tracking-free but paid-for version of their service would be less protective of privacy than a ban on tracking walls. Myopia might lead most people to choose the free version, because they focus on the short-term loss of paying for a service, even if this means they have to consent to behavioural targeting, contrary to earlier plans.[1635] Furthermore, many say it's "extortion" if they have to pay for privacy.[1636]

In conclusion, behavioural economics insights are in line with the formal legal conclusion. Firms aren't allowed to infer consent from mere silence, and shouldn't be allowed to do so. But even if firms offered transparency and asked for opt-in consent for tracking in compliance with the law, the problem of take-it-or-leave-it choices and tracking walls would remain. As long as the law allows take-it-or-leave-it choices, opt-in systems won't be effective privacy nudges.

[1630] Traung 2012, p. 42; Irion & Luchetta 2013, p. 38; Calo 2013, p. 50.
[1631] Helberger 2013, p. 19. See also Strandburg 2013, p. 90-91, and chapter 7, section 3 and 4.
[1632] Irion & Luchetta 2013, p. 38.
[1633] Article 23(1) of the Audio Visual Media Services Directive says: "The proportion of television advertising spots and teleshopping spots within a given clock hour shall not exceed 20 %."
[1634] Helberger 2013, p. 18. See also Smythe 1977.
[1635] See myopia chapter 7, section 4, and on the attraction of "free" offers Ariely 2008 (chapter 3); Hoofnagle & Whittington 2013.
[1636] See Cranor & McDonald 2010, p. 27.

8.4 Consent for tracking technologies

This section discusses how the e-Privacy Directive's consent requirement for the use of tracking technologies could be improved. Human attention is scarce and requiring consent too often overwhelms people. Requiring consent too often also imposes too much transaction costs on people. There's little reason to require consent for truly innocuous practices. In the Data Protection Directive, the balancing provision is an appropriate legal basis for such practices.[1637] Article 5(3) of the e-Privacy Directive already has exceptions for, in short, cookies that are necessary for establishing communication, and cookies that are necessary for a service that's requested by the user.[1638] More exceptions to the cookie consent requirement could be introduced.

The Working Party suggests, in short, that an exception should be introduced for innocuous analytics cookies.[1639] Some analytics cookies could be relatively innocent, for instance if they can only be used to count website visitors and for some basic analysis of which pages are most popular. In such cases, the processing could probably be based on the balancing provision in many circumstances – if it weren't for the e-Privacy Directive. A right to opt out might suffice under general data protection law, assuming the firm complies with all other data protection principles.[1640] As an aside: it's questionable whether the popular analytics software Google analytics would fall within the exception suggested by the Working Party. Google could use the system to track people across the web.[1641]

It might be better if the lawmaker phrased the consent requirement for tracking in a more technology neutral way. Such a rule could be included in the general data

---

[1637] See chapter 6, section 2, on the balancing provision (article 7(f) of the Data Protection Directive).
[1638] See chapter 6, section 4.
[1639] Article 29 Working Party 2012, WP 194, p. 10-11. A similar exception for innocuous analytics cookies is proposed in the Netherlands (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).
[1640] It's also conceivable that no personal data are processed, depending on how the analytics software works.
[1641] It's unclear whether Google uses Google Analytics to track people from website to website. Google says on one of its web pages: "The Google Analytics Tracking Code also reads the double-click [advertising] cookie (…)" (Google Developers 2014). See on DoubleClick: chapter 2, section 2.

protection regime, rather than in the e-Privacy Directive. The law could require consent for collecting and further processing of personal data, including pseudonymous data, for behavioural targeting and similar purposes – regardless of the tracking technology.[1642] As outlined in chapter 6, one of the aims of article 5(3) is to protect people against surreptitious tracking.[1643] It doesn't make sense if the law only protects people against surreptitious tracking if it involves storing or accessing information on a user's device.[1644]

Phrasing the consent requirement for behavioural targeting in a more technology neutral way could also mitigate another problem. In some ways the scope of article 5(3) seems too narrow. For instance, it's unclear whether the provision applies if firms use passive device fingerprinting for behavioural targeting. Passive device fingerprinting relies on looking at information that a device discloses, such as the type of browser, installed fonts, and other settings. The device could send such information as a part of standard network traffic.[1645] It could be argued that passive device fingerprinting doesn't involve "access to information already stored" on a device.

