Improving privacy protection in the area of behavioural targeting

Zuiderveen Borgesius, F.J.

Publication date
2014
Document Version
Final published version

7 Informed consent in practice

Considering the important role of informed consent in the current regulatory regime for behavioural targeting, this study can't ignore how people make privacy choices in practice. Is it feasible that people manage their privacy in the area of behavioural targeting through the legal instrument of informed consent?

For this chapter literature from the emerging field of the economics of privacy was analysed, as well as behavioural economics literature and social science studies on how people make privacy choices. The chapter could also be seen as a critical analysis of the privacy as control perspective, as the idea of informed consent is closely related to the control perspective.[1238]

Economics and behavioural economics provide useful tools to analyse certain problems with informed consent in practice. Even if one doesn't agree with economic rational choice theory (which is discussed in section 2), concepts such as information asymmetry, transaction costs and externalities can help to analyse different problems with the informed consent approach. While economists might use different phrases, the arguments derived from economics aren't necessarily new for legal scholars. To illustrate, if a lawyer says "[t]he opt-out options Google offers authenticated users are labour-intensive,"[1239] an economist might say that the transaction costs are too high.

[1238] See on the privacy as control perspective chapter 3, section 1, and chapter 4, section 5.
[1239] College bescherming persoonsgegevens (Dutch DPA) 2013 (Google) p. 31.

To apply economic theory, this chapter compares consenting to behavioural targeting with entering into a market transaction.[1240] This study does *not* argue that personal data should be seen as tradable goods on a market.[1241] Rather, the approach in this chapter is as follows. If one compares, for argument's sake, consenting to behavioural targeting with entering into a market transaction, economic theory suggests that there are market failures that justify more legal intervention.

Another reason to discuss economics in this study is that it's sometimes suggested that behaviourally targeted advertising is needed to fund the internet: "[w]hat powers the 'free' Internet are data collection and advertising."[1242] However, this chapter shows that such claims are too simple. For instance, in the long term behavioural targeting may decrease ad revenues for some website publishers. Furthermore, the chapter shows that it's an open question whether behavioural targeting is good or bad from an economic perspective.

Section 7.1 of this chapter discusses studies on people's attitudes towards behavioural targeting. Section 7.2 introduces the economic analysis of law, and the economic analysis of privacy. The section also discusses the limitations of the economic perspective on privacy. Section 7.3 analyses problems with informed consent through an economic lens. Section 7.4 turns to behavioural economics. The analysis in this chapter can help to explain the alleged privacy paradox (section 7.5): people say they care about privacy, but often fail to protect their information. Section 7.6 concludes.

[1240] For ease of reading, this chapter speaks of "consent to behavioural targeting." From a legal perspective, it would be more correct to speak of (i) unambiguous consent to personal data processing for behavioural targeting (in the sense of article 7(f) of the Data Protection Directive), and of (ii) consent to the use of tracking technologies (in the sense of article 5(3) of the e-Privacy Directive.

[1241] See on inalienability Calabresi & Melamed 1972.

[1242] Thierer 2010. See for similar claims e.g. Interactive Advertising Bureau Europe Youronlinechoices.

7.1 People's attitudes regarding behavioural targeting

Research suggests that, while some like the idea, most people don't want targeted advertising based on their online behaviour. People realise the possible benefits from targeted ads and content, but also find the underlying data processing creepy.

Turow et al. found in a nationally representative phone survey that 66% of adult Americans didn't want to receive advertisements that are tailored to their interests. The number was 55% for the age group between 18 and 24. When people were told that tailored advertisements would be based on their browsing behaviour, 87% didn't want targeted advertising. People were also asked whether they would allow marketers to "follow you online in an anonymous way in exchange for free content." 68% said they would definitely not allow it, and 19% probably wouldn't.[1243] The researchers conclude: "Contrary to what marketers say, Americans reject tailored advertising (…). Whatever the reasons, our findings suggest that if Americans could vote on behavioural targeting today, they would shut it down."[1244] The TRUSTe company found similar results: only 15% of the respondents would "definitely or "probably" consent to tracking for more relevant advertising.[1245]

In a survey by Cranor & McDonald, 18% of the respondents wanted behaviourally targeted advertising because it leads to more relevant advertising. 12% didn't mind being tracked. On the other hand, 46% found it "creepy" when advertisements are based on their browsing behaviour. 64% agreed with the statement "[s]omeone keeping track of my activities online is invasive."[1246] The researchers also questioned people about firms analysing the contents of email messages for targeted advertising. This is a common practice for so-called "free" email services such as Gmail and Yahoo. 4% liked their email being scanned because it could lead to more relevant

