Improving privacy protection in the area of behavioural targeting

Zuiderveen Borgesius, F.J.

Publication date
2014
Document Version
Final published version

6 Informed consent in data protection law

Informed consent plays a central role in the current regulatory framework for behavioural targeting. Therefore, this chapter examines the role of informed consent in data protection law. The e-Privacy Directive requires consent for the use of tracking cookies and similar technologies. And unambiguous consent is generally required as a legal basis for personal data processing for behavioural targeting.

The requirement for firms to obtain the individual's consent for certain practices is indicative of data protection law's aim to put people in control of their personal data. But while consent plays an important role in data protection law, this chapter shows the role is also limited. Data subjects can't set data protection law aside with consent.

A data controller may only process personal data on the basis of the data subject's consent, or on one of the other five legal bases. Article 7 of the Data Protection Directive lists the six possible legal bases to process personal data, starting with (a) consent. The other legal bases only allow processing when it's "necessary." Briefly stated, the other legal bases are as follows. Data processing is allowed if it's necessary (b) for the performance of a contract with the data subject, (c) to comply with a legal obligation, (d) to protect the data subject's vital interests, (e) for a task carried out in the public interest, for instance by the state, or (f) for legitimate interests of the controller that outweigh the data subjects fundamental rights.[984] This study refers to this last legal basis (f) as the balancing provision. The European Commission proposal for a Data Protection Regulation copies the same legal bases without major

[984] Article 7 of the Data Protection Directive. See for an introduction on the legal bases Article 29 Working Party 2014, WP 207, p. 16-21. See on the six legal bases and behavioural targeting Van Der Sloot & Zuiderveen Borgesius 2011, p. 99-100.

revisions.[985] For the private sector, the three most relevant legal bases are consent, a contract, or the balancing provision; the study focuses on these.

Section 6.1 of this chapter discusses a contract with the data subject, section 6.2 the balancing provision, and section 6.3 the data subject's consent. Section 6.4 discusses the e-Privacy Directive's consent requirement for the use of tracking technologies. Section 6.5 analyses the role of consent in data protection law, and shows the role is important, but also limited. People can't set data protection provisions aside by giving consent, or by contractual agreement. Hence, data protection law limits the data subject's contractual freedom. Nevertheless, section 6.6 rejects the idea that data protection law is too paternalistic. Section 6.7 concludes.

6.1 Contract

A first legal basis that a firm can rely on for processing personal data is a contract. Data processing is allowed when it's "necessary for the performance of a contract to which the data subject is party (…)."[986] For example, a shop has to process certain personal data when somebody pays with a credit card. And a magazine publisher doesn't need to obtain consent to process the name and address of a subscriber, as far as these personal data are needed to deliver the magazine at the subscriber's home. The personal data are "necessary" to deliver the magazine to the subscribers and thus to fulfill the contract.[987]

Many firms can't base the processing of personal data for behavioural targeting on a contract. For instance, if an ad network collected data about people without them being aware, it's difficult to see how it could have entered a contract with those people. To illustrate, the Working Party has examined Google's privacy policy, after Google made amendments in March 2012, which allowed Google to combine user

---

[985] Article 6 of the European Commission proposal for a Data Protection Regulation (2012).
[986] In some cases firms can also rely on this ground prior to entering a contract. See article 7(a) of the Data Protection Directive. See also chapter 9, section 6, on article 15 of the Data Protection Directive.
[987] See for a similar example College bescherming persoonsgegevens (Dutch DPA) 2013 (Google), p. 77.

data across most Google services. According to the Working Party, Google can't rely on the legal basis contract for combining data across its various services.[988] Similarly, the Dutch Data Protection Authority rejects the idea that Google could rely on a contract to process personal data of people who Google tracks through its ad networks, because people haven't accepted any offer.

> Passive users (…), in other words visitors to websites that use Google's (advertising) services, do not receive any proposal from Google to enter into a contract, electronically or otherwise. So they can hardly be said to have accepted an offer (since they have not even received one). Passive users will in most cases not even be aware that they have encountered or will encounter Google cookies when using third-party websites. The Terms of Service therefore certainly do not give rise to a contractual relationship with the passive users.[989]

Necessity

For a firm to be able to rely on the legal basis contract, the processing must be "necessary" for the performance of a contract with the data subject.[990] The *Huber* case of the European Court of Justice gives guidance for the interpretation of "necessary" in the Data Protection Directive. According to the Court, necessity "is a concept which has its own independent meaning in Community law."[991] The Court emphasises that data processing must be proportionate to the goal pursued. For instance, if

---

[988] Article 29 Working Party 2013 (Google letter). See in more detail on the investigation into Google chapter 8, section 1.
[989] College bescherming persoonsgegevens (Dutch DPA) 2013 (Google), p 85. See along similar lines CNIL 2014 (Google), p. 24-25.
[990] In some cases firms can also rely on this ground prior to entering a contract. See article 7(a) of the Data Protection Directive. See also chapter 9, section 6, on article 15 of the Data Protection Directive.
[991] ECJ, C-524/06, Huber, 16 December 2008, par. 52.

anonymous data can be used to achieve the same goal, no personal data should be retained.[992] As the Advocate General explains, the word necessary sets a higher threshold than "more convenient, easier or quicker."[993] The Advocate General refers to the case law of the other European Court, the European Court of Human Rights. The latter says "[t]he adjective 'necessary' is not synonymous with 'indispensable', neither has it the flexibility of such expressions as 'admissible', 'ordinary', 'useful', 'reasonable' or 'desirable' (…)."[994] Case law of the latter court confirms that data processing must be proportionate in relation to the processing purpose.[995]

It's sometimes suggested that "necessary" in the Data Protection Directive must always be interpreted as "necessary" in the case law of the European Court of Human Rights.[996] But caution is needed when interpreting this case law from Strasbourg and Luxembourg. In the *Huber* case of the European Court of Justice, the state was the data controller. The state didn't aim to rely on the legal basis contract, but on another legal basis: data processing is "necessary for the performance of a task carried out in the public interest" (article 7(e)).[997]

An argument can be made that firms should have more leeway than the state. Some might argue that people primarily need protection against the state, rather than against other private actors. This would suggest that "necessary" must be interpreted more leniently when there is a legal basis contract (article 7(b)), than when applying article 7(e), regarding processing for public interests. On the other hand, the aim of the state

---

[992] ECJ, C-524/06, Huber, 16 December 2008, par. 60, par. 65-68, and dictum. As noted, the proportionality is one of the core principles of data protection law. See chapter 4, section 2.
[993] Opinion AG (3 April 2008) for ECJ, C-524/06, Huber, 16 December 2008, par. 29.
[994]ECtHR, Silver and Others v. United Kingdom, No. 5947/72; 6205/73; 7052/75; 7061/75; 7107/75; 7113/75; 7136/75, 25 March 1983, par 97.
[995] ECtHR, S. and Marper v. United Kingdom, No. 30562/04 and 30566/04. 4 December 2008, par. 103. See about "necessary in a democratic society" in the article 8 case law Harris et al. 2009, p. 349-359.
[996] For instance, the Dutch legislator interprets "necessary" in the Dutch Data Protection Act the same as "necessary" in the case law of the European Court of Human Rights, and the Dutch Data Protection Authority also takes this view. (See College bescherming persoonsgegevens 2013 (Google), p. 76-77). Some commentators take a similar view (see e.g. Kranenborg & Verhey 2011, p. 84; Bygrave & Schartum 2009, p. 163). See critically on interpreting "necessary" in data protection law the same way as in article 8 of the European Convention on Human Rights: González Fuster & Gutwirth 2013, p. 538.
[997] But see Bygrave, who suggests "necessary" in other data protection law provisions should probably be interpreted the same (Bygrave 2014, p. 150).

should be to work for the common good, while firms aim for profit. This would suggest that a firm should have less leeway.[998] Without taking sides in this debate, it's clear that it's not enough that a firm finds it helpful or profitable to process personal data; the concept of necessity requires more.

The question of necessity can be divided into two steps: subsidiarity and proportionality.[999] The subsidiarity question concerns whether the firm could pursue its purpose in another way that's less intrusive. The relevant question is whether a lighter measure is available. That lighter measure doesn't have to perform as well as the measure in question, according to the Advocate General in the *Huber* case. "It is not necessary for the alternative system to be the *most* effective or appropriate; it is enough for it to be able to perform adequately."[1000] The second question regarding necessity is whether the data processing is proportionate. In other words, do the measures not exceed the limits of what is appropriate and necessary in order to achieve the objective?[1001]

Necessity for the performance of a contract

The Working Party says that the legal basis contract isn't appropriate for behavioural targeting. The processing has to be genuinely necessary for providing the service in question. According to the Working party, "it is important to determine the exact rationale of the contract, i.e. its substance and fundamental objective, as it is against this that it will be tested whether the data processing is necessary for its performance."[1002] Therefore, in general, firms can't rely on the legal basis contract for behavioural targeting.[1003]

---

[998] See Gutwirth 2002, p. 38.
[999] See for instance College bescherming persoonsgegevens (Dutch DPA) 2013 (Google), p. 76-77; p. 87-88.
[1000] Opinion AG (3 April 2008) for ECJ, C-524/06, Huber, 16 December 2008, par 16 (emphasis original).
[1001] See on the proportionality principle in data protection law: chapter 4, section 2.
[1002] Article 29 Working Party 2014, WP 217, p. 17.
[1003] The Working Party's view that behavioural targeting can be based on article 7(b) doesn't receive much criticism in the literature. Google appears to invoke the legal basis contract for behavioural targeting, but Data

> Article 7(b) is not a suitable legal ground for building a profile of the user's tastes and lifestyle choices based on his click-stream on a website and the items purchased. This is because the data controller has not been contracted to carry out profiling, but rather to deliver particular goods and services, for example. Even if these processing activities are specifically mentioned in the small print of the contract, this fact alone does not make them "necessary" for the performance of the contract.[1004]

The analysis becomes more complicated if a firm uses the same personal data for behavioural targeting and to provide its service. Suppose a firm offers an app with a personalised news service. The app analyses the user's reading habits and recommends other news articles based on the user's earlier media consumption. Processing some personal data (the user's reading habits tied to a unique identifier) is necessary for performing the contract, as the app can only offer its personalised news service by analysing the user's personal data. That processing can be based on the legal basis contract (b), because the processing is necessary for the performance of the contract. But following the Working Party's reasoning, it's not necessary for provision of the personalised news service to use the same personal data for targeted advertising. Hence, the firm must obtain consent for behavioural targeting if the firm wants to use the same data to target ads to the user.[1005]

Perhaps a firm that provides a social network site could try to argue that it can base personal data processing for behavioural targeting on a contract.[1006] A social network site provider has a direct relationship with its user. The firm would have to argue that

---

Protection Authorities in France and the Netherlands reject this idea (CNIL 2014 (Google), p. 25; College bescherming persoonsgegevens 2013 (Google), p. 85-87).

[1004] Article 29 Working Party 2014, WP 217, p. 17.

[1005] See Article 29 Working Party 2013, WP 202, p. 13.