In theory the lawmaker could try to ensure, for instance in a recital, that article 5(3) also applies to information that is emitted by devices. But this might make the scope of article 5(3) too wide. Take the following hypothetical. A train company estimates how many people there are in each carriage, by capturing the signal from their phones. The company immediately deletes all unique identifiers and aggregates the data, thereby anonymising the data.[1646] The company only knows that there are 50

[1642] Perhaps the profiling definition (article 4(3)(a)) of the LIBE Compromise, proposal for a Data Protection Regulation (2013) could serve as a starting point for a legal definition of behavioural targeting. The Dutch lawmaker has tried to capture behavioural targeting in legal language in the Telecommunications Act (for a translation see Zuiderveen Borgesius 2012, p. 5).

[1643] Article 5(3) also has other aims; see chapter 6, section 4.

[1644] If article 5(3) were revised, it should be remembered that the current provision also aims to protect people against unauthorised access to information on their devices. See chapter 6, section 4.

[1645] See chapter 2, section 2. The Working Party said in December 2013 that it was planning to release guidance on device fingerprinting, but at the time of writing this isn't published yet (Article 29 Working Party (Work programme 2014-2015)).

[1646] For this example, we will assume anonymisation is possible. See chapter 5, section 3 for the difficulties of anonymisation.

people in car A, 3 people in car B, and so on. The company uses this information to display on electronic signs which cars still have seating. The processing is limited to counting people and deleting the personal data. Assuming the company offers a clear and easy way to opt out and complies with all data protection principles, it could be argued that the processing can be based on the balancing provision. However, if article 5(3) would apply to capturing any signals emitted by user devices, the company would have to ask consent. Such a consent requirement might annoy travellers and hamper the introduction of a useful service. Following this line of thinking, it would be best not to apply article 5(3) to all information that is disclosed by devices. True, it could also be argued that the risks involved in the hypothetical service are too high and that, therefore, an opt-in system should be required. In any case, general data protection law allows for a more nuanced assessment than the hard consent requirement of article 5(3) of the e-Privacy Directive.

Even if people realise that they are being tracked through device fingerprinting or through a built-in device identifier, it's difficult to defend themselves. It's hard for users to hide their device's fingerprint, or to change the device identifier. The Working Party says "[u]nique, often unchangeable, device identifiers should not be used for the purpose of interest based advertising and/or analytics, due to the inability of users to revoke their consent."[1647] Perhaps the law could explicitly prohibit behavioural targeting that relies on identifiers that are difficult to delete or change. Or the law could prohibit firms from using tracking technologies that are likely to be unknown for the average user, unless firms take measures to make the tracking transparent and controllable.[1648] Such a requirement could already be read in the current transparency principle.

Firms can behave in a manner that might formally comply with the e-Privacy Directive's consent requirement, while breaching the spirit of the law.[1649] For instance,

---

[1647] Article 29 Working Party 2013, WP 202, p. 17.
[1648] See 35th International Conference of Data Protection and Privacy Commissioners 2013.
[1649] See on such "creative compliance" chapter 8, section 1.

website publishers can ask repeated consent for every website visit, or show people an avalanche of pop-up windows. It could be argued that such behaviour doesn't comply with the preamble of the 2009 directive, which amended the e-Privacy Directive. "The methods of providing information and offering the right to refuse should be as user-friendly as possible."[1650] But that doesn't give much guidance. It's hard to preclude firms from breaching the spirit of the law. This is a general problem with laws that require firms to implement opt-in systems to nudge people in a certain direction – if the firm wants to nudge people in the opposite direction.[1651]