---

[1243] Turow et al. 2009, p. 16.
[1244] Turow et al. 2009, p. 4.
[1245] TRUSTe Research in partnership with Harris Interactive 2011.
[1246] Cranor & McDonald 2010, p. 23. See in detail about the demographics of the respondents p. 5-6. See also McDonald 2010.

advertising. About one in ten indicated "it's ok as long as the email service is free."[1247] But 62% found advertising based on email content creepy.[1248] A study among university students in Toronto found similar results.[1249]

Some studies find less negative attitudes to behavioural targeting. Hastak and Culnan found that 48% felt uncomfortable about their browsing behaviour being used for advertising. 23% were comfortable with it. That number grew to 40% if websites would give information about behavioural targeting and would offer an opt-out system.[1250] Some, but not all, industry-sponsored surveys find more positive attitudes towards behavioural targeting. For instance, one report says: "[m]ost consumers (84%) state they would *not* pay for access to online content that is free now, and instead, they would rather receive targeted advertising in exchange for free access to online content" (emphasis original). On the other hand, the report says: "Nearly all (93%) Internet users would use or already use the DNT button, however, only 22% of users are aware of this function."[1251] It should be noted that industry-sponsored studies aren't always clear on the methodology.[1252]

Ur et al. report on 48 in-depth interviews about online behavioural advertising. After being informed about behavioural targeting, people saw disadvantages and benefits. Almost half of the participants liked the idea of more relevant advertising. On the other hand, a majority mentioned privacy when asked whether there were downsides to behavioural targeting. "Participants commonly said they were scared about being tracked and monitored."[1253] People also complained about the lack of control.[1254] Most participants didn't like the idea of behavioural targeting. "However, this attitude seemed to be influenced in part by beliefs that more data is collected than actually

---

[1247] Cranor & McDonald 2010, p. 22.
[1248] Cranor & McDonald 2010, p. 21.
[1249] Foster et al. 2011.
[1250] Hastak & Culnan 2010.
[1251] Annalect 2012.
[1252] See for criticism on studies by Westin for instance Hoofnagle & Urban 2014.
[1253] Ur et al. 2012, p. 7.
[1254] Ur et al. 2012, p. 6.

is."[1255] The researchers conclude that people find behavioural targeting "smart, useful, scary, and creepy at the same time."[1256]

Results from European researchers are in line with the American results. A large study (26,574 people) in the European Union found that people were worried about privacy, and that they wanted more control over their information. "Nearly three-quarters of Europeans say their approval should be required in all cases before any kind of personal information is collected and processed."[1257] The study also found that seven out of ten people were concerned that firms might use data for new purposes such as targeted advertising without informing them.[1258] Only 22% indicated that they trusted search engines, social network sites, or email services to protect their information.[1259]

In interviews in the United Kingdom, Brown et al. found that people disliked third party data collection. "There was a strongly negative, almost emotional reaction in every group to the idea of third parties collecting data across a range of different devices and activities to develop an understanding of every aspect of consumers' lives."[1260] Interviews in the Netherlands suggest that few people were aware of behavioural targeting. People expressed privacy concerns after being told about it.[1261] A study by the Dutch Dialogue Marketing Association found that 70% of the respondents didn't want behavioural advertising.[1262] A 2012 representative study in the United Kingdom found that 8% of the respondents were comfortable with advertising based on their browsing history.[1263] 10% was conformable with Gmail scanning the contents of emails for targeted advertising. Around eight out of ten

---

[1255] Ur et al. 2012, p. 11.
[1256] Ur et al. 2012, p. 6.
[1257] European Commission 2011 (Eurobarometer), p. 172.
[1258] European Commission 2011 (Eurobarometer), p. 146.
[1259] European Commission 2011 (Eurobarometer), p. 138.
[1260] Brown et al. 2010, p. 83.
[1261] Helberger et al. 2012, p. 70.
[1262] Boogert 2011.
[1263] Bartlett 2012, p. 36-37.

people worried about firms using their data without consent and selling data to third parties.[1264]

Sometimes it's suggested that the younger generation doesn't care about privacy. "People have really gotten comfortable not only sharing more information and different kinds, but more openly and with more people. That social norm is just something that has evolved over time," said Mark Zuckerberg, Facebook's CEO.[1265] Such claims have some appeal at first glance. Some teenagers post "drunk" pictures or other information about private matters on Facebook. But research suggests that young people do care about privacy. Dana boyd concludes from her ethnographic research: "[m]uch to the surprise of many adults, teens actually care about privacy and take measures to make accessible content meaningless to outside viewers."[1266] An American study by the Pew Research Centre finds that young adults (18-29) are more likely than other older people to take steps like clearing cookies or browsing history.[1267] Other studies by the Pew Research Centre confirm that young people care about privacy.[1268] Given these outcomes, the claim that young people don't care about privacy seems incorrect. Furthermore, even if teens cared less about their privacy, this wouldn't prove that social norms have changed. Some teens drive too fast, drink too much, or take drugs recreationally. 10 or 20 years later, many have changed their habits.[1269]