[1006] In some cases, the user of a social network site could be seen as a data controller, but we'll leave this complication aside (see Article 29 Working Party 2009, WP 163; Helberger & Van Hoboken 2010).

it entered a contract with the user when the user opened an account. And the firm would have to argue that behavioural targeting "is necessary for the performance of a contract" with the data subject (the user). The "contract" would imply that the user discloses personal data, in exchange for the use of the service.[1007]

Indeed, European social network providers have argued that personal data processing for behavioural targeting is "part of the processing that is necessary for the performance of a contract to which the data subject is party." They add "it is absolutely necessary to provide a legal basis for denying services to users that refuse to be the subjects of targeted advertising."[1008] Facebook makes a similar argument.[1009] But the Working Party says "[t]he user should be put in a position to give free and specific consent to receiving behavioural advertising, independently of his access to the social network service."[1010] Literature also suggests that the legal basis "necessary for the performance of a contract" must be interpreted narrowly.[1011]

If a firm could rely on a contract with the data subject as a legal basis for personal data processing for behavioural targeting, the tracking and further processing would be subject to the contract. Arguably Data Protection Authorities should be more cautious when interpreting the contents of a contract, than when explaining the requirements for consent, which is a sui generis construction of data protection law. It could be argued that for the interpretation of contracts, contract law and consumer law set out the primary guidelines. For instance, under consumer law a standard contract term is unfair if, contrary to the requirement of good faith, it causes a significant imbalance to the parties' rights and obligations, to the detriment of the consumer.[1012]

[1007] See on such "exchanges" chapter 7, section 2.
[1008] European Social Networks 2011, p. 5.
[1009] Facebook proposed amendments 2013, p. 27. Facebook proposes the following sentence for recital 34: "Controllers should be able to make consent to the processing a condition of access to a service which may not be otherwise free." See on such take-it-or-leave-it choices section 3 and 4 of this chapter, chapter 7, section 4, and chapter 8, section 3 and 5.
[1010] Article 29 Working Party, WP 187, p. 8; p. 18.
[1011] Kuner 2007, p. 243-244.
[1012] Article 3(1) of the Unfair Contract Terms Directive. As noted in chapter 4, section 4, some EU consumer law principles could be applied to the relation between firms and data subjects.

On the other hand, even if a firm had a legal basis for processing because of a contract, the firm would still have to comply with the other data protection requirements. Therefore, the idea that Data Protection Authorities have little to say about processing that's "necessary for the performance of a contract" isn't very plausible.

There's another reason why the difference between the legal bases consent (article 7(a)) and a contract (article 7(b)) is relevant.[1013] The procedural requirements for consent in data protection law are stricter than for many contracts. In principle, any expression of will is sufficient to enter a contract, although the law sometimes requires formalities.[1014] And in general contract law, terms and conditions are often part of the contract. But as discussed below, according to the Working Party firms can't obtain consent for data processing through terms and conditions.[1015]

While the difference between the legal bases contract and consent is relevant, in some ways it doesn't matter much which of the two is the legal basis for processing. Chapter 7 discusses practical problems with informed consent to behavioural targeting. These problems would be largely the same if firms could base personal data processing for behavioural targeting on a contract.

In conclusion, the Working Party says a firm can only rely on the legal basis contract if the processing is genuinely necessary to provide the service. The Working Party's view implies that, in general, firms can't rely on this legal basis for behavioural targeting.

[1013] Le Métayer & Monteleone 2009 argue that consenting in data protection law shouldn't be seen as entering a contract (p. 138). See on that topic also Verhelst 2012; Van Der Sloot 2010; Traung 2012, p. 38.
[1014] Zweigert & Kötz 1987, p. 366.
[1015] See section 3 of this chapter, and chapter 8, section 3. See also Article 29 Working Party, WP 187, p. 33-34.

6.2 Balancing provision

A second legal basis that a firm can rely on for personal data processing is the balancing provision, also called the legitimate interest clause. In brief, a firm can rely on the balancing provision when its legitimate business interests, or those of a third party, outweigh the data subject's fundamental rights. The relevant provision is as follows.[1016]

> Member States shall provide that personal data may be processed (…) if: (…)
>
> (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection under article 1(1).[1017]

The balancing provision is the appropriate ground for innocuous standard business practices.[1018] Many data processing practices happen on a small scale and bring limited risks. For instance, a bakery shop might have a list of names and addresses of regular customers on its computer, for the purpose of sending New Year's greeting cards. Within the context of an existing customer relationship, a firm can generally rely on the balancing provision for postal direct marketing for similar products (first

---

[1016] Article 7(f) of the Data Protection Directive. The official English version of the Directive says "for" ("the interests for fundamental rights"). The Directive says "or" in other languages. Therefore I assume that "for" should be read as "or." (See Korff 2005, p. 68, footnote 19; Article 29 Working Party 2014, WP 217, p. 29. The proposal for a Data Protection Regulation also uses "or").

[1017] Article 1(1) of the Data Protection Directive says: "Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy." Therefore, any interest or fundamental right of the data subject could override the interests of the data controller.

[1018] See recital 30 of the Data Protection Directive.

party direct marketing).[1019] It's often assumed that postal direct marketing to non-customers (third party direct marketing) can also be based on the balancing provision.[1020]

The balancing provision is a very open norm and national Data Protection Authorities have diverging interpretations.[1021] To foster a more harmonised approach across Europe, the Working Party released a long and detailed opinion on the balancing provision in 2014.[1022]

Legitimate interests

Can firms base personal data processing for behavioural targeting on the balancing provision? Let's take a simple case as an example: an ad network tracks people's browsing behaviour over thousands of websites, to compile nameless individual profiles, to single people out and target them with advertising.

A preliminary question is whether the firm has a legitimate interest.[1023] As Gutwirth notes, "the ultimate purpose of the processing should be lawful. An illegal or illegitimate interest can never be pursued by a legitimate processing operation."[1024] By way of illustration, if a controller processes personal data with the goal of unlawfully discriminating against people, the interest can't be legitimate.[1025] A legitimate interest must be lawful. The "lawfully" requirement suggests the ad network must also

---

[1019] See for instance article 23(4) of the Data Protection Act of Poland. "The legitimate interests, referred to in [the balancing provision], are considered to be: (1) direct marketing of own products or services provided by the controller (..)." See on first party direct marketing also recital 41 of the e-Privacy Directive.
[1020] The European Commission amended proposal for a Data Protection Directive (1992) says: "This balance-of-interest clause is likely to concern very different kinds of processing, such as direct-mail marketing and the use of data which are already a matter of public record; Member States are to weigh the balance of interest in accordance with procedures which they are to establish taking account in particular of the general principles [of data protection] and of the rights of data subjects" (p. 15). See also Korff 1993, p. 7-8; Korff 2005, p. 43; Carey 2002, p. 106. Recital 39b of the LIBE Compromise, proposal for a Data Protection Regulation (2013) says that postal direct marketing can generally be based on the balancing provision, even if it's not first party marketing.
[1021] Irion & Luchetta 2013, p. 53; Korff 2010a, p. 72-73; Kuner 2007, p. 245; Impact Assessment for the proposal for a Data Protection Regulation (2012), Annex 2, p. 27. Traung 2012 calls the provision "circular nonsense" (p. 41).
[1022] Article 29 Working Party 2014, WP 217, p. 7.
[1023] Article 29 Working Party 2014, WP 217, p. 24-29; Article 29 Working Party 2013, WP 203, p. 12.
[1024] Gutwirth 2002, p. 99.
[1025] See Article 29 Working Party 2013, WP 203, p. 25.

comply with other laws, such as the e-Privacy Directive's consent requirement for tracking technologies.[1026] These requirements are also relevant when a firm relies on a legal basis other than the balancing provision, but the balancing provision emphasises that the firm's interests must be legitimate.

The ad network could invoke its right to conduct a business, as protected by the EU Charter of Fundamental Rights: "[t]he freedom to conduct a business in accordance with Union law and national laws and practices is recognised."[1027] But this right isn't absolute and has to be balanced against other fundamental rights, such as the right to privacy and the right to data protection.[1028] As an aside, a firm that breached data protection provisions or other legal rules wouldn't have a strong case if it invoked its right to conduct a business. Its business wouldn't be "in accordance with Community law and national laws", as required by the Charter.[1029] This implies, for instance, that the firm must comply with the e-Privacy Directive, which requires consent for the use of most tracking technologies.[1030]

The balancing provision speaks of legitimate interests pursued by "the third party or parties to whom the data are disclosed."[1031] If an ad network allows advertisers to advertise to specific people (identified with a cookie for instance), it essentially rents out access to those people. Under the Data Protection Directive, this should probably be seen as a type of data disclosure. The definition of processing speaks of "disclosure by transmission, dissemination *or otherwise making available*."[1032] The ad network makes data available for advertisers, including when it doesn't provide them with a copy of the data. Korff notes that list rental is a type of data disclosure, and his

---

[1026] Article 29 Working Party 2014, WP 217, p. 25.
[1027] Article 16 of the EU Charter of Fundamental Rights. The Advocate General of the European Court of Justice confirms that the provision of online advertising relates to the freedom to conduct a business (Opinion AG (25 June 2013), C-131/12, Google Spain, par 95).
[1028] Article 52(3) of the EU Charter of Fundamental Rights. See also CJEU, C-70/10, Scarlet v Sabam, 24 November 2011, par. 46. The Google Spain case suggests that a firm's economic interests have less weight than the data subject's privacy rights (CJEU, C-131/12, Google Spain, 13 May 2014, par. 81, dictum, 4).
[1029] Article 16 of the EU Charter of Fundamental Rights.
[1030] See section 4 of this chapter.
[1031] The Data Protection Directive defines 'third party" in article 2(f).
[1032] Article 2(b) of the Data Protection Directive.

conclusion can be applied to ad networks by analogy.[1033] In any case, the analysis of the balancing provision remains roughly the same, regardless of whether a firm invokes its own interests, or those of third parties. Let's assume that the ad network in our example has a legitimate interest.[1034]

Necessity

For a firm to be able to rely on the balancing provision, having a legitimate interest is not enough; the processing must be "necessary." As noted, the question of necessity can be divided into two steps: subsidiarity and proportionality.[1035] Regarding subsidiarity: it seems questionable whether tracking people's browsing behaviour is the least intrusive manner possible for the ad network to enable advertisers to promote their products or services. There are many other types of online advertising that are less privacy-invasive, such as contextual advertising (advertising about cars on websites about cars). But an ad network that specialises in behavioural targeting could try to argue that the tracking is necessary for its business model. However, it doesn't follow that the ad network has to track people's browsing behaviour and construct detailed profiles. For the ad network, other ways of pursuing its interests may include finding a way that involves processing less personal data.[1036]

The second question regarding necessity is whether the tracking and further processing is proportionate in relation to the ad network's interests. The processing is disproportionate if it exceeds the limits of what is appropriate to pursue the ad networks business interests.[1037] For some behavioural targeting practices, which entail

---

[1033] Korff 2005, p. 63. With list rental, a list broker sends leaflets to a set of people, but the advertiser doesn't receive a copy of the list. See chapter 2, section 6.
[1034] See Article 29 Working Party 2014, WP 217, p. 25: marketing is a legitimate interest.
[1035] See for instance College bescherming persoonsgegevens (Dutch DPA) 2013 (Google), p. 76-77; p. 87-88.
[1036] Privacy enhancing technologies could help here (see Article 29 Working Party 2014, WP 217, p. 42). See on privacy preserving behavioural targeting chapter 9, section 3.
[1037] See on the proportionality principle in data protection law: chapter 4, section 2.

large-scale collection of detailed information about people, it seems questionable whether they are proportionate.[1038]

If the tracking and further processing is "necessary" for the ad network's legitimate interests, the ad network must pass another hurdle. The balancing provision requires that the ad network's interests "must not be overridden by the fundamental rights and freedoms of the data subject."[1039] The interests of the firm and the data subject must be weighed. When balancing the conflicting interests, it has to be taken into account that the right to data protection and the right to privacy are fundamental rights.[1040]

People have an interest in using the internet without being tracked. Many people find tracking and behavioural targeting intrusive.[1041] Collecting and storing data can cause a chilling effect, and large-scale data storage brings risks, such as data breaches. In some cases there could be a risk of unfair discrimination or manipulation.[1042] People have a reasonable expectation of privacy regarding their internet use, and storage of information about internet use can interfere with the right to private life, regardless of how those data are used.[1043] A Council of Europe resolution suggests that online tracking is a privacy threat:

> [P]ersonal ICT systems as well as ICT-based communications may not be accessed or manipulated if such action violates privacy or the secrecy of correspondence; access or manipulation through "cookies" or other unauthorised

---

[1038] See also chapter 9, section 3, and Kuner 2008.
[1039] Article 7(f) of the Data Protection Directive. This requirement could be seen as a separate, or second, balancing test. See CJEU, C-468/10 and C-469/10, ASNEF, 24 November 2011, par. 38; College bescherming persoonsgegevens (Dutch DPA) 2013 (Google), p. 88. The Working Party distinguishes more steps within the balancing provision (Article 29 Working Party 2014, WP 217).
[1040] CJEU, C-468/10 and C-469/10, ASNEF, 24 November 2011, par. 41. See also ECJ, C-465/00, C-138/01 and C-139/01, Österreichischer Rundfunk, 20 May 2003, par. 68; CJEU, C-131/12, Google Spain, 13 May 2014, par. 74.
[1041] See chapter 7, section 1, for a review of research on people's attitudes towards behavioural targeting.
[1042] See chapter 3, section 3.
[1043] ECtHR, Copland v. United Kingdom, No. 62617/00, 3 April 2007, par. 42. See the case law discussed in chapter 3, section 2.