8.5 Do Not Track

To foster data subject control, user-friendly systems should be developed to enable people to express their choices. This section discusses an example of such a system: the Do Not Track standard. European Data Protection Authorities have asked browser vendors since 1999 not to allow third party cookies by default.[1652] However, Data Protection Authorities have little legal power to regulate browser vendors.[1653] Data protection law imposes obligations on data controllers. But with behavioural targeting the browser vendor is rarely the data controller. The ad network and the website publisher are joint controllers if they determine the purposes and means of the processing.[1654] At the time of writing most browser vendors allow third party cookies by default. This can probably be partly explained by the fact that the major browser

---

[1650] Recital 66 of Directive 2009/136/EC.
[1651] See section 3 of this chapter.
[1652] Article 29 Working Party 1999, WP 17. "Cookies should, by default, not be sent or stored" (p. 3). See similarly Article 29 Working Party 2010, WP 171.
[1653] More generally, Data Protection Authorities have little legal power to regulate the technical architecture that enables and shapes data processing. An important question is whether there are ways to ensure democratic input and societal debate on the development of such technologies. This research avenue falls outside the scope of this thesis.
[1654] Article 29 Working Party 2010, WP 171, p. 10-12. See on "controllers": chapter 4, section 2.

vendors are connected to firms that use behavioural targeting. The browser users aren't paying customers.[1655]

In the US, the Federal Trade Commission (FTC) has called upon the online advertising industry to adopt a Do Not Track system since 2010. The FTC didn't have a particular system in mind, but did explain what such a system should offer. Among other things, the system should be user-friendly and should stop firms from collecting information if people express a choice not to be tracked.[1656]

The 2009 directive that amended the e-Privacy Directive hints at a user-friendly system for users to give or withhold consent. "Where it is technically possible and effective, in accordance with the relevant provisions of [the Data Protection Directive], the user's consent to processing may be expressed by using the appropriate settings of a browser or other application."[1657] In 2011, EU Commissioner Kroes suggested that a Do Not Track system could enable firms to comply with the e-Privacy Directive's consent requirement.[1658] The Working Party later confirmed that, under certain conditions, a Do Not Track standard could enable firms to comply with the e-Privacy Directive's consent requirement.[1659]

World Wide Web Consortium's DNT Group

Since September 2011, a Tracking Protection Working Group of the World Wide Web Consortium ("DNT Group") has been engaged in a discussion about a Do Not Track standard.[1660] The World Wide Web Consortium (W3C) is an international organisation where member organisations cooperate to develop technical web

---

[1655] See Kristol 2001, p. 169-170; Soghoian 2010; Soghoian 2010a; Wingfield 2010. Mozilla (of the Firefox browser) is an exception. Mozilla receives funding from Google, but doesn't seem to have other connections to behavioural targeting. Apple does have an ad network, but its Safari browser blocks third party cookies. Google (of the Chrome browser) and Microsoft (of the Internet Explorer browser) both use behavioural targeting,
[1656] Federal Trade Commission 2010, p. 63-69. The FTC repeated its call in Federal Trade Commission 2012, p. 53. See also Department of Commerce United States 2010, p. 51; p. 72. See on the early history of Do Not Track Soghoian 2011.
[1657] Recital 66 of Directive 2009/136/EC.
[1658] Kroes 2011.
[1659] Article 29 Working Party 2011, WP 188, p. 10; Kohnstamm (chairman of the Article 29 Working Party) 2012.
[1660] W3C Tracking Protection Working Group (website).

standards.[1661] The W3C standards aren't legally binding; the success of a W3C standard is measured by its rate of adoption.[1662] The DNT Group mainly consists of representatives from firms. But several non-governmental organisations and academics also participate in the discussion, as does a representative of the Article 29 Working Party.[1663] The DNT Group could thus be seen as a multi-stake-holder negotiation.[1664]