Surveys and interviews give more reliable information than mere intuition, but they must be interpreted with caution. People often act differently in practice than might be expected from them based on survey results. This is the case for privacy choices as well. People say they care deeply about privacy, yet often divulge personal

---

[1264] Bartlett 2012, 39.
[1265] Zuckerberg, quoted in Kirkpatrick 2010. See generally on Zuckerburg on privacy The Zuckerberg files 2014.
[1266] Boyd 2012, p. 16 (internal citations omitted). Ethnography is "a qualitative research methodology used by social scientists to understand and document cultural practices. Born out of anthropology – and embraced by many other disciplines – ethnographic work seeks to capture and explain the social meaning behind everyday activities" (boyd 2014, p. 23).
[1267] Pew Research Center 2013, p. 10.
[1268] Pew Research Center 2013a.
[1269] See Richards 2014a, p. 17-18.

information in exchange for minimal benefits. Section 5 returns to this "privacy paradox."[1270] Furthermore, it's difficult to generalise findings from studies that use different methods. Many studies discussed above are from the US, and one should be careful when extrapolating the results to Europe. Another problem with surveys about privacy is that people who care a lot about their privacy may refuse to answer survey questions.[1271]

While caution is needed with interpreting the surveys and interviews, a couple of common themes emerge. People have mixed feelings. They see advantages in personalised advertising, but find it creepy at the same time. A small minority says it prefers behaviourally targeted advertising because it leads to more relevant ads. But a majority says it doesn't want behavioural targeting. Such survey results provide an argument in favour of legal intervention to improve privacy protection in the area of behavioural targeting.

7.2 Economics of privacy

In this chapter, economic theory is used to analyse problems with a legal construction: informed consent to data processing for behavioural targeting. This section gives a cursory introduction on the economic analysis of law.[1272] The section then introduces the emerging field of the economics of privacy. Finally, the limitations of the economic analysis of privacy are highlighted.

Law and economics is described by Posner as the "economic analysis of legal rules and institutions."[1273] Economics can be defined as "the science which studies human behaviour as a relationship between ends and scarce means which have alternative

---

[1270] See Acquisti 2010b, p. 6.
[1271] Heisenberg 2005, p. 39-40.
[1272] The introduction doesn't capture all the subtleties of economic theory and law and economics scholarship.
[1273] Posner 2011, p. xxi. This study uses the phrases "economic analysis of law" and "law and economics" interchangeably. See for an introduction to law and economics Kornhauser 2011.

uses."[1274] Like lawyers, economists look at the world in a particular way. Economics concerns the question of how parties make decisions when trying to maximise their preferences, with the limited means at their disposal.

In neoclassical economics (economics for short), it's usually assumed that parties want to maximise their own welfare, or their own utility.[1275] For example, a firm aims to maximise profit. But welfare doesn't merely concern money or things that are usually given a monetary value. An individual also aims to maximise welfare, which may include happiness, satisfaction, psychological well-being, or privacy.[1276]

Economists often use rational choice theory to predict human behaviour. Rational choice theory analyses behaviour assuming that people generally want to maximise their welfare, and that people can choose the best way to maximise their welfare. In short, it's assumed that people act "rationally" on average. Rational choice theory is a tool to predict human behaviour and doesn't aim to fully describe reality.[1277] "It is a *method* of analysis," says Becker, "not an assumption about particular motivations."[1278] Rational choice theory doesn't suggest that people always act rationally. But by assuming that people act rationally on average, the theory can still be used to predict human behaviour, and to reflect on how to regulate behaviour. For example, say a lawmaker raises the fines for speeding to deter people from driving too fast. The lawmaker assumes that people weigh the benefit of quick arrival against the potential cost of paying a fine. Even though some people might still drive too fast, on average, the measure could lead to less speeding.[1279]

[1274] Robbins 2007 (1934), p. 15.
[1275] This study speaks of economics for ease of reading, but it would be more correct to speak of "neoclassical economics." The neoclassical school of economics is merely one of a number of schools in economic thought, but neoclassical economics is presently the most influential school. Other schools include Austrian, Marxist, and Keynesian economics. See for an accessible overview of economic thought, distinguishing nine schools: Chang 2014, p. 109-169 (chapter 4) with further references (p. 165).
[1276] See Cooter & Ulen 2012, p. 12.
[1277] Posner 2011, p. 4.
[1278] Becker 1993, p. 385.
[1279] See Posner 1998, p. 1556-1557.