> automated devices violate privacy, in particular where such automated access or manipulation serves other interests, especially of a commercial nature.[1044]

But the data subject's rights aren't absolute: "under certain conditions, limitations may be imposed", says the European Court of Justice. Therefore, "a fair balance [must] be struck between the various fundamental rights and freedoms protected by the EU legal order."[1045]

When balancing the opposing interests, all circumstances have to be taken into account, such as "the seriousness of the infringement of the data subject's fundamental rights."[1046] Relevant factors can include the sensitivity of the data, the scale of data collection, the reasonable expectations of the data subject, and the risks involved.[1047] For instance, mobile location data are of a rather sensitive nature. Firms can never rely on the balancing provision for processing special categories of data, such as data regarding political opinions or health, as the Data Protection Directive requires "explicit consent" for processing special categories of data for marketing purposes.[1048] The safeguards a firm has in place to protect the data subject's interests should also be taken into account. For instance, does the firm offer sufficient transparency, and does it offer a clear opt-out option?[1049]

In most cases the data subject's interests must prevail over the ad network's interests, as behavioural targeting involves collecting and processing information about personal matters such as people's browsing behaviour. Several authors have already

---

[1044] Parliamentary Assembly, Resolution 1843 (2011) The protection of privacy and personal data on the Internet and online media, 7 October 2011, par 18.6.
[1045] CJEU, C-468/10 and C-469/10, ASNEF, 24 November 2011, par. 43.
[1046] CJEU, C-468/10 and C-469/10, ASNEF, 24 November 2011, par. 44.
[1047] See Article 29 Working Party 2014, WP 217, p. 33-43.
[1048] Article 8 of the Data Protection Directive. There are exceptions for the "explicit consent" requirement, but these aren't relevant for behavioural targeting. Some member states don't accept consent as a legitimate basis for processing special categories of data. See on special categories of data chapter 5, section 6; chapter 9, section 5.
[1049] Article 29 Working Party 2014, WP 217, p. 41. See also WP 185, p. 16; Korff 2005, p. 43; College bescherming persoonsgegevens (Dutch DPA) 2013 (Google), p. 89. See on opting out below, on the right to object.

concluded that ad networks can't rely on the balancing provision for behavioural targeting that involves tracking over multiple websites.[1050] The Dutch lawmaker comes to the same conclusion.[1051] Similarly, the Working Party says that "free, specific, informed and unambiguous 'opt-in' consent (…) should be required, for example, for tracking and profiling for purposes of direct marketing, behavioural advertis[ing], data-brokering, location-based advertising or tracking-based digital market research."[1052] In sum, the most convincing view is that personal data processing for behavioural targeting that relies on following people over various internet services, can't be based on the balancing provision.

It has also been suggested that in some circumstances, firms might be able to base data processing for first party behavioural targeting on the balancing provision. For instance, perhaps an online bookstore that tracks people's behaviour within its website to provide recommendations might be able to rely on the balancing provision. Arguably people are more likely to understand what happens when they see behaviourally targeted ads, which are based on browsing behaviour within one website.[1053]

Right to object

The Data Protection Directive grants data subjects the right to object "on compelling legitimate grounds" to the processing of their data when firms rely on the balancing provision. If there's a "justified objection", the processing may no longer involve those data.[1054] This right is thus not an absolute right, but a qualified right to object.

[1050] See Koëter 2009; Traung 2010, p. 218; Antic 2012, p. 106; Moerel 2014, p. 58; Van Der Sloot 2011.
[1051] See for an English translation of the relevant remarks of the Dutch legislator: College bescherming persoonsgegevens (Dutch DPA) 2013 (Google), p. 81, footnote 294.
[1052] Article 29 Working Party 2013, WP 203, p. 46. See similarly Article 29 Working Party 2014, WP 217, p. 45; Article 29 Working Party 2013 (draft LIBE comments), p. 4; Article 29 Working Party 2013 (Google letter), Appendix, p. 4.
[1053] See Koëter 2009, p. 109-111. In the US, the Federal Trade Commission also says first party marketing could be allowed without consent, while third party marketing requires consent (Federal Trade Commission 2012, p. 44).
[1054] Article 14(a) of the Data Protection Directive.

Therefore, the data subject's reasons for objecting must be balanced against the legitimate interests of the firm.[1055]

In the case of direct marketing, the Data Protection Directive grants data subjects the right to object, without requiring the data subject to have "compelling legitimate grounds." This right to object to direct marketing must be interpreted as an absolute right to object.[1056] As Korff puts it, the Data Protection Directive "speaks of a right to 'object to' rather than a right to prevent or stop the processing in question, but it is clear that the latter is intended. If a data subject exercises the right to object to direct marketing (…), the controller in question must comply with that objection."[1057]

Behavioural targeting is a form of direct marketing, as confirmed in the code of conduct of the Federation of European Direct and Interactive Marketing for the use of personal data in direct marketing, which is approved by the Working party. "Direct marketing in the on-line environment refers to one-to-one marketing activities where individuals are targeted."[1058] The Council of Europe Recommendation on profiling confirms that people have an absolute right to object to profiling for direct marketing (in cases where the profiling doesn't require consent).[1059]

[1055] See CJEU, C-131/12, Google Spain, 13 May 2014, par. 76.
[1056] See Article 29 Working Party 2013, WP 203, p. 35.
[1057] Korff 2005, p 100. Article 14 of the Data Protection Directive is somewhat difficult to read, and provides to alternative possibilities for member states to implement the right to object. Korff 2005 provides an analysis. See also Article 29 Working Party 2013, WP 203, p. 35.
[1058] Capitalisation adapted. The Working Party approved the code in Article 29 Working Party 2010, WP 164. The FEDMA defines direct marketing as follows. "The communication by whatever means (including but not limited to mail, fax, telephone, on-line services etc.) of any advertising or marketing material, which is carried out by the direct marketer itself or on its behalf and which is directed to particular individuals" (code approved in Article 29 Working Party 2003, WP 77).
[1059] Article 5(3) of 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. The Recommendation applies to behavioural targeting (see the profiling definition in article 1(e)), and Polakiewicz 2013.

Proposal for a Data Protection Regulation

The European Commission proposal for a Data Protection Regulation duplicates the balancing provision without major changes.[1060] But the proposal requires a firm that relies on the balancing provision to provide the data subject with information about the legitimate interests pursued by the firm.[1061] The requirement to give this information could already be read in the current regime, as a firm is required to provide all information that's necessary to guarantee fair processing.[1062] But that requirement is rather vague, so it's useful that the proposal requires firms to inform the data subject about how they apply the balancing provision.[1063]

The LIBE Compromise allows firms, under certain conditions, to rely on the balancing provision for behavioural targeting with pseudonymous data.[1064] The Working Party warns that the LIBE Compromise could be misunderstood as allowing firms to base most behavioural targeting practices on the balancing provision, as long as firms use pseudonymous data.[1065]

In conclusion, under current law, personal data processing for behavioural targeting, in particular if it involves tracking an internet user over multiple websites, generally can't be based on the balancing provision. If, in rare circumstances, a firm could rely on the balancing provision for behavioural targeting, the data subject would have the right to stop the data processing: to opt out.

[1060] But see Purtova, who argues that the proposal tilts the balance in favour of data controllers in the new version of the balancing provision (Purtova 2014).
[1061] Article 6(f) and article 14(b) of the European Commission proposal for a Data Protection Regulation (2012).
[1062] Article 10 and 11 of the Data protection Directive. See chapter 4, section 3.
[1063] Like the Data Protection Directive, the European Commission proposal for a Data Protection Regulation (2012) uses ambiguous language to describe the right to object to the use of personal data for direct marketing (article 19(1) and 19(3)).
[1064] See article 2(a), article 6(f), and recitals 38 and 58a of the LIBE Compromise, proposal for a Data Protection Regulation (2013). The LIBE Compromise also requires a "highly visible" opt-out possibility (article 20(1); see also article 19(2)).
[1065] Article 29 Working Party 2013 (draft LIBE comments).

6.3 Consent for personal data processing

If firms want to process personal data, and can't base the processing on the balancing provision or another legal basis, they must ask the data subject for consent. Consent is defined as "any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed."[1066] People can always withdraw their consent.[1067]

Indication of wishes

Consent must be an indication of the data subject's wishes. If there's no indication of wishes there can't be consent, so there's no need to check the other requirements for consent. The predominant view in general contract law is that an indication of wishes can be expressed in any form, and can also be implicit.[1068] Consent in data protection law can also be given in any form.[1069] For instance, dropping ones business card in a bowl with a sign saying "leave your name and address to receive our monthly newsletter" can imply consent to the processing of some personal data.[1070]

Without special circumstances, mere inactivity isn't an indication of wishes. "Consent cannot be inferred from the absolute silence of the data subject," summarises Kosta.[1071] A Council of Europe Resolution confirms that consent for online data processing "requires an expression of consent in full knowledge of such use, namely the manifestation of a free, specific and informed will, and excludes any automatic or tacit usage."[1072]

[1066] Article 2(h) of the Data Protection Directive.
[1067] European Commission amended proposal for a Data Protection Directive (1992), p. 2. See also Kosta 2013a, p. 251, with further references. The European Commission proposal for a Data Protection Regulation (2012) makes the right to withdraw consent explicit in article 7(2).
[1068] Zweigert & Kötz 1987, p. 688.
[1069] Kuner 2007, p. 68; Kosta 2013a, p. 386; Article 29 Working Party, WP 187, p. 11.
[1070] Article 29 Working Party, WP 187, p. 11.
[1071] Kosta 2013a, p. 256. See also Kuner 2007, p. 69.
[1072] Parliamentary Assembly, Resolution 1843 (2011) The protection of privacy and personal data on the Internet and online media, 7 October 2011, par 18(4). The Resolution is not legally binding.