The Do Not Track standard should enable people to use their browser to signal to websites that they don't want to be tracked. A website publisher or another firm that receives a "Do not track me" signal could reply to the browser: "OK, I won't track you."[1665] Hence, the Do Not Track standard doesn't actually block third party cookies or other tracking technologies. But if the firm continued to track a person after it replied to that person "OK, I won't track you", the law could come into play. In principle, general contract law could be applied. In contract law an indication of wishes can be expressed in any form, and also implicitly. An automatic "I won't track you" reply to a browser request could be seen as an expression of will to enter an agreement, in which the firm promises it won't monitor browsing behaviour.[1666]

A Do Not Track system could dramatically reduce the transaction costs of opting out of each behavioural targeting firm separately.[1667] In that way, the Do Not Track standard is somewhat comparable with a centralised Do Not Call registry where

---

[1661] See <www.w3.org>.
[1662] See Doty & Mulligan 2013.
[1663] Rob van Eijk (of the Dutch Data Protection Authority) participates for the Working Party. I presented a paper at a workshop that was organised by the DNT Group (Zuiderveen Borgesius 2012), and I have given a presentation on the Dutch Telecommunication Act during a conference call in January 2013.
[1664] See Doty & Mulligan 2013. See generally on self-regulation in the internet context: Bonnici 2008, on technical standards p. 115-150.
[1665] The above is a simplification. The DNT Group foresees more possible answers from firms (W3C, DNT Last Call Working Draft 24 April 2014, section 6.2).
[1666] See on the legal requirements for an expression of will chapter 6, section 1, 3 and 4. See for a US perspective on applying contract law to Do Not Track Fairfield 2012.
[1667] And, unlike the cookie-based opt-out systems offered by the industry, such as the Youronline choices website that is discussed below, Do Not Track doesn't rely on cookies. Therefore, people don't lose their Do Not Track setting if they clear their cookies.

people can opt out of telemarketing. Similarly, some countries have "Robinson lists": databases with names of people who don't want to receive direct marketing mail.[1668]

It's not immediately apparent how Do Not Track – an opt-out system – could help firms to comply with the e-Privacy Directive. But an arrangement along the following lines could be envisioned. Firms should refrain from tracking internet users in Europe that haven't set a Do Not Track preference. Only if a person signals to a specific firm "Yes, you can track me" after receiving sufficient information, that firm may place a cookie to track that user. Hence, in Europe not setting a preference would have the same legal effect as setting a preference for "Do not track me." In Europe, Do Not Track would thus be a system to opt in to tracking.[1669] In countries without a legal requirement to obtain consent for tracking, firms might be allowed to track people who don't set a Do Not Track preference. Do Not Track would thus be a system to opt out of tracking in the US. Since 1 January 2014, a Californian law requires, in short, website publishers to disclose how they respond to Do Not Track signals.[1670]

At the time of writing, after almost three years of discussion, the DNT Group still hasn't reached consensus regarding certain major topics. The most contentious topic is what firms should do when they receive a "Do not track me" signal from somebody. Research shows that most people expect that activating Do Not Track will result in firms not collecting data, in phase 1 of the behavioural targeting process.[1671] In short, people expect Do Not Track really to mean Do Not Collect. Like the Federal

---

[1668] See on Robinson lists Tempest 2007.

[1669] In Europe Do Not Track would be a system to opt in to tracking, as data processing for behavioural targeting is only allowed after consent, and the e-Privacy Directive requires consent for most tracking technologies (see chapter 6). The territorial scope of the e-Privacy Directive and the Data protection Directive is complicated. A full discussion of the territorial scope falls outside this study's scope. See on the territorial scope of EU data protection law the references in chapter 4, section 1, and chapter 1, section 4.

[1670] Business and Professions Code, section 22575-22579.

[1671] McDonald & Peha 2011; Hoofnagle et al. 2012a.