Law and economics literature often analyses which rule leads to the highest aggregate welfare for society (social welfare).[1280] In theory, there are situations in which social welfare increases: if somebody gains, and nobody incurs a loss. If nobody can increase their welfare without imposing costs on others, the situation is called "Pareto efficient."[1281] A different efficiency criterion is Kaldor Hicks efficiency, which refers to a situation where one person gains more than another person loses. According to this criterion, social welfare increases, if there's a change in which the gains of the winners are so great that they could compensate the losses of the losers. The Kaldor Hicks criterion doesn't require that winners actually compensate losers. In other words, the Kaldor Hicks criterion concerns the size of the pie and not how the pie is distributed. Any change that increases the pie is an improvement under the Kaldor-Hicks criterion.[1282] From this perspective, the question of how welfare is distributed within society is less relevant. In economics, tax is often seen as the best way to distribute wealth within society. Like this, for legal rules other than tax rules it makes sense to concentrate on how to enlarge the pie, rather than how to distribute the pie.[1283]

In economic theory, a (hypothetical) perfectly functioning free market leads to the highest social welfare – provided there are no market failures and setting aside how welfare is distributed within society. Private exchanges should lead to the highest social welfare, because people are assumed to enter contracts only when they expect to gain something from it, as they aim to maximise their expected welfare. Therefore, in theory unrestricted trade in a market without market failures leads to the highest aggregate welfare. This explains why economists are sometimes sceptical of laws that interfere with the free market, or that interfere with contractual freedom.[1284]

[1280] The economic analysis of law could thus be seen as a utilitarian approach.
[1281] See Kornhauser 2011.
[1282] See Kornhauser 2011.
[1283] See e.g. Kaplow & Shavell 1994. See also Hesselink 2011a, p. 298-301; Wagner 2010, p. 63.
[1284] Trebilcock 1997, p. 7; Hermalin et al. 2007, p. 24.

In reality, the ideal type of a perfectly functioning free market is exceedingly rare. From an economic perspective, there may be reason for the lawmaker to intervene when the market doesn't function as it ideally should. The law should aim at reducing market failures, such as information asymmetries, externalities, and market power. But legal intervention brings costs and economic distortions as well, and this has to be taken into account. From this perspective, legal intervention should thus be limited to situations where the costs of intervention are lower than the costs of the market failure.[1285]

Sometimes the law seems to be based implicitly on a kind of rational choice model. Put differently, sometimes the law appears to assume that people make choices in their own best interests, as long as they have enough information upon which to base their decisions.[1286] Contractual freedom, or party autonomy, is one of the primary principles of contract law – although it's never absolute.[1287] The notion of "informed consent" in data protection law, influenced by Westin's privacy as control perspective, also seems to be inspired by the idea that data subjects make "rational" choices. As Hoofnagle & Urban put it, "Westin's homo economicus (…) is expected to negotiate for privacy protection by reading privacy policies and selecting services consistent with her preferences."[1288]

Economic analysis of privacy

Economic theory can be used to analyse aspects of people's choices regarding privacy.[1289] One of the leading scholars in the economics of privacy is Acquisti. He

---

[1285] Market failure is "[a] general term describing situations in which market outcomes are not Pareto efficient" (Organisation for Economic Co-operation and Development (OECD) 1993, p. 55). See Hermalin et al. 2007, p. 30; Luth 2010, p. 15.
[1286] Ben-Shahar & Schneider 2011, p. 650; Sunstein & Thaler 2008, p. 6.
[1287] Grundmann summarises: "party autonomy dominates and the limits are seen as exceptions" (Grundmann 2002, p. 271). See also article II – 1:102 of the Draft Common Frame of Reference (Principles, Definitions and Model Rules of European Private Law), which contains the principle of contractual freedom: "Parties are free to make a contract or other juridical act and to determine its contents, subject to any applicable mandatory rules."
[1288] Hoofnagle & Urban 2014 (abstract).
[1289] See for an overview of the field of the economics of privacy Acquisti 2010a; Acquisti 2010b; Acquisti & Brandimarte 2012; Hui & Png 2006; Brown 2013.

explains: "the economics of privacy attempts to understand, and sometimes measure, the trade-offs associated with the protection or revelation of personal information."[1290]

An example of a trade-off is using a social network site. The user discloses personal data (a cost) to gain welfare: the use of a so-called "free" service. For instance, people don't pay with money for Facebook, which in turn analyses their behaviour for marketing purposes. Many email services offer a similar trade-off. They analyse the contents of messages for targeted advertising.[1291] As a US judge notes about Google: "in this model, the users are the real product."[1292] A website publisher that allows third party tracking on its website also offers a trade-off to visitors. Website visitors disclose personal information, and in exchange they can consult the website. Another example of a trade-off is joining a supermarket loyalty card programme. Customers disclose personal data, like their name and information about their shopping habits, in exchange for discounts.