In *Schecke,* the European Court of Justice says that merely informing a person that data processing will take place "thus does not seek to base the personal data processing (…) on the consent" of the data subject.[1073] The Advocate General is more explicit. "Acknowledging prior notice that publication of some kind will happen is not the same as giving 'unambiguous' consent to a particular kind of detailed publication. Nor can it properly be described as a 'freely given specific indication' of the applicants' wishes in accordance with the definition of the data subject's consent in article 2(h)."[1074] Other judgments of the European Court of Justice confirm that consent cannot easily be assumed.[1075]

In case law outside the field of data protection law, the European Court of Justice affirms that consent can't be inferred from inactivity. For instance, in two trademark cases, "implied consent (…) cannot be inferred from (…) mere silence", [1076] and "'consent' (…) must be so expressed that an intention to renounce a right is unequivocally demonstrated."[1077] In a case where the European Commission didn't initiate an infringement procedure, this inactivity "cannot be interpreted as the Commission's tacit consent."[1078]

Likewise, in general contract law, mere silence doesn't constitute an indication of will. According to the Vienna Sales Convention for instance, "[a] statement made by or other conduct of the offeree indicating assent to an offer is an acceptance. Silence or inactivity does not in itself amount to acceptance".[1079] Several proposals for international contract law use the same phrase.[1080] Indeed, it would have peculiar

---

[1073] CJEU, C-92/09 and C-93/09, 9 November 2010, Volker und Markus Schecke and Eifert, par. 63.
[1074] Opinion AG (17 June 2010) for CJEU, C-92/09 and C-93/09, 9 November 2010, Volker und Markus Schecke and Eifert, par. 79.
[1075] The Court suggests that "consent" in the Data Protection Directive requires "express" consent (CJEU, C-28/08 and T-194/04, Bavarian Lager, 29 June 2010). And the Court reads "an opportunity to determine" as requiring "prior", "free, specific and informed consent" (CJEU, C-543/09, 5 May 2011, Deutsche Telekom, par. 55-58).
[1076] ECJ, C-414/99 to C-416/99, 20 November 2001, Zino Davidoff, par. 55.
[1077] CJEU, C-482/09, 22 September 2011, Budějovický Budvar, par. 42-44.
[1078] CJEU, C-577/08, 29 June 2010, Brouwer, par. 39.
[1079] Article 18(1) of the Vienna Convention on International Sale of Goods.
[1080] The same phrase is used in article II 4:204(2) of the Draft Common Frame of Reference (Principles, Definitions and Model Rules of European Private Law), and article 34 (of Annex 1) of European Commission

results if the law allowed a seller to infer an expression of will from mere silence. A shop owner could demand payment if somebody failed to object to an offer to buy a TV.

After the European Commission presented its first proposals for a Data Protection Directive in the early 1990s, firms argued that giving people the possibility to object should suffice in order to obtain consent. The International Chamber of Commerce, a business lobbying organisation, said for instance: "[s]ince new products and services constantly emerge, it is virtually impossible for the customer or the controller (…) to foresee at the outset all the specific applications for which the customer's data could be used"[1081] If the law required unambiguous consent, "[c]ompanies would be faced with administrative burdens and potential delays in introducing new services."[1082] The International Chamber of Commerce added that opt-out systems should suffice in order to obtain consent.

> It is far more common to employ a notice or 'opt out' approach, under which individuals are informed of the use to be made of personal data and have the opportunity to object to those uses. Such an approach, or other forms of implied consent, would offer individuals an effective protection of their personal data without putting undue restrictions on all use of personal information.[1083]

The EU lawmaker didn't follow such suggestions in the final text of the 1995 Directive.[1084] The 2012 European Commission proposal for a Data Protection

---

2011 (proposal Common European Sales Law). Inertia selling, where a firm sends consumers a product and demands payment if they don't return the product, is banned in the Consumer Rights Directive (article 27).

[1081] International Chamber of Commerce 1992, p. 261.

[1082] International Chamber of Commerce 1992, p. 261. See for a similar argument regarding the 2012 proposals: Amazon proposed amendments.

[1083] International Chamber of Commerce 1992, p. 261.

[1084] Kosta 2013a, p. 83-108.

Regulation has led to comparable lobbying in favour of opt-out systems. The arguments used are still remarkably similar to those in the 1990s, although nowadays they're usually coupled with remarks about "big data."[1085]

In the UK regulators and commentators seem to be more inclined to accept a system that allows people to object – an opt-out system – as a way of obtaining "implied consent."[1086] For instance, the English Information Commissioner's Office (ICO), the regulator that oversees compliance with the e-Privacy Directive, drops cookies through its website as soon as a visitor arrives, and explains in a banner that it has done so. The ICO appears to suggest that explaining how a user can delete cookies is enough to obtain "implied consent."[1087] The English notion of implied consent has led to an infringement proceeding by the European Commission. In brief, the English implementation of the e-Privacy Directive accepted a form of implied consent as a justification to interfere with the confidentiality of communications. This became salient when a firm called Phorm assumed that people had consented to deep packet inspection for behavioural targeting. The European Commission closed the infringement proceeding after the United Kingdom amended its law.[1088]

Viewing an opt-out system as sufficient to obtain consent has been met with criticism in literature. For example, Kosta says "there is no such thing as 'opt-out consent'."[1089] She adds that "reference to 'opt-out' consent is a misnomer. An 'opt-out' regime refers to the right of a data subject to object to the processing of his personal data and does not constitute consent."[1090] The Working Party confirms that consent needs

---

[1085] See for instance Interactive Advertising Bureau United Kingdom 2012; Amazon proposed amendments; International Chamber of Commerce 2013.
[1086] Kosta 2013a, p. 192. See also Impact Assessment for the proposal for a Data Protection Regulation (2012), p. 19.
[1087] The banner says: "We have placed cookies on your computer to help make this website better. You can change your cookie settings at any time. Otherwise, we'll assume you're OK to continue" (Information Commissioner's Office 2013a)
[1088] European Commission 2009; European Commission 2012. The new law only allows interception where both the sender and recipient have consented to it (The Regulation of Investigatory Powers (Monetary Penalty Notices and Consents for Interceptions) Regulations 2011 You are here: 2011 No. 1340). See on Phorm chapter 2, section 2. See also McStay 2011, p. 15-42; Bernal 2011.
[1089] Kosta 2013a, p. 202.
[1090] Kosta 2013a, p. 387. See also Traung 2012; McStay 2012.

affirmative action. "There are in principle no limits as to the form consent can take. However, for consent to be valid it should be an active indication of the user's wishes."[1091]

The difference between direct marketing that's based on the balancing provision (on an opt-out basis) and direct marketing that's based on the legal basis consent (opt-in) isn't merely theoretical. The balancing provision sometimes allows firms to process personal data for direct marketing on an opt-out basis, but in such cases the provision requires the firm to weigh the interests involved. By relying on fictitious opt-out consent, firms could try to escape the responsibility to balance its interests against those of the data subject.[1092]

A number of larger behavioural targeting firms, cooperating in the Interactive Advertising Bureau, offer people the chance to opt out of targeted advertising on a centralised website: youronlinechoices.com. But under this scheme, participating firms may continue to process information about people (phase 1 and 2 of behavioural targeting), as they merely promise to stop showing targeted advertising (phase 5) after people object.[1093] In short, the website offers the equivalent of Do Not Target, rather than Do Not Track.[1094] But even if the opt-out system did stop firms from tracking people, it's hard to see how such an opt-out system could meet data protection law's requirements for consent.[1095]

The Data Protection Directive says that consent must be "unambiguous." This seems superfluous. As Kosta puts it, "the element that the consent has to be given unambiguously should be intrinsic in the concept of consent in order for it to qualify

---

[1091] Article 29 Working Party 2013, WP 208, p. 3.
[1092] The legal basis consent doesn't legitimise disproportionate data processing. See section 5 of this chapter, and chapter 9, section 2.
[1093] The opt-out page of the Internet Advertising Bureau says: "Declining behavioral advertising only means that you will not receive more display advertising customised in this way" (Interactive Advertising Bureau Europe – Youronlinechoices).
[1094] See on the difference between Do Not Track (/Do Not Collect) and Do Not Target chapter 8, section 5.
[1095] Article 29 Working Party 2011, WP 188, p. 6.

as valid."[1096] The word "unambiguous" seems to have led to confusion.[1097] Some appear to believe that non-unambiguous consent – if there were such a thing – can be given by failing to object. Views along these lines were expressed in discussions about the e-Privacy Directive's consent requirement for tracking technologies (see section 4 of this chapter).

In sum, consent to personal data processing requires an "indication of wishes" to be valid. In some circumstances consent can be implied, but mere silence doesn't signify consent. The European Commission proposal for a Data Protection Regulation tightens the requirements for consent, and always requires consent to be explicit (see chapter 8).[1098] Just like in the 1990s, firms have reacted to the 2012 proposal by lobbying for a regime that accepts "implied consent."[1099]

Specific and informed

The Data Protection Directive also requires consent to be "specific" and "informed."[1100] Specific means that consent "must relate to a particular data processing operation concerning the data subject carried out by a particular controller and for particular purposes."[1101] For instance, consent to use personal data "for commercial purposes" would be too vague.[1102] The Working Party confirms that "blanket consent without specifying the exact purpose of the processing is not acceptable."[1103]

[1096] Kosta 2013a, p. 235.
[1097] See Traung 2012, p. 38.
[1098] Chapter 8, section 3, discusses the proposals regarding consent.
[1099] See on lobbying in the 1990s chapter 4, section 1. For examples of lobbying regarding consent and the 2012 proposals, 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.
[1100] Kosta suggests that "specific" and "informed" are largely overlapping, and that the requirement of specificity may be superfluous (Kosta 2013a, p. 224).
[1101] European Commission amended proposal for a Data Protection Directive (1992), p. 12. See also Article 29 Working Party 2013, WP 202, p. 15.
[1102] See European Commission amended proposal for a Data Protection Directive (1992), p. 15. The European Commission gives "for commercial purposes" as an example of a processing purpose which isn't specified. But the same example can be applied to "specific" consent.
[1103] Article 29 Working Party, WP 187, p. 17.

Consent has to be informed. In a case on working hours (not regarding data protection law), the European Court of Justice required "full knowledge of all the facts" for consent to be valid.[1104] A firm can't establish whether somebody *is* informed when he or she consents. For instance, a firm can never guarantee that people read the text of a consent request. But as transparency is a precondition for valid consent, firms must provide information in accordance with the requirements of data protection law. If a consent request doesn't clearly explain how the firm wants to use the data, the consent can't be informed.

Obtaining consent of a data subject must be distinguished from the transparency requirement. The Data Protection Directive always requires data controllers to be transparent about data processing, whether they rely on consent or not.[1105] It's not possible to obtain consent by silently changing a privacy policy. If a data subject doesn't know about new terms and conditions, there can't be an expression of will.[1106] It would be absurd to argue that the person consented.

Freely given

Consent must be freely given, so consent given under pressure isn't valid. As Kosta puts it, "consent of the data subject is still freely given when positive pressure is exercised, while the exercise of any kind of negative pressure renders the consent invalid."[1107] An extreme example of negative pressure is holding a gun to somebody's head while asking whether he or she consents. The consent wouldn't be free. But to make consent involuntary, pressure doesn't have to be so great. For instance, if an employer asks an employee for consent, the consent might not be sufficiently free,

---

[1104] ECJ, C-397/01 en C-403/01, Pfeiffer and others, 5 October 2004, dictum (2) and par. 82.
[1105] See article 11 of the Data Protection Directive. This requires information "where the data have not been obtained from the data subject." In such cases there's no consent. See chapter 4, section 3.
[1106] As Radin puts it, there would be "sheer ignorance" on the side of the user (Radin 2013, p. 19-21).
[1107] Kosta 2013a, p. 256.

because of the imbalance of power.[1108] And the European Court of Justice says people applying for passports can't be deemed to have freely consented to have their fingerprints taken, because people need a passport.[1109]

But positive pressure is generally allowed. For instance, in most circumstances, data protection law probably allows firms to entice people to consent by offering something in return, such as a discount.[1110] In principle, a firm is allowed to say: you can use this service if you consent to being tracked. But it can be difficult to differentiate between positive and negative pressure, for instance if a data controller offers a take-it-or-leave-it choice. A service could be so important that people have no genuine choice not to use it. Bygrave suggests that the requirement of fair data processing implies that firms shouldn't pressure people too much into disclosing data, and that firms shouldn't abuse their market power.[1111] The European Data Protection Supervisor and national Data Protection Authorities have voiced similar opinions.[1112] The voluntariness of consent is discussed in more detail in the next section.[1113]