Trade Commission, European Data Protection Authorities say firms should stop collecting data if somebody signals "Do not track me."[1672]

But many firms prefer Do Not Target. They want to continue collecting data when they receive a "Do not track me" signal. The firms merely want to stop showing targeted ads (phase 5). Members of the Digital Advertising Alliance, a large marketing trade group, don't even want to offer Do Not Target. The Digital Advertising Alliance has proposed a system in which firms can continue collecting data, and can continue targeting ads to people who signal "Do not track me." The firms say they'll keep a profile with inferred interests of somebody who signals "Do not track me", but will delete that person's browsing history.[1673] The DNT Group rejected the proposal of the Digital Advertising Alliance.[1674] At the time of writing, there's no agreement in the DNT Group about which data uses should still be allowed when people signal "Do not track me."

Another point of discussion is whether a signal from a browser, or other user agent, with a default setting of "Do not track me" should be respected.[1675] In 2012, Microsoft announced that the next version of its Internet Explorer browser would be set on "Do not track me" by default.[1676] Many marketers responded angrily. Some firms say that default Do Not Track signals don't express a user's choice, and can thus be ignored. Yahoo for instance, one of the largest behavioural targeting firms, said it would ignore the DNT signals from Microsoft Internet Explorer.[1677] There's some irony in this, as currently the behaviour of hundreds of millions of people is monitored while they were never given a choice. And as noted, the Interactive Advertising Bureau UK

[1672] See for instance Kohnstamm (chairman of the Article 29 Working Party) 2012: "According to European laws Do Not Track should be 'do not collect'."
[1673] The Digital Advertising Alliance thus proposes to delete some data in phase (2) of the behavioural targeting process.
[1674] W3C, DNT Last Call Working Draft 24 April 2014, par. 4.
[1675] In theory, this shouldn't be an issue in Europe. As noted, in Europe Do Not Track would be a system to opt in to tracking.
[1676] Lynch 2012.
[1677] Yahoo Public Policy Blog 2012. The Digital Advertising Alliance, a marketing trade group, also said companies don't have to honour the Do Not Track signals from Microsoft's browser (Mastria 2012).

suggests that people can give consent to tracking cookies by leaving the default settings of their browser untouched.[1678]

At the time of writing, the question of how to treat browsers that signal "Do not track me" by default is still subject to debate. In brief, the DNT Group's current view is that browser vendors should not make their browsers signal "Do not track me" by default. This might be different if a browser is explicitly marketed as a privacy-preserving browser, for instance with a brand name like "SuperDoNotTrack."[1679]

Meanwhile, major browser vendors have already technically implemented a system that enables people to signal Do Not Track preferences. Many people have selected the "Do not track me" setting. Some estimate that "Do Not Track is already set in about 20% of browser requests to European websites."[1680] However, most behavioural targeting firms ignore Do Not Track signals, saying they don't know what "Do not track me" means.[1681] For instance, the Chief Privacy Officer of Yahoo reportedly said in 2011: "[r]ight now, when a consumer puts Do Not Track in the header, we don't know what they mean."[1682] Google has reportedly expressed similar opinions.[1683]

From the start, proposals for a Do Not Track standard have excluded tracking within one website.[1684] In brief, there's agreement within the DNT Group that tracking within one website shouldn't be affected by "Do not track me" signals. This would imply that firms such as Amazon or Facebook are allowed to analyse people's behaviour within their own website, regardless of whether people signal "Do not track me." In contrast, the e-Privacy Directive's consent rule also applies to first party tracking