Whether people realise that firms gather personal data is another matter. Acquisti notes that trade-offs can exist, even when people don't realise they disclose personal information: "the existence of such trade-offs does not imply that the economic agents are always aware of them as they take decisions that will impact their privacy."[1293] Hence, a "trade" could be analysed with economic theory, even when from a legal perspective there's no agreement to trade personal data for the use of a service. As noted, this study does not suggest that consenting to data processing *should* be seen as entering a contract from a legal perspective.[1294]

[1290] Acquisti 2010, p. 23.
[1291] See Acquisti & Brandimarte 2012, p. 548; European Data Protection Supervisor 2014, p. 10.
[1292] United States District Court, Northern District of California, San Jose division, Case C-12-01382-PSG, Order granting to dismiss (re: docket No. 53, 57, 59), 3 December 2013, In re Google, Inc, privacy policy litigation. See also Blue_beetle 2010: "If you are not paying for it, you're not the customer; you're the product being sold."
[1293] Acquisti 2010a, p. 4.
[1294] There is some debate on the question of whether consent to data processing should be seen as entering a (type of) contract. See chapter 6, section 1.

Economic theory doesn't dictate the ideal level of privacy protection

This study doesn't aim to answer the question of whether behavioural targeting leads to a net benefit or a net cost for society from an economic viewpoint. Like people who work in other disciplines, economists disagree on the ideal level of privacy protection. Neither economic theory nor empirical economic research has provided a definitive answer to the question of whether behavioural targeting – or a law that limits behavioural targeting – would lead to more or less social welfare. Some economists say that more legal protection of personal data is good, but others argue the opposite. "Economic theory", concludes Acquisti, "has brought forward arguments both supporting the view that privacy protection *increases* economic efficiency, and that it *decreases* it."[1295] Empirical economic research doesn't arrive at definitive conclusions either. "Considering the conflicting analyses", says Acquisti, "the only straightforward conclusion about the economics of privacy and personal data is that it would be futile to attempt comparing the aggregate values of personal data and privacy protection, in search of a 'final,' definitive, and all-encompassing economic assessment of whether we need more, or less, privacy protection."[1296] Other scholars agree that it's an open question whether more or less legal protection of privacy would be better from an economic perspective.[1297]

Why would it be "futile" to try to calculate the level of privacy protection that leads to the highest level of aggregate welfare? It's hard to agree on which costs and benefits to count, and many costs and benefits will only become clear after many years. Furthermore, many privacy-related costs are difficult, perhaps impossible, to quantify. Researchers have tried to measure the benefits of using of personal data and the benefits of legal limits on using personal data. They come to contradicting

---

[1295] Acquisti 2010a, p. 34 (emphasis original). But see Swire, who suggests "economists are largely privacy skeptics (Swire 2003, p. 24).
[1296] Acquisti 2010b, p. 19. See also Acquisti 2010a, p. 42.
[1297] See e.g. Irion & Luchetta 2013, p. 39; Strandburg 2013.

conclusions. Some say that legal privacy protection reduces social welfare, because it limits data flows.[1298]

For example, behavioural targeting has benefits, for firms and internet users. Behavioural targeting leads to profit for many firms. Internet users can benefit when revenue from targeted advertising is used to fund so-called "free" internet services. (However, in the end consumers pay for this advertising if firms pass on the advertising costs in product prices.) Behaviourally targeted advertising can bring products under the consumers' attention, which could save them searching costs. But it would be difficult to calculate the total benefits of behavioural targeting.[1299]

Likewise, aggregating all costs of behavioural targeting is difficult, or even impossible. Costs for firms include money spent on data processing systems. Furthermore, some estimate that billions of Euros are lost, because people would engage in more online consumption if they felt their privacy were better protected online.[1300] The European Commission says it would be good for the market if people worried less about their privacy. "Lack of trust makes consumers hesitate to buy online and adopt new services."[1301]

Not protecting personal data can incur costs for data subjects. Some privacy-related costs could be calculated, at least in theory. For example, when a firm experiences a data breach, the leaked data could lead to identity fraud. Such costs could materialise years after the data are collected. Or if a person's email address is disclosed too widely, this could lead to that person receiving spam. The time it takes to clean one's inbox is a cost.[1302] If people invest time in avoiding being tracked, this is costly as well.[1303] Other privacy-related costs are harder to quantify. Such costs include