6.4 Consent for tracking technologies

European legal discussions on behavioural targeting often focus on the e-Privacy Directive's consent requirement for tracking technologies, rather than on the general data protection rules. The 2002 e-Privacy Directive was updated in 2009.[1114]

Article 5(3) of the e-Privacy Directive applies to anyone that wants to store or access information on a user's device, including if no personal data are involved.[1115] The

---

[1108] Kosta 2013a, p. 386; Article 29 Working Party, WP 187, p. 13-14. See also Naczelny Sąd Administracyjny [Supreme Administrative Court], 1 December 2009, I OSK 249/09 (Inspector General for Personal Data Protection), English translation: <www.giodo.gov.pl/417/id_art/649/j/en/> accessed 28 May 2014.
[1109] CJEU, C-291/12, Schwartz v. Stadt Bochum, 17 October 2013, par. 32.
[1110] See European Agency for Fundamental Rights 2014, p. 59.
[1111] Bygrave 2002, p. 58-59.
[1112] European Data Protection Supervisor 2011, p. 13-15.
[1113] See also section 3 and 4 of chapter 7, and section 3 and 5 of chapter 8.
[1114] The e-Privacy Directive 2002/58 was updated by Directive 2009/136. This study refers to the consolidated version from 2009.

preamble shows that article 5(3) aims to protect the device itself and its contents against unauthorised access. "Terminal equipment of users of electronic communications networks and any information stored on such equipment are part of the private sphere of the users requiring protection under the European Convention for the Protection of Human Rights and Fundamental Freedoms."[1116] The Working Party confirms that the provision applies, for instance, to apps that access information on a user's smartphone, such as location data or a user's contact list.[1117]

Another rationale for article 5(3) is protecting the user's device against parties that want to store information on a user's device, without the user's knowledge. The provision aims, for instance, to protect people against the secret installation of adware or spyware. Yet another rationale is protecting the user against surreptitious tracking, as explained in the preamble.[1118]

> So-called spyware, web bugs, hidden identifiers and other similar devices can enter the user's terminal without their knowledge in order to gain access to information, to store hidden information or to trace the activities of the user and may seriously intrude upon the privacy of these users.[1119]

Early proposals for the 2002 version of the e-Privacy Directive required firms to ask for consent before they placed certain kinds of cookies. After fierce lobbying by the marketing industry, the final version used ambiguous wording about a "right to refuse." The 2002 version of article 5(3) is usually interpreted as an opt-out

---

[1115] A user (article 2(a) of the e-Privacy Directive) isn't the same as a "subscriber" (article 2(k) of the Framework Directive 2002/21). We'll leave this complication aside for this study.
[1116] Recital 24 of the e-Privacy Directive.
[1117] Article 29 Working Party 2013, WP 202, p. 10.
[1118] See e.g. recital 24 and 25 of the e-Privacy Directive, and recital 65 and 66 of Directive 2009/136. See also Kierkegaard 2005; Kosta 2013.
[1119] Recital 24 of the e-Privacy Directive. Recital 25 adds that "so-called 'cookies', can be a legitimate and useful tool, for example, in analysing the effectiveness of website design and advertising."

system.[1120] Websites had an obligation to clearly inform people about the use of cookies, but few websites did.

2009 revision

Since 2009, article 5(3) of the revised e-Privacy Directive, sometimes called the Cookie Directive,[1121] requires firms to obtain the user's consent before using tracking technologies such as cookies. The general rule can be summarised as follows. Firms that want to store or access a cookie on a user's device must (i) give the user clear and complete information about the cookie's purpose, and (ii) obtain the user's consent. Certain functional cookies are exempted from the information and consent requirements. For example, no consent is needed for a cookie for a digital shopping cart or for a log-in procedure.[1122] For the definition of consent, the e-Privacy Directive refers to the definition in the Data Protection Directive: a free, informed, specific indication of will.[1123]

For ease of reading this study speaks of consent for "cookies" or for "tracking technologies", but article 5(3) applies to any information that can be stored on a user's device. Article 5(3) thus also applies to spyware and adware. Hence, if a firm wants to install adware, for instance coupled with a browser toolbar, it must give clear and comprehensive information to the user, and obtain the user's consent.[1124] It follows from the preamble of the amending directive that the provision also applies when spyware or similar files are distributed on USB sticks, music CDs etc.[1125]

[1120] Kierkegaard 2005. Some authors read the 2002 version as an opt-in system (see Traung 2010; Helberger et al. 2011).
[1121] See e.g. McStay 2012.
[1122] See in detail on the exempted cookies Article 29 Working Party 2012, WP 194.
[1123] Article 2(f) and recital 17 of the e-Privacy Directive.
[1124] The Dutch Telecommunications authority imposed a 1 million euro fine on a spyware distributor. On appeal, the fine was overturned (College van Beroep voor het bedrijfsleven [Trade and Industry Appeals Tribunal], 20 June 2013, ECLI:NL:CBB:2013:CA3716 (Dollarrevenue/Autoriteit Consument en Markt).
[1125] See recital 65 of Directive 2009/136. The provision would apply for instance to the CDs distributed by SONY in 2005, which installed spyware when people put the CD in their computer (Russinovich 2005). It has been argued that the provision also applies to accessing information in a digital TV decoder for behavioural targeting (Minister of Economic Affairs, Agriculture and Innovation of the Netherlands 2012).

Who has to comply? Article 5(3) states: "anyone" that wants to access information stored in a users' device, or wants to store information in a user's device. In principle, it's the firm operating the cookie (such as an ad network) that must obtain consent. But from the beginning, the Working Party has said that a website publisher that allows third parties to place cookies shares the responsibility for information and consent.[1126]

The firm operating the cookie, or the website publisher, must at least explain the cookie's purpose. The e-Privacy Directive says the information provided to users must be "clear and comprehensive" and must be in accordance with the Data Protection Directive. The latter requires more information if this is necessary to guarantee fairness.[1127] The Working Party gives several examples of how firms could ask for informed consent, including a pop-up window.[1128]

In short, article 5(3) requires informed consent for the use of most tracking technologies that are used for behavioural targeting. A problem with article 5(3) is that the provision is over inclusive. For instance, the provision also requires consent for many cookies that aren't used for tracking people across the web. Chapter 8 returns to this topic.[1129]

Browser settings

A sentence from recital 66 of the 2009 directive that amended the e-Privacy Directive has caused much confusion and discussion. The recital says people can express consent with their browser under certain circumstances:

[1126] Article 29 Working Party 2010, WP 171, p. 24.
[1127] Article 5(3) of the e-Privacy Directive; article 10 and 11 of the Data Protection Directive.
[1128] Article 29 Working Party 2011, WP 188, p. 9-11.
[1129] Chapter 8, section 4.

> 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.[1130]

Most browsers offer users the possibility to block first party cookies, third party cookies, or all cookies. Some conclude from recital 66 that default browser settings could be relied upon as an expression of consent for tracking cookies. For instance, the Interactive Advertising Bureau UK says: "We believe that default web browser settings can amount to 'consent' (…)".[1131] Perhaps the fact that the e-Privacy Directive doesn't speak of "unambiguous" consent has contributed to the confusion. In line with data protection law's requirement of an expression of will for valid consent, the Working Party has repeatedly rejected the idea that default settings of browsers could signify consent:[1132]

> Where the website operator can be confident that the user has been fully informed and actively configured their browser or other application then, in the right circumstances, such a configuration, would signify an active behaviour and therefore be respected by the website operator. (…) The process by which users could signify their consent for cookies would be through a positive action or other active behaviour, provided they have been fully informed of what that action represents.[1133]

[1130] Recital 66 of Directive 2009/136.
[1131] Interactive Advertising Bureau United Kingdom 2012 (emphasis original).
[1132] See e.g. Article 29 Working Party, WP 187, p. 32.
[1133] Article 29 Working Party 2013, WP 208, p. 4 (emphasis original).

Many commentators agree that default browser settings can't signify a specific and informed indication of wishes. It's unlikely that all people who that do *not* tweak their browser's default settings want to consent to all kinds of cookies. There wouldn't be an expression of wishes. And if a browser accepts a lot of cookies, including for the future, such "consent" can't be informed and specific.[1134] In addition, if browser settings could be relied upon for an expression of consent, this would imply that a party could assume that users consent to spyware or viruses if their browsers don't block such files.[1135]

There are more arguments against relying on default browser settings as a consent mechanism. For example, browser settings are merely mentioned in a recital.[1136] The informed consent requirement is laid down in article 5(3) of the e-Privacy Directive. Case law and literature suggest that if a recital and an article contradict each other, and both have a clear meaning, the article must prevail.[1137] Hence, a clear article such as article 5(3) should probably prevail over an ambiguous recital such as recital 66. Apart from that, recital 66 doesn't contradict article 5(3), but should be read as a reminder that consent can be given in any form.[1138]

Furthermore, European law suggests that a privacy-friendly interpretation of the e-Privacy Directive is called for. The e-Privacy Directive aims to protect the right to privacy and the right to data protection.[1139] These rights are included in the EU Charter of Fundamental Rights,[1140] and according to the European Court of Justice, the

---

[1134] See e.g. Traung 2012; McStay 2012; Kosta 2013. See also Article 29 Working Party, WP 171, p. 14.
[1135] Helberger et al. 2011, p. 63.
[1136] Recital 66 of Directive 2009/136.
[1137] Klimas & Vaiciukaite 2008. The European Court of Justice says "the preamble to a Community act has no binding legal force and cannot be relied on either as a ground for derogating from the actual provisions of the act in question or for interpreting those provisions in a manner clearly contrary to their wording" (ECJ, C-136/04, Deutsches Milch-Kontor GmbH, 24 November 2005, par. 32).
[1138] Traung 2010, p. 225.
[1139] See article 1 and article 5 of the e-Privacy Directive. See also the Data Protection Directive, which aims for a "high level of protection" of fundamental rights and in particular privacy (recital 10). Article 8(4)(c) of the Framework Directive 2002/21/EC (amended in 2009) requires national regulatory authorities to "contribut[e] to ensuring a high level of protection of personal data and privacy."
[1140] Article 7 and 8 of the EU Charter of Fundamental Rights.

e-Privacy Directive must be interpreted in line with fundamental rights.[1141] The e-Privacy Directive's preamble says that users' devices are part of the user's private sphere,[1142] and the European Court of Human Rights interprets the right to private life broadly.[1143] In addition, the Charter and other EU Treaties emphasise the importance of a high level of consumer protection.[1144]

Taking the requirements for consent into account, recital 66 should probably be read as follows. If browsers were developed with a function to express consent in line with the Data Protection Directive, such browsers could be used to consent to the use of cookies. However, for the moment most browsers aren't suitable to give informed consent for cookies. Chapter 8 discusses the Do Not Track standard, which could enable people to express their wishes with their browser.[1145]

The 2009 version of article 5(3) should have been implemented in national legislation in May 2011, but many member states missed this deadline.[1146] At the time of writing, enforcement of the consent requirement for tracking cookies is in its infancy, among other reasons because the national laws implementing the consent rule are rather new.[1147] Discussions about a Do Not Track standard may have delayed enforcement as well. It's unclear how national authorities will apply the implementation of article 5(3).[1148] The approaches seem to vary. For instance, the UK appears to accept a kind