---

[1678] See chapter 6, section 4.
[1679] W3C, DNT Last Call Working Draft 24 April 2014, par. 4.
[1680] Baycloud Systems 2014. The US Interactive Advertising Bureau has claimed: "My members [are] seeing 20-25% of user base sending flag. (…) We expect DNT:1 signals to approach 50% in short-term" (Zaneis 2013).
[1681] Some firms, such as Twitter, say they stop collecting data when they receive a "Do not track me" signal (Twitter 2012). Mayer & Narayanan (Donotrack.us website) give a list of firms that are taking steps to honour Do Not Track signals.
[1682] Quoted in Mullin 2011.
[1683] Mullin 2011.
[1684] Schunter & Swire 2013, p. 12. Some complain that Do Not Track helps larger firms such as Google and Facebook and hurts ad networks that don't offer consumer services (see Chapell 2014).

cookies.[1685] Therefore, it's hard to see how a Do Not Track standard that doesn't apply to first party tracking could help firms to comply with the e-Privacy Directive.

In April 2014 the DNT Group published a "last call working draft" of the Tracking Preference Expression document, with the *technical* requirements for a Do Not Track standard. A last call is an invitation for people inside and outside W3C to comment on the technical soundness of a proposed standard. But many major issues remain undecided, and must be set out in another document (the Tracking Compliance and Scope specification). For instance, the DNT Group still has to decide which types of data can be processed according to the standard when people signal "Do not track me."

> Of note, this document does not define site behavior for complying with a user's expressed tracking preference (…). The Tracking Compliance and Scope (TCS) specification which standardizes how sites should respond to Do Not Track requests, including what information may be collected for limited permitted uses despite a Do Not Track signal, is under discussion.[1686]

A few days after the DNT Group published the last call working draft, Yahoo announced it wouldn't honour Do Not Track signals.[1687] Hence, it seems questionable whether the standard will be widely respected by firms. And meanwhile, the Do Not Target versus Do Not Collect debate continues.

To enable websites to comply with EU law, the Do Not Track standard should at least comply with the following two conditions. First, firms must not collect data for

---

[1685] See chapter 6, section 4..
[1686] W3C, DNT Last Call Working Draft 24 April 2014, introduction. See section 6.2.1 of the document for the proposed definition of tracking.
[1687] Yahoo Public Policy Blog 2014.

behavioural targeting about people in the EU who don't set a preference. Silence is not consent after all.[1688] Second, if a person visits a website and signals "Do not track me", the website and its partners shouldn't follow that person's activities. No tracking should generally mean no data collection.[1689] Some minor exceptions may be needed for this rule. For instance, in some cases it may be necessary for website publishers to store the IP address of certain visitors for a short period, for security reasons.[1690]

Tracking walls and take-it-or-leave-it choices

From the beginning of the discussions, the Do Not Track standard would allow a website to ask a visitor who signals "Do not track me" for an exception, along the following lines. "We see your Do Not Track signal. But do you make an exception for me and my ad network partners so we can to track you?"[1691] Hence, if a standard were developed that complied with EU law, many websites would probably respond by installing tracking walls. This would be comparable with the situation that would result from strictly implementing article 5(3) of the e-Privacy Directive.[1692]

The possibility of tracking walls and take-it-or-leave-it choices isn't a flaw of the Do Not Track system, but a logical consequence of the general principle of contractual freedom, and of the consent rules in the Data Protection Directive.[1693] If a "Do not track me" setting leads to being confronted with tracking walls on many websites, people might change their setting to forego that extra click.[1694] And people might just click "yes" to requests for exceptions.[1695] In sum, a hypothetical Do Not Track standard that complied with EU law would probably bring us back to the problem of tracking walls.

[1688] See chapter 6, section 3.
[1689] See Kohnstamm (chairman of the Article 29 Working Party) 2012.
[1690] See on that topic Soghoian 2011a.
[1691] See for instance W3C, DNT Last Call Working Draft 24 April 2014, section 7.
[1692] See section 3 of this chapter, and chapter 6, section 3 and 4.
[1693] See on tracking walls and take-it-or-leave-it choices chapter 6, section 3 and 4, and chapter 8, section 3.
[1694] See Strandburg 2013, p. 169-170.
[1695] See chapter 7, section 3 and 4.