---

[1298] Acquisti 2010b; Acquisti 2010a, p. 25-29.
[1299] Acquisti 2010b, p. 13; Acquisti 2010a, p. 42.
[1300] Acquisti 2010b, p. 13; Acquisti 2010a, p. 21.
[1301] European Commission proposal for a Data Protection Regulation (2012), p. 1. See also recital 5 of the e-Privacy Directive.
[1302] Acquisti & Brandimarte 2012.
[1303] Calo 2013, p. 30.

annoyance, a creepy feeling, and the long-term effects on society. In sum, while it could be attempted to quantify whether behavioural targeting leads to a net benefit or to a net loss for society, such an economic analysis would be riddled with imperfections. Moreover, as discussed below, there's more to life than economic analysis.

Behavioural targeting and so-called "free" services

Sometimes marketers suggest that behavioural targeting is needed to fund the so-called "free" internet, or that stricter rules would impose too much costs on businesses.[1304] Firms would lose income that they derive from personal data, and firms would spend money on compliance. But the observation that regulation imposes costs on firms doesn't conclude the economic analysis. In economics, the relevant question is whether society as a whole wins or loses. But as it's often claimed that behavioural targeting funds the "free" internet, this claim is unpacked a bit further here.

Advertising funds an astonishing amount of internet services. Without paying with money, people can use online translation tools, access many (although not all) quality newspapers, use email accounts, watch videos, listen to music, etc.[1305] It's also clear that a lot of money is at stake with behavioural targeting. For example, in 2007 Google paid 3.1 billion dollars for DoubleClick, which was a leading firm in the field of behavioural advertising.[1306] Facebook makes its money from advertising and many ads on its site are likely to behaviourally targeted.

Notwithstanding, there's reason for scepticism about the argument that the web wouldn't be "free" anymore without behavioural targeting. After reviewing the limited available data, Strandburg concludes that "apocalyptic predictions of this sort

---

[1304] See for instance Interactive Advertising Bureau United Kingdom 2012; Interactive Advertising Bureau Europe 2013.
[1305] People do usually pay for internet access at home or through a cellphone plan.
[1306] Google Investor Relations 2007.

should be taken with a large grain of salt."[1307] Even if behavioural targeting were completely banned, online advertising would remain possible. For instance, contextual advertising (such as advertising for wine on websites about wine) doesn't require monitoring people's behaviour. And for years Google didn't use behavioural targeting for its search ads.[1308] Moreover, it seems plausible that advertisers who couldn't use behavioural targeting anymore would spend some of the money saved on that type of advertising on other kinds of online advertising. Furthermore, there's little public information on how effective behavioural targeting is in improving the click-through rate on ads, when compared to contextual advertising.[1309] One industry-funded paper suggests that behaviourally targeted ads cost around 2.5 as much for advertisers than randomly presented ads.[1310] But scholars have criticised the paper for its methods and assumptions.[1311]

As a side note, behavioural targeting isn't limited to so-called "free" services. Many providers of paid services also engage in behavioural targeting. For instance, internet access providers have inspected their subscribers' internet use for behavioural targeting. Meanwhile they continued to charge their subscribers.[1312] Many paid smart phone applications also collect data for behavioural targeting.[1313]

There's little public information about the relative share of behavioural targeting income compared to other types of online advertising – let alone from independent sources.[1314] Industry organisations sometimes claim that many jobs are dependent on behavioural targeting.[1315] But other industry reports suggest that behavioural targeting

---

[1307] Strandburg 2013, p. 152. Similarly Mayer 2011.
[1308] See Hoofnagle 2009.
[1309] See Strandburg 2013, p. 10; Mayer & Mitchell 2012, p. 8.
[1310] Beales 2010.
[1311] Mayer & Mitchell 2012, p. 8.
[1312] See on deep packet inspection for behavioural targeting chapter 2, section 2.
[1313] Thurm & Iwatani Kane 2010. See chapter 2, section 3.
[1314] See Strandburg 2013, p. 10; Mayer & Mitchell 2012, p. 8.
[1315] See for high estimates Interactive Advertising Bureau Europe & McKinsey 2010. See also Direct Marketing Association (United States) 2013: "The DDME ["Data-Driven Marketing Economy"] added $156 billion in revenue to the U.S. economy and fueled more than 675,000 jobs in 2012 alone. (…) Regulation would impact all innovation, small businesses, jobs and economic growth."

isn't a major part of all online advertising income. The ValueClick firm estimated in 2008 that behavioural targeting makes up a 3.4% share of all online advertising income.[1316] A 2009 report for the Interactive Advertising Bureau US estimated the behavioural targeting share to be 18%.[1317] The Dutch Interactive Advertising Bureau concluded in 2011 that 2% of all online advertising income in the Netherlands is based on behavioural targeting.[1318] This is partly a question of definitions. For instance, Google's search ads were counted as non-behaviourally targeted in the report. Nowadays, Google's search ads are, or at least could be, behaviourally targeted.