---

[1141] ECJ, C-275/06, Promusicae, 29 January 2008, par. 67-68, and dictum. See also recital 62 of the Citizens' Rights Directive.
[1142] Recital 24 of the e-Privacy Directive; recital 65 of Directive 2009/136.
[1143] See chapter 3, section 2.
[1144] See article 38 and article 51(1) of the EU Charter of Fundamental Rights, and article 12, article 114(3) and article 169 of the Treaty on the Functioning of the EU (consolidated version 2012).
[1145] Chapter 8, section 5.
[1146] Article 4(1) of Directive 2009/136. According to the Working Party, all member states had implemented the amended e-Privacy Directive on 1 January 2013 (Article 29 Working Party 2013, WP 208, p. 2). It's not unusual that member states implement directives late.
[1147] Regulators have taken some action regarding the national implementation of article 5(3). For example, the Agencia Española de Protección de Datos (Spanish Data Protection Authority) issued a fine for non-compliance in January 2014 (Agencia Española de Protección de Datos 2014; see Pastor 2014). The Dutch Data Protection Authority has concluded in several investigations that article 5(3) was breached (see e.g. College bescherming persoonsgegevens 2013 (TP Vision); College bescherming persoonsgegevens 2014 (YD)). See regarding Google and article 5(3) chapter 8, section 1.
[1148] The Working Party has tried to align the implementation. In line with earlier Opinions, the Working Party says "an active indication of the user's wishes" is required for consent to cookies (Article 29 Working Party 2013, WP 208, p. 3).

of opt-out system,[1149] whereas the Netherlands requires, in short, opt-in consent for tracking cookies.[1150]

Take-it-or-leave-it choices

It's somewhat unclear what "free" consent means in the context of the e-Privacy Directive. The Dutch experience with the consent requirement for tracking cookies can serve as an illustration. In the Netherlands the consent requirement for tracking cookies came into effect in January 2013. The implementation law made clear that unambiguous (opt-in) consent was required for tracking cookies.[1151] Many websites reacted by denying entry to visitors that didn't accept third party tracking cookies, by installing "cookie walls" or "tracking walls" – barriers users could only pass if they allowed the website and its partners to track them.[1152] One could question whether consent is voluntary if a website installs a tracking wall.[1153] Among others, Kosta suggests that a tracking wall makes consent involuntary. "In such a case the user does not have a real choice, thus the consent is not freely given."[1154]

Indeed, in some cases consent may not be sufficiently "free" when a website uses a tracking wall. For example, the Dutch Data Protection Authority says that the national public broadcasting organisation isn't allowed to use a tracking wall.[1155] The Data Protection Authority says that the public broadcaster has a "situational monopoly", because the only way to access certain information online is through the broadcaster's website.[1156] This makes the consent involuntary. It remains to be seen whether Data

---

[1149] Information Commissioner's Office 2013a.
[1150] See below.
[1151] Article 11.7a of the Dutch Telecommunications Act (version applicable on 30 May 2014). The explanatory memorandum makes clear that opt-in consent is required for tracking cookies. See for a translation of the provision Zuiderveen Borgesius 2012, p. 5.
[1152] See Helberger 2013.
[1153] See Article 29 Working Party 2013, WP 208; Impact Assessment for the proposal for a Data Protection Regulation (2012), Annex 4, p. 76.
[1154] Kosta 2013, p. 17. See also Roosendaal 2013, p. 186.
[1155] Helberger 2013, p. 18.
[1156] College Bescherming Persoonsgegevens (Dutch DPA) 2013 (cookie letter).

Protection Authorities will use similar "situational monopoly" reasoning when commercial broadcasters and website publishers use tracking walls.

The Working Party is sceptical about tracking walls, but doesn't really prohibit them. It says people "should have an opportunity to freely choose between the option to accept some or all cookies or to decline all or some cookies."[1157]

> In some Member States access to certain websites can be made conditional on acceptance of cookies, however generally, the user should retain the possibility to continue browsing the website without receiving cookies or by only receiving some of them, those consented to that are needed in relation to the purpose of provision of the website service, and those that are exempt from consent requirement. It is thus recommended to refrain from the use of consent mechanisms that only provide an option for the user to consent, but do not offer any choice regarding all or some cookies.[1158]

Recital 25 of the e-Privacy Directive says "[a]ccess to specific website content may still be made conditional on the well-informed acceptance of a cookie or similar device, if it is used for a legitimate purpose." It is likely that the EU lawmaker didn't foresee that some websites would completely block visitors that don't accept third party tracking cookies. But the Working Party suggests that recital 25 isn't meant to allow firms to put the whole website behind a tracking wall: "[t]he emphasis on 'specific website content' clarifies that websites should not make conditional 'general access' to the site on acceptance of all cookies."[1159] The Working Party adds that

---

[1157] Article 29 Working Party 2013, WP 208, p. 5.
[1158] Article 29 Working Party 2013, WP 208, p. 5 (internal footnote omitted).
[1159] Article 29 Working Party 2013, WP 208, p. 5.

website publishers should "only limit certain content if the user does not consent to cookies."[1160]

The careful phrases suggest that the Working Party doesn't mean to say that all take-it-or-leave-it choices and tracking walls are prohibited.[1161] This seems to be the correct interpretation of current law. If there are alternative service providers, it is likely that data protection law will allow a firm to offer such a take-it-or-leave-it choice.[1162] When interpreting data protection law's consent rules, the general principle of freedom of contract can provide inspiration by analogy. True, contractual freedom isn't absolute.[1163] Nevertheless, the principle of contractual freedom would be hard to reconcile with reading a full prohibition of take-it-or-leave-it choices in current data protection law. That said, data protection law does require consent to be "free."

Several factors can be taken into account when assessing whether a firm is allowed to offer a take-it-or-leave-it choice, for instance with a tracking wall on its website. The following is a non-exhaustive list of circumstances in which the legality of tracking walls is particularly questionable. The firm has a monopoly position.[1164] There are no competitors that offer a similar, more privacy-friendly service.[1165] It's not a realistic option for people to go to a competitor, for instance because of a lock-in situation.[1166]

[1160] Article 29 Working Party 2013, WP 208, p. 5.
[1161] But see the English Information Commissioner's Office, which says: "Organisations should not coerce or unduly incentivise people to consent, or penalise anyone who refuses. Consent cannot be a condition of subscribing to a service or completing a transaction" (Information Commissioner's Office 2013b, p. 14).
[1162] See also European Agency for Fundamental Rights 2014, p. 59.
[1163] As Chang puts it, "[a]ll societies keep certain things off the market – human beings (slavery), human organs, child labour, firearms, public offices, health care, qualifications to practice medicine, human blood, educational certificates and so on" (Chang 2014, p. 395). See on inalienable rights, of which "transfer is not permitted between a willing buyer and a willing seller," also Calabresi & Melamed 1972 (p. 1092).
[1164] As Bygrave notes, "fairness (…) implies that a person is not unduly pressured into supplying data on him-/herself to a data controller or accepting that the data are used by the latter for particular purposes. From this, it arguably follows that fairness implies a certain protection from abuse by data controllers of their monopoly position" (Bygrave 2002, p. 58).
[1165] See section 28(3)(b) of the Federal Data Protection Act in Germany.
[1166] See on lock-in situations and transaction costs chapter 7, section 3. In some cases, the law aims to reduce the problem of lock-in. For instance, the Universal Services Directive (2002/22/EC) requires phone companies to offer number portability (article 30(1)). The European Commission proposal for a Data Protection Regulation (2012) introduces a right to data portability in article 18.

There are circumstances that make it difficult or burdensome to leave the service.[1167] (It makes little sense to join another social network if all of one's friends are on Facebook.) A service is aimed at, or often used by, children.[1168] Under the given circumstances, it's unfair to expose people to tracking.[1169] Lastly, if a tracking wall affects millions of people, it deserves more scrutiny than when it only affects a few people.[1170] In sum, to assess the voluntariness of consent, all circumstances have to be taken into account – as is usually the case when applying legal provisions.

Confidentiality of communications

Apart from article 5(3), article 5(1) of the e-Privacy Directive is also relevant for behavioural targeting. Article 5(1) concerns the confidentiality of communications and can be summarised as follows. Member states must ensure the confidentiality of communications and the related traffic data by means of publicly available electronic communications services. In particular, member states must prohibit tapping, storage or other types of communications surveillance, without the consent of the users. Hence, the provision emphasises member states' positive obligations regarding confidentiality of communications.[1171]

Certain forms of behavioural targeting are clearly covered by article 5(1). If an internet access provider employs deep packet inspection to analyse people's internet use, including email communication, article 5(1) applies.[1172] Email messages are a form of communication, and the e-Privacy Directive applies to telecommunications providers, such as internet access providers.[1173] But web browsing and using IPTV or

---

[1167] For instance, there could be transaction costs. See chapter 7, section 3.
[1168] The Article 29 Working Party says that tracking shouldn't be made a condition for the use of a social network service. Perhaps this remark is partly inspired by the fact that many children use such sites (Article 29 Working Party, WP 187, p. 18).
[1169] See chapter 4, section 4 on the interpretation of fairness. See also Bygrave 2002, p. 58.
[1170] See Radin 2013.
[1171] Steenbruggen 2009, p. 176; p. 356.
[1172] See for an example, Phorm, which was discussed in section 3 of this chapter, and in chapter 2, section 2.
[1173] See on the scope of the e-Privacy Directive chapter 5, section 6; chapter 9, section 5. An "electronic communications service" is, in short, a service that consists wholly or mainly in the conveyance of signals on

video-on-demand services also fall within the European legal definition of communication.[1174] Monitoring people's web browsing is thus only allowed upon obtaining their consent, as member states must prohibit "interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned."[1175] It has been suggested, amongst others by the European Data Protection Supervisor, that article 5(1) doesn't only apply to telecommunications providers.[1176] This would imply that ad networks must also comply with the provision in many circumstances.[1177] Regardless of the debate surrounding the applicability of article 5(1), consent is required by article 5(3) for most tracking technologies.

6.5 A limited but important role for informed consent

Informed consent has an important but limited role in data protection law. Consent is important, because the data subject can allow, or choose not to accept, data processing that would otherwise be prohibited.

Consent could be seen as a legal basis for data processing activities for which there's no overriding interest. "If no consent is given," Gutwirth notes, "the other legitimate grounds in themselves seem to span the whole gamut of possibilities, unless one assumes that such consent legitimizes disproportionate and illegitimate processing – which is very questionable."[1178] In theory (and leaving aside the EU Charter of

---

electronic communications networks (article 2(c) of the Framework Directive 2002/21/EC (amended in 2009)). It's thus a transmission service.

[1174] The e-Privacy Directive defines communication in article 2(d): "any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service. This does not include any information conveyed as part of a broadcasting service to the public over an electronic communications network except to the extent that the information can be related to the identifiable subscriber or user receiving the information." See Steenbruggen 2009, p. 181; p. 354. Traung 2010, p. 227.

[1175] Article 5(1) of the e-Privacy Directive.

[1176] See Traung 2010, p. 227; González Fuster et al. 2010, p. 115; European Data Protection Supervisor 2008, par 33. See also Article 29 Working Party 2006, WP 118.

[1177] If somebody browses the web while using an electronic communications service that is not publicly available (perhaps a Wi-Fi network in a coffee shop), this might be different. A full discussion of the scope of article 5(1) would go beyond the scope of this study.

[1178] Gutwirth 2002, p. 100.

Fundamental Rights), a data protection regime without a consent provision could be envisaged.[1179] In such a regime, a firm that couldn't rely on a contract with the data subject would have to check whether it could rely on the balancing provision. But if the data subject's fundamental rights outweighed the firm's interests, the data processing couldn't legally take place. In the current regime, firms can ask consent for processing that isn't "necessary."[1180] But even after consent is obtained, firms have to comply with the other data protection provisions.[1181]

A strong believer in informational self-determination and data subject control might see consent as the primary condition for data processing, at least in the private sector.[1182] In this view, the other legal bases are exceptions for data processing that's "necessary" for overriding interests. If the other legal bases were seen as exceptions to the consent requirement, the balancing provision would be a peculiar provision, because of its vagueness.