Other possibilities for user-friendly consent mechanisms

Do Not Track could be seen as a system that aims to make consent more meaningful. There would be other possibilities to enable people to express their choices. For instance, a centralised system could be developed where people can choose to be tracked.[1696] The Interactive Advertising Bureau (IAB) shows such as system would be possible. The IAB runs a website where people can opt out of receiving targeted ads: youronlinechoices.com. There are, however, serious problems with the website. For instance, the website merely offers the equivalent of Do Not Target. Firms may continue to track people who have opted out.[1697] The website's FAQ explains: "[d]eclining behavioral advertising only means that you will not receive more display advertising customised in this way."[1698] But it seems plausible that people expect the website to offer Do Not Collect.[1699]

Additionally, the site works with opt-out cookies. Hence, if a person clears his or her cookies – a measure that is often suggested to limit tracking – the opt-outs are lost.[1700] Furthermore, in 2011 the Working Party noted that the Youronlinechoices website included code that enables user tracking, while users weren't informed about this.[1701] Nevertheless, the website does show that a centralised system for firms to obtain consent for tracking would be possible.

In sum, if a Do Not Track standard were developed that complied with EU law, many websites would probably respond by installing tracking walls. Even if firms provided

---

[1696] See Article 29 Working Party 2011, WP 188, p. 6.
[1697] Article 29 Working Party 2011, WP 188, p. 7. As an aside, suggesting to people that they can opt out of tracking while they can only opt out of receiving behaviourally targeted ads is hard to reconcile with article 7 of the Unfair Commercial Practices Directive on "misleading omissions". See on consumer law chapter 4, section 4.
[1698] Interactive Advertising Bureau Europe – Youronlinechoices.
[1699] In the US there's a similar website. Research suggests that many people expect it to offer Do Not Collect rather than Do Not Target (Cranor & McDonald 2010, p. 18).
[1700] In reaction to the Federal Trade Commission's call for a Do Not Track system, Google has released an extension for its Chrome browser in 2011: "Keep My Opt-Outs". This extension "enables you to opt out permanently from ad tracking cookies." See Google Public Policy Blog 2011.
[1701] Article 29 Working Party 2011, WP 188, p.7.

clear information, even if people understood the information, and even if firms asked prior consent, people might still feel they have to consent to behavioural targeting.

8.6 Conclusion

This chapter discussed how the law could improve individual empowerment in the behavioural targeting area. Strictly enforcing the data protection principles would be a good start. The law also needs amendments.

Of course, the Data Protection Directive is only relevant if the practice of behavioural targeting is found to come within the directive's scope. This will be the case if behavioural targeting is seen as processing personal data. Hence, from a normative perspective, data protection law should apply to behavioural targeting, including when firms use pseudonymous data. Apart from that, as discussed in chapter 5, a sensible interpretation of data protection law implies that data that are used to single out a person should be seen as personal data.

To reduce the information asymmetry in the area of behavioural targeting, the transparency principle should be enforced. In line with European consumer law, the lawmaker should require firms to phrase privacy policies and consent requests in a clear and comprehensible manner. Codifying the clear language requirement could discourage firms from using legalese in privacy policies. The rule wouldn't be enough to ensure actual transparency, but it could help to lower the costs of reading privacy policies. Furthermore, interdisciplinary research is needed to develop tools to make data processing transparent in a meaningful way.

Regarding consent, the existing rules must be enforced. Even though website publishers have started to inform visitors about cookies, many fail to ask consent for behavioural targeting, or don't even offer an option to opt out of tracking. Firms shouldn't be allowed to infer consent from mere silence. This follows from legal doctrine. Furthermore, behavioural economics insights suggest that requiring opt-in

consent could nudge people towards disclosing fewer data. The European Commission proposal reaffirms that consent requires a clear expression of will.