As noted in chapter 2, in the long run, behavioural targeting may actually decrease ad revenues for some website publishers.[1319] Without behavioural targeting, advertisers that want to reach New York Times readers have to advertise on the New York Times website. Behavioural targeting enables advertisers to target people who received a cookie on the New York Times website. This implies that advertisers can reach New York Times readers without buying expensive advertising space on the New York Times website. In sum, while it can't be ruled out that some services would cease being offered for "free" if the law limited the possibilities for behavioural targeting, the long-term economic effects of legal intervention are uncertain.

The argument that behavioural targeting shouldn't be limited because it funds "free" services resembles a well-known economic argument to be cautious with consumer protection rules: consumers as a group pay the price for rules that aim to protect consumers. Firms that suffer costs from consumer protection rules are likely to pass on these to consumers by raising prices. For instance, it could be argued that legal minimum safety standards for a consumer product raise the price of that product. The higher price could mean that consumers who can only afford to buy low quality goods

---

[1316] Otlacan 2008.
[1317] Beales 2010, p. 13.
[1318] Interactive Advertising Bureau The Netherlands 2011; Interactive Advertising Bureau The Netherlands & Deloitte 2011.
[1319] See chapter 2, section 1 and 6.

can't buy the product at all.[1320] In practice, such arguments don't stop the lawmaker from requiring minimum safety standards or adopting consumer protection rules. This makes sense. As Wagner puts it, "[r]ational consumers will be prepared to pay extra in exchange for some protection from the delivery of defective products."[1321]

To conclude, it's contentious whether more legal protection of personal data would increase or decrease social welfare from an economic perspective. "In principle, there is an optimal level of data protection regulation, but, given the state of the art, it is not possible to locate it with any degree of precision," summarise Irion & Luchetta. "There is no indication whatsoever (…) whether more or less privacy would be beneficial."[1322] Acquisti adds that "it may not be possible to resolve this debate using purely economic tools."[1323]

Limitations of economic analysis of privacy

Economics and behavioural economics provide useful analytical tools to analyse certain practical problems with informed consent for behavioural targeting. But economic analysis has its limitations, especially when discussing fundamental rights. Policy questions can't be answered solely on economic grounds. As Posner notes in his law and economics handbook, "there is more to justice than economics."[1324]

> But there is more to notions of justice than a concern with efficiency. It is not obviously inefficient to allow suicide pacts; to allow private discrimination on racial, religious, or sexual grounds; to permit killing and eating the weakest passenger in the lifeboat in circumstances of genuine desperation, to force people to give self-incriminating

[1320] See Sunstein 2013a, p. 8; Luth 2010, p. 35, with further references.
[1321] Wagner 2010, p. 63.
[1322] Irion & Luchetta 2013, p. 39.
[1323] Acquisti 2010a, p. 34.
[1324] Posner 2011, p. 35.

> testimony; to flog prisoners; to allow babies to be sold for adoption; to permit torture to extract information; to allow the use of deadly force in defense of a pure property interest; to legalize blackmail; or to give convicted felons a choice between imprisonment and participation in dangerous medical experiments. Yet all these things offend the sense of justice of modern Americans, and all are to a greater or lesser (usually greater) extent illegal. An effort will be made in this book to explain some of these prohibitions in economic terms, but many cannot be. Evidently, there is more to justice than economics, and this is a point the reader should keep in mind in evaluating normative statements in this book.[1325]

Acquisti agrees that economic analysis isn't the end of the story: "the value of privacy eventually goes beyond the realms of economic reasoning and cost benefit analysis, and ends up relating to one's views on society and freedom."[1326] Certain privacy harms "not merely intangible, but in fact immeasurable."[1327] He warns against an "extremisation" of the debate.[1328] Too much attention to economics and trade-offs may take our attention away from privacy infringements that are harder to quantify. Indeed, sometimes it's suggested that there's no need to regulate behavioural targeting because the "harm" is difficult to quantify in monetary terms.[1329] In any case, European data protection law applies to personal data processing, whether there's

---

[1325] Posner 2011, p. 35. I don't suggest that Posner finds law and economics ill-equipped to discuss privacy. Posner suggests that the protection of personal information is bad from an economic perspective (Posner 1978).
[1326] Acquisti 2004, p. 27. See generally on the limitations of economic analysis of privacy Cohen 2012, chapter 6.
[1327] Acquisti 2010b, p. 3.
[1328] Acquisti 2011.
[1329] This line of argument seems to be more prevalent in the US than in Europe. See e.g. Lenard & Rubin 2010; Szoka & Thierer 2008.