In theory, a data protection regime without a balancing provision could also be imagined.[1183] But such a regime would require a lot of consent requests, including for relatively innocuous practices. The balancing provision protects people from too many consent requests for trivial matters. Some practices would be almost impossible to do legally if the balancing provision didn't exist. For instance, Data Protection Authorities allowed Google to rely on the balancing provision for the processing of personal data (pictures including people) for its Streetview service.[1184] It's difficult to

---

[1179] The EU Charter of Fundamental Rights mentions consent as a legal basis for personal data processing (article 8(1)).
[1180] A data protection regime without a consent provision isn't fully hypothetical. For instance, early data protection acts in Belgium and France didn't include a consent clause (see De Hert et al. 2013, p. 59).
[1181] See chapter 9, section 2.
[1182] See Purtova 2011, p. 235-237. In some countries, consent is seen as the primary legal basis for processing (Korff 2002, p. 71).
[1183] A data protection regime without a balancing provision isn't fully hypothetical. For example, Spain had a very narrow version of the balancing provision, which only applied to data that appeared in public sources. The European Court of Justice didn't accept this (CJEU, C-468/10 and C-469/10, ASNEF, 24 November 2011). And the 1992 Data Protection Act in Hungary (replaced in 2012) didn't have a clear balancing provision (Act LXIII of 1992 on the Protection of Personal Data and Public Access to Data of Public Interest).
[1184] See Van Der Sloot & Zuiderveen Borgesius 2012a.

see how Google could have obtained consent of all people whose images (personal data) were included on pictures.

In any case, in 1992 the European Commission suggested that there's no priority between the legal bases. "Consent is no longer the main criterion, subject to exceptions; it is now the first of several alternatives (new article 7(a))."[1185] In sum, the legal bases consent and the balancing provision both have a role to play in data protection law. Apart from that, it doesn't seem plausible that one of the legal bases would be abolished.[1186]

e-Privacy Directive

The e-Privacy Directive says its provisions "particularise and complement" the Data Protection Directive.[1187] Article 5(3) of the e-Privacy Directive complements the requirement in data protection law of a legal basis for personal data processing. If a firm uses a tracking cookie to process personal data, it needs a legal basis for the processing. Hence, usually an ad network would need to obtain "unambiguous consent" for personal data processing, even if it obtained consent for using the cookie. In practice it would make sense to merge the consent request for the cookie and the following personal data processing operation.[1188] If a firm could base personal data processing for behavioural targeting on the balancing provision, the firm would still have to obtain consent for the use of the tracking cookie. From the firm's perspective, it's thus hardly relevant on which legal basis it can rely upon for personal data processing for behavioural targeting.[1189]

Therefore, article 5(3) could be interpreted as blocking firms from relying on the balancing provision for behavioural targeting. Seen in this light, article 5(3) of the e-

---

[1185] European Commission amended proposal for a Data Protection Directive (1992), p. 16 (capitalisation adapted).
[1186] It would be difficult to abolish the legal basis consent, as it's included in the EU Charter of Fundamental Rights (article 8 (2)).
[1187] Article 1(2) of the e-Privacy Directive.
[1188] Article 29 Working Party 2013, WP 202, p. 14. Consent (article 7(a) of the Data Protection Directive) is usually the only available legal basis for behavioural targeting; see section 1-3 of this chapter,
[1189] See Article 29 Working Party 2014, WP 217, p. 46.

Privacy Directive codified an interpretation of the Data Protection Directive's legal basis requirement in the behavioural targeting context. As article 5(3) applies to the storing or accessing any information (personal data or not) on a user's device, article 5(3) implicitly sidesteps the discussion of whether tracking cookies and similar files are personal data.[1190]

Other rules in the e-Privacy Directive can also be seen as codifying an interpretation of the Data Protection Directive's legal basis requirement, for instance the rules on spam.[1191] In short, the e-Privacy Directive only allows sending marketing emails to non-customers after the receiver's prior consent is obtained (an opt-in system). "The use of (…) electronic mail for the purposes of direct marketing may be allowed only in respect of subscribers or users who have given their prior consent."[1192] Hence, firms can't rely on the balancing provision for sending commercial emails to non-customers. But within the context of an existing customer relationship, the e-Privacy Directive allows a firm to send marketing emails to offer similar products or services, if the email includes a clear opt-out possibility. There's thus an opt-out system for certain first party direct marketing emails, which resembles the regime of the balancing provision.[1193] The e-Privacy Directive has more rules that essentially block certain types of firms from relying on the balancing provision for processing for direct marketing. For instance, certain types of firms (in short: telecommunication providers) are required to obtain consent for processing traffic and location data, unless a specified exception applies.[1194]

In a nutshell, if direct marketing uses any other method than paper, human phone calls, or visits to people's houses, EU law requires the individual's consent – with the

---

[1190] However, the scope of article 5(3) is too broad, as it also requires consent for certain types of innocuous cookies. See chapter 8, section 4.
[1191] See on the right to object to direct marketing and the e-Privacy Directive Article 29 Working Party 2014, WP 217, p. 45-47.
[1192] Article 13 of the e-Privacy Directive. For direct marketing by automatic calling machines (robo calls) or by fax, consent is also required, subject to exceptions.
[1193] Article 13(2) of the e-Privacy Directive. See also recital 41.
[1194] See on the scope of the e-Privacy Directive chapter 5, section 6, chapter 8, section 4, chapter 9, section 5.

exception of some types of first party direct marketing. The opt-out regime for paper, human phone calls, and house visits can plausibly be explained by the fact that such marketing techniques are relatively costly. The higher costs of such practices reduce the chance of abusive practices. It's cheaper to send spam email to millions of people, than to hire workers to call millions of people.[1195]

Default rules and mandatory rules

Regarding direct marketing, the Data Protection Directive's consent provision and the balancing provision could be seen as mirror images. The legal bases consent (article 7(a)) and the balancing provision (article 7(f)) provide default positions that the data subject can alter.[1196]

Sometimes personal data processing for direct marketing is *only* allowed after consent. The default position is: data processing is not allowed. Without consent, a firm may not process personal data. But with consent the data subject can allow data processing that would otherwise be prohibited. In other words, the data subject can alter the default by giving consent to data processing. Sometimes data processing for direct marketing is allowed *without* consent. If a firm can rely on the balancing provision, the default is: data processing is allowed.[1197] But the data subject has the right to stop the data processing: to opt out. By opting out, the data subject can alter the default position to: data processing is not allowed.[1198]

In law and economics terms, the consent requirement lays down a "default" rule, also called a "non-mandatory" rule. Default rules "apply unless the parties make deviating arrangements."[1199] The data subject can make a deviating arrangement by giving

---

[1195] See recital 42 of the e-Privacy Directive.
[1196] Purtova 2014 makes a similar point, but refers to the default positions as "entitlements", a concept introduced by Calabresi & Melamed 1972.
[1197] Of course, firms need to comply with all data protection law's requirements, regardless of the legal basis for processing.
[1198] See article 14(b) of the Data Protection Directive. See section 2 of this chapter.
[1199] Hesselink 2005, p. 46. In a famous law and economics article on default rules, Ayres & Gertner speak of "rules that parties can contract around by prior agreement" (Ayres & Gertner 1989, p. 87). A rule that lays down a default

consent to data processing. Likewise, the regime for direct marketing that follows from the balancing provision could be seen as a default rule. The data subject can make a deviating arrangement by objecting to data processing (opting out).

The other data protection rules are "mandatory" (with arguably a few exceptions.[1200]) In law and economics terms, mandatory "rules cannot be contracted around; they govern even if the parties attempt to contract around them."[1201] People can't set data protection law's mandatory rules aside by contractual agreement, or with consent.[1202] For instance, the following declaration wouldn't be enforceable:

> I hereby consent to the use of my personal data for improving products and services (including more relevant advertising), and other business purposes.[1203] I hereby waive my rights to access, correction and erasure. I will not hold you liable in case of a data breach. The above applies not only to you, the data controller, but also to the selected parties that may obtain my personal data from you.[1204]

In sum, while consent plays an important role, that role is limited at the same time. The freedom to consent to data processing could be seen as an extremely limited version of contractual freedom.

---

is sometimes called "contractible." Mandatory rules can also be called ius cogens (versus default rules: ius dispositivum).

[1200] First, in some cases (not regarding direct marketing) the data subject has a relative right to object (article 14(a). Second, with consent the data subject can allow data export to outside the EU (article 26(b)). Third, the data subject can allow the processing of special categories of data with "explicit consent" (article 8(2)(a)).

[1201] Ayres & Gertner 1989, p. 87. The mandatory character of data protection law can also be framed differently. The right to protection of personal data (article 8 of the EU Charter of Fundamental Rights) can be seen as an inalienable right (see Calabresi & Melamed 1972).

[1202] The Working Party says consent "is primarily a ground for lawfulness, and it does not waive the application of other principles" (Article 29 Working Party 2011, WP187, p. 7). See also chapter 9, section 2.

[1203] The purpose ins't sufficiently "specified", and the consent isn't sufficiently "specific" and "informed" (article 6(1)(b) and article 2(h) of the Data Protection Directive).

[1204] These rights are not waivable (see article 12 and 23 of the Data Protection Directive).

6.6 Data protection law unduly paternalistic?

Sometimes it's suggested that data protection law is too paternalistic, because it limits the data subject's contractual freedom. For example, Bergkamp says data protection law "is driven by paternalistic motives; individuals need to be protected and be given inalienable but vague fundamental rights, the scope of which government officials define *ex post* in specific cases."[1205] Even worse: data protection law "does not permit variation by contract."[1206]

This study does not find data protection law unduly paternalistic.[1207] There are at least three reasons why data protection law isn't unduly paternalistic. First, in line with positive law, this study takes the view that some paternalism can be justified. Second, pure paternalism is only present when a legal rule only aims at protecting a person against him- or herself. But there are other rationales for data protection law than protecting people against themselves. Third, data protection law leaves some important choices to the data subject.

There's a huge body of literature on paternalism from many disciplines.[1208] Cserne discusses paternalism in the context of contract law. His paternalism definition is apt for this study.

[1205] Bergkamp 2002, p. 37. See also Cuijpers 2007.
[1206] Bergkamp 2002, p. 38. It must be noted that Bergkamp's position seems rare.
[1207] Few authors argue explicitly that data protection law isn't too paternalistic, perhaps because data protection law is rarely accused of being too paternalistic. An implicit argument that data protection law isn't too paternalistic can be found in, for instance, De Hert & Gutwirth 2006; Blume 2012; Purtova 2011, p. 204.
[1208] See for good and easy to read introductions Cserne 2008; Dworkin 2010; Ogus 2010; Sunstein 2013. See on privacy law and paternalism, from a US perspective Solove 2013.

> There are three conditions for an act to be paternalistic. The paternalist
>
> (1) interferes with the subject's liberty,
>
> (2) acts primarily out of benevolence toward the subject (i.e., his goal is to protect or promote the interests, good or welfare of the subject),
>
> (3) acts without the consent of the subject.[1209]

Data protection law's mandatory rules comply with the definition's first element, because the data subject can't waive them. Such mandatory rules limit the data subject's choices, so they interfere with his or her liberty. (This study uses liberty in a narrow sense, roughly comparable with contractual freedom.[1210] A general discussion of the meaning of liberty and paternalism falls outside this study's scope.[1211]) Data protection law's mandatory rules also comply with the third element. The mandatory rules interfere with the data subject's liberty, without his or her consent.[1212]

The second element of the definition requires that the lawmaker "acts primarily out of benevolence toward the subject." This concerns the rationale for a rule. The legal system contains many prohibitions and mandatory rules that have nothing to do with paternalism. For instance, a rule can protect other parties by limiting a person's

---

[1209] Cserne 2008, p. 18. Outside the legal field, Dworkin 2010 gives a similar description. See on paternalism in the context of behavioural targeting Hoofnagle et al. 2012.
[1210] Liberty in the sense of contractual freedom is also called "party autonomy" in the context of contract law (see Grundmann 2002; Grundmann et al. 2001). See on party autonomy and rational choice theory chapter 7, section 2.
[1211] See for a general discussion of freedom, or liberty, in connection with the case law of the European Court of Human Rights: Marshall 2009.
[1212] It could be argued that the data subject gave some kind of broad consent to the democratically elected lawmaker. But we'll leave this line of argument aside. See critically on such arguments Cserne 2008, p 32-33.

freedom: thou shall not kill.[1213] Likewise, if a rule mainly aims to protect a public interest, it's not a purely paternalistic rule. Such rules aren't purely paternalistic, because the lawmaker doesn't act primarily out of benevolence toward the subject.