Human attention is scarce and too many consent requests can overwhelm people. One problem with the consent requirement for tracking technologies in article 5(3) of the e-Privacy Directive is that the scope of article 5(3) has proven to be too broad. Article 5(3) also applies to some cookies that pose little privacy risks and that aren't used to collect detailed information about individuals, such as certain types of cookies that are used for website analytics. But there's little reason to ask consent for truly innocuous practices. It would probably be better if the lawmaker phrased the consent requirement for tracking in a more technology neutral way. The law could require consent for the collection and further processing of personal data, including pseudonymous data, for behavioural targeting and similar purposes – regardless of the technology that's used. An option that could be explored is whether a separate legal instrument is needed for behavioural targeting (see section 7 of the next chapter).

Furthermore, a user-friendly system should be developed to make it easier for people to give or refuse consent. Work is being done in this area. The Tracking Protection Working Group of the World Wide Web Consortium (DNT Group) is in the process of trying to develop a Do Not Track standard. The Do Not Track standard should enable people to signal with their browser that they don't want to be tracked. But even a hypothetical Do Not Track system that would comply with European law would probably lead to tracking walls. The next chapter examines whether specific rules regarding such take-it-or-leave-it choices are needed in some circumstances.[1702]

How should the suggestions in this chapter be assessed in the light of the central question of this thesis: how could European law improve privacy protection in the area of behavioural targeting, *without being unduly prescriptive*? In this study, the

---

[1702] Chapter 9, section 5 and 7.

"not unduly prescriptive" requirement means that measures shouldn't be unreasonably costly for society, or unreasonably paternalistic.

Enforcing and tightening data protection law's transparency requirements wouldn't be unduly paternalistic, if at all. Requiring firms to be transparent about behavioural targeting doesn't interfere with the data subject's liberty.[1703] Furthermore, from an economic perspective, markets don't function well when there's information asymmetry. Protecting a well-functioning market has nothing to do with paternalism. Requiring firms to use an opt-in system for valid consent (rather than an opt-out system) could be seen as a measure to nudge people towards disclosing less personal information. As the data subject can still allow tracking, by giving consent, such a rule hardly interferes with the data subject's liberty. This implies that an opt-in requirement isn't very paternalistic. Apart from the fact that a nudge hardly interferes with liberty, there are other rationales for an opt-in requirement than protecting the data subject against him or herself.[1704] Again this implies that opt-in requirements aren't unduly paternalistic.

Drafting readable privacy policies costs time and money. The costs of relatively simple measures, such as avoiding legalese in consent requests and privacy policies, may be manageable. While not too costly, the effectiveness of such measures remains to be seen; they must be tested in practice. However, making data processing transparent in a meaningful way may require serious investments, for instance in design and research.[1705] In some cases other measures, such as mandatory rules or prohibitions, may be cheaper.[1706] In sum, the costs of empowering the individual shouldn't be underestimated, and in some cases they can be considerable. But in general it can't be said that the costs are unreasonable.

[1703] See the paternalism definition in chapter 6, section 6.
[1704] In US literature, nudges are sometimes called "libertarian paternalism" (Sunstein & Thaler 2008, introduction). Some see nudges as (too) paternalistic; see e.g. Mitchell 2004. This depends largely on the paternalism definition one uses.
[1705] See on transparency enhancing tools (TETs): chapter 9, section 6.
[1706] See Helberger 2013a, p. 28.

In conclusion, aiming for data subject control isn't a panacea, but compared to the current situation, where hundreds of millions of people are tracked without being aware, some improvement must be possible. Enforcing and tightening the data protection principles could help to empower the data subject. However, aiming for individual empowerment alone won't suffice to defend privacy in the area of behavioural targeting. Even if firms provided clear information, even if people understood the information, and even if firms asked prior consent, many people might still feel they must consent to behavioural targeting when encountering take-it-or-leave-it choices. Hence, protection of the individual is needed as well. This approach is discussed in the next chapter.

* * *