It's not always easy to establish the rationale for a rule. People might disagree about the rationale for a rule, even if they agree on the rule.[1214] For instance, an obligation to wear a motorcycle helmet could be defended on paternalistic grounds. But the helmet obligation could also be defended by pointing out the costs for society that would result from motorcyclists having accidents that lead to death or injury.[1215] Smoking bans could likewise be defended on both paternalistic and non-paternalistic grounds.[1216]

The Data Protection Directive aims to "protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy."[1217] This could be seen as acting out of benevolence toward the data subject, and thus as paternalism. But protecting fundamental rights is also a public interest. Many scholars say that the right to data protection and the right to privacy are important for our society as a whole.[1218] The protection of privacy and the fair processing of personal data concern the question of what kind of society we want. This goes beyond individual interests.

The European Court of Human Rights suggests that respect for privacy is important for a democratic society.[1219] And the Court speaks of "[t]he interests of the data subjects *and the community as a whole* in protecting the personal data."[1220] Following

---

[1213] See Mill 2011 (1859). Protecting other parties can be seen as an answer to externalities (see chapter 7, section 3).
[1214] Sunstein 1995a.
[1215] Such costs for others could be seen as negative externalities. See chapter 7, section 3.
[1216] See Cserne 2008, p. 34-38.
[1217] Article 1(1) of the Data Protection Directive.
[1218] See e.g. Simitis 1987; Regan 1995; Schwartz 1999; Schwartz 2000; Westin 2003; Rouvroy & Poullet 2009; De Hert & Gutwirth 2006; Allen 2011; Van der Sloot 2012. See also chapter 3, section 1.
[1219] See ECtHR, Rotaru v. Romania, No. 28341/95, 4 May 2000, par. 59; ECtHR, Klass and others v. Germany, No. 5029/71, 6 September 1978, par. 49.
[1220] ECtHR, S. and Marper v. United Kingdom, No. 30562/04 and 30566/04. 4 December 2008, par. 104. (emphasis added).

that reasoning, data protection law isn't purely paternalistic.[1221] Literature on the right to confidentiality of communications contains similar reasoning. The right to confidentiality of communications protects the trust society has in a communication channel.[1222] Furthermore, chapter 7 shows that economic theory accepts several rationales for regulatory intervention that have nothing to do with paternalism.[1223] Some of these rationales can be invoked for data protection law.

That said, benevolence towards the data subject is undoubtedly among the rationales for data protection law. But rules that can be explained by paternalistic motives aren't necessarily *unduly* paternalistic. Looking at positive law in Europe, there are many rules that could plausibly be explained, at least in part, by paternalistic motives.[1224] The European legal system accepts, and perhaps even requires, some paternalism.[1225] Pursuant to the EU Charter of Fundamental Rights for instance, "Union policies shall ensure a high level of consumer protection."[1226] And the Treaty on the European Union says the Union aims for a "social market economy."[1227] Briefly stated, in Europe the question is not: "is legal paternalism acceptable?" The question is: "how much legal paternalism is acceptable?"

European consumer law, broadly defined, contains many rules that remind one of data protection law's transparency principle. The rules aim to empower consumers to make choices in their own best interests. For instance, rules that require firms to include information on packaging aim to empower consumers to make decisions in their own best interests.[1228] Such rules only mildly interfere with contractual freedom. But consumer protection law also contains rules that directly regulate the contents of contracts. As the European Commission puts it, "in some situations, providing a basis

---

[1221] See Sunstein, who says paternalism does not "include government efforts to promote certain familiar and widely held social goals; consider laws designed to protect privacy (…)" (Sunstein 2014, p. 80).
[1222] Asscher 2002, p. 18; p. 247; Steenbruggen, p. 44-49; p. 354.
[1223] See chapter 7, section 2 and 3.
[1224] Ogus 2010.
[1225] But see for another view Van Aaken 2013.
[1226] Article 38 of the EU Charter of Fundamental Rights.
[1227] Article 3(3) of the Treaty on EU (consolidated version 2012).
[1228] See Luth 2010.

for informed choice and legal redress has been regarded as insufficient, notably as regards protection of physical health and safety."[1229] For example, minimum safety standards could be seen as bans of products that don't comply with the requirements.[1230] Other products can't be legally bought at all. Many national consumer protection statutes contain a blacklist of contract terms that aren't enforceable.[1231] Such rules limit contractual freedom, and paternalistic motives are likely to be among the motives. On the other hand, many consumer protection rules can also be explained as a response to market failures, such as information asymmetries.[1232]

In the context of consumer law, Hesselink suggests that rules that aim to protect consumers must generally be mandatory to have any effect. Otherwise the firm, which is usually the one drafting the contract, can set the protective rules aside in the contract.

> Obviously, the main character of rules inspired by the policy of consumer protection is that they are protective. This means that the rules of contract law aim at the protection of the consumer against the other party to the contract (the professional). In order to make this protection effective such rules are typically mandatory, i.e. they cannot be waived.[1233]

[1229] European Commission 2002, p. 6.
[1230] See for instance the General Product Safety Directive. Food is heavily regulated as well (see Van Der Meulen & Van Der Velde 2004).
[1231] See Ebers 2007 (p. 344) on the implementation of the Unfair Contract Terms Directive.
[1232] See on information asymmetry and other market failures chapter 7, section 3.
[1233] Hesselink 2007, p. 339. The European Court of Justice uses similar reasoning in favour of mandatory rules (CJEU, ECJ, C-243/08, Pannon GSM, 4 June 2009, par. 22-25). See also recital 22 of the Consumer Sales Directive (1999/44/EC): "the parties may not, by common consent, restrict or waive the rights granted to consumers, since otherwise the legal protection afforded would be thwarted (…)"

Balancing protecting people and respecting their freedom of choice is common in the law.[1234] "Paradoxically", says Mak, "interference in the contractual relationship is sometimes required in order to guarantee that both contract parties can fully enjoy their freedom of self-determination."[1235] Similar reasoning applies to data protection law. Seen from this angle, data protection law aims to strike a balance between protecting and empowering people.

6.7 Conclusion

This chapter discussed the role of informed consent in the regulatory regime for privacy and behavioural targeting. Discussions about the regulation of behavioural targeting tend to focus on the consent requirement for tracking technologies in the e-Privacy Directive.

Since 2009, article 5(3) of the e-Privacy Directive requires any party that stores or accesses information on a user's device to obtain the user's informed consent. Article 5(3) applies to many tracking technologies such as tracking cookies. There are exceptions to the consent requirement, for example for cookies that are strictly necessary for a service requested by the user, and for cookies that are necessary for the transmission of communication.

For the definition of consent, the e-Privacy Directive refers to the Data Protection Directive, which states that valid consent requires a free, specific, informed indication of wishes. People can express their will in any form, but mere silence or inactivity isn't an expression of will. During the drafting of the Data Protection Directive in the early 1990s, many firms argued that they should be allowed to presume consent for processing, as long as people don't opt out. But the EU lawmaker rejected this idea.

[1234] See for instance Study Group on Social Justice in European Private Law 2004; Grundmann et al. 2001; Hesselink 2005.
[1235] Mak 2008, p. 26.

Nowadays, marketers often suggest that people who don't block tracking cookies in their browser give implied consent to tracking cookies. But this interpretation of the law seems incorrect. As the Article 29 Working Party notes, the mere fact that a person leaves the browser settings untouched doesn't mean that the person has expressed the will to be tracked. In sum, the e-Privacy Directive requires consent for the use of most tracking technologies. There's much debate on whether opt-out systems are sufficient to obtain the user's consent or not.

In line with the transparency principle, consent has to be specific and informed. Furthermore, only "free" consent can be valid. Nevertheless, in most circumstances, current data protection law will probably allow controllers to offer take-it-or-leave-it choices. Hence, in principle website publishers are allowed to install tracking walls that deny entry to visitors that do not consent to being tracked.

As far as personal data are being processed, the Data Protection Directive also applies to behavioural targeting. As we saw in the previous chapter, behavioural targeting does indeed entail personal data processing in most cases. The Data Protection Directive only allows personal data processing if it can be based on consent or another legal basis. For the private sector, the most relevant legal bases are: a contract, the balancing provision, and the data subject's consent.

As discussed in chapter 4, marketers feared that direct mail marketing would only be allowed with the data subject's prior consent when the European Commission presented a proposal for a Data Protection Directive in 1990. After lobbying by the direct marketing industry, the European Commission said in 1992 that personal data processing for certain types of direct mail marketing can be based on the balancing provision: on an opt-out basis.[1236] In brief, a firm can rely on the balancing provision when the processing is necessary for its legitimate business interests, and these interests are not overridden by the data subject's fundamental rights. The "necessary"

[1236] See chapter 4, section 1.

requirement sets a higher threshold than useful or profitable. If a firm relies on the balancing provision for direct marketing, data protection law grants the data subject the right to stop the processing: to opt out.

The Data Protection Directive doesn't state explicitly whether behavioural targeting (a type of direct marketing) can be based on the balancing provision. But the most convincing view is that behavioural targeting can't be based on the balancing provision, in particular if it involves tracking an internet user over multiple websites. In most cases the data subject's interests must prevail over the firm's interests, as behavioural targeting involves collecting and processing information about people's browsing behaviour, which many people regard as personal. Indeed, the Working Party says firms can almost never base personal data processing for behavioural targeting on the balancing provision.

A firm can also process personal data if the processing is necessary to perform a contract with the data subject. For instance, certain data have to be processed for a credit card payment, or for a newspaper subscription. Some internet companies suggest that a user enters a contract by using their services, and that it's necessary for this contract to track the user for behavioural targeting. As the Interactive Advertising Bureau US puts it, "visiting a web site is a commercial act, during which a value exchange occurs. Consumers receive content, and in exchange are delivered [targeted] advertising."[1237] But according to the Working Party, in general, firms can't rely on this legal basis for behavioural targeting. In any case, the practical problems with informed consent to behavioural targeting which are discussed in the next chapter would be largely the same if firms could base the processing for behavioural targeting on a contract with the data subject.

If firms want to process personal data, and can't base the processing on a legal basis such as a contract or on the balancing provision, they must ask the data subject for

---

[1237] Rothenberg (IAB US) 2013. See for a critical analysis of such claims: chapter 7, section 2.

consent. The Working Party says consent is generally the required legal basis for personal data processing for behavioural targeting. In sum, consent plays an important role in the EU legal regime for behavioural targeting. Data protection law is clearly influenced by the perspective of privacy as control over personal information.

While consent plays an important role in EU data protection law, that role is limited at the same time. The other provisions in the Data Protection Directive are mandatory (with a few exceptions). The data subject can't waive data protection law's safeguards, and can't contract around the rules. Therefore, data subjects don't enjoy full contractual freedom regarding personal data concerning them.

Nevertheless, this study takes the view that data protection law isn't unduly paternalistic. The European legal system accepts, and perhaps requires, a degree of paternalism. Furthermore, there are other rationales for data protection law than protecting people against themselves. The right to privacy and the right to data protection aim to contribute to a fair society, which goes beyond protecting individual interests. And from an economic perspective, regulatory intervention isn't paternalistic if it aims to reduce market failures, such as information asymmetries. The relevance of market failures for the regulation of behavioural targeting is elaborated in the next chapter.

* * *