(quantifiable) harm or not. The harm question is relevant where data protection law requires balancing different interests.[1330]

The problem that some types of costs and benefits are hard to quantify isn't unique for privacy. As Ramsay puts it, "[t]here is always the danger that the more measurable costs (e.g., compliance costs) to directly affected groups will be regarded as outweighing the intangible benefits to a large and diffuse consumer group."[1331] He adds that firms may be tempted to exaggerate the costs:

> If policy making is based on an economic cost-benefit analysis, then it will be in the interests of pressure groups (…) to demonstrate through their own analysis the benefits or costs of particular policies – to the extent that certain concentrated producer groups have greater access to information and expertise this may cause policy-making to be skewed in their interests, and there is always the danger therefore that cost-benefit analysis will simply become another technique to be abused to promote particular interests.[1332]

Fairness, fundamental rights, and privacy's value in a democratic society play a marginal role in the economic analysis of privacy.[1333] But such considerations are important. Irion & Luchetta note that data protection law isn't economic regulation, and that its success shouldn't be measured by looking at its economic impact.[1334] And in the European legal system, economic arguments don't trump other arguments – and they shouldn't. As Hesselink puts it, "the law should govern the market rather than the

---

[1330] The balancing provision (article 7(f) of the Data Protection Directive) is the main example, but applying open norms such as "excessive" also requires the balancing of interests.
[1331] Ramsay 1985, p. 358.
[1332] Ramsay 1985, p. 358. Baldwin et al. 2011 (p. 323) and Sunstein 2013a (p. 175) also warn for this effect.
[1333] See for an amusing text on the difficulties of combining the viewpoints of an economic approach and a EU data protection approach Kang & Buchner 2004.
[1334] Irion & Luchetta 2013, p. 23. Of course, examining the economic impact of regulation is useful.

other way round."[1335] With these caveats, let's see what economics and behavioural economics have to offer.

7.3 Informed consent and economics

The economic analysis of privacy decisions is largely based on the view of privacy as control over personal information. Through an economic lens, consent to behavioural targeting can be compared with entering into a market transaction with a firm. Under rational choice theory, there may be reason for the lawmaker to intervene in contractual freedom, for instance because of market failures such as information asymmetries, externalities, or market power.[1336]

Information asymmetry

Information asymmetry describes "a situation where one party possesses information about a certain product characteristic and the other party does not."[1337] Since the 1970s economists devote much attention to markets with asymmetric information, for example where consumers have difficulties evaluating the quality of products or services. Akerlof used the market for used cars as an example.[1338] Suppose sellers offer bad cars ("lemons") and good cars. Sellers know whether they have a bad or a good car for sale, but buyers can't detect hidden defects. A rational buyer will offer the price corresponding to the average quality of all used cars on the market. But this means that sellers of good cars are offered a price that is too low. Hence, owners of good cars won't offer their cars for sale. The result is that the average quality of used cars on the market decreases. Buyers will therefore offer lower prices, and fewer people will offer their cars for sale. The average quality of cars on the market will

---

[1335] Hesselink 2005, p. 179.
[1336] US legal scholars have applied insights from law and economics to consent to online data processing (e.g. Kang 1998; Schwartz 2003). In Europe, Brown 2013 gives an analysis of market failures in the area of online privacy.
[1337] Luth 2010, p. 23.
[1338] Akerlof 1970. He focuses on one problem resulting from information asymmetry: adverse selection. Another market failure that is related to information asymmetry falls outside the scope of this study: moral hazard.

drop. Sellers thus don't compete on quality in a market characterised by asymmetric information about quality, resulting in a race to the bottom. This can lead to products or services of low quality.

From an economic perspective, there may be reason for the lawmaker to intervene, because information asymmetries can lead to market failure. For instance, an economist might argue that one of the main rationales for consumer law is responding to information asymmetry.[1339] Seen from this angle, the main reason for responding to information asymmetry is protecting a well-functioning market, rather than paternalistic motives towards the consumer. If a lawyer said that consumer law aims to protect consumers because of their weaker bargaining position, an economist might add that the weaker bargaining position can be largely explained by information asymmetry.[1340]

Information asymmetry and behavioural targeting

The current state of affairs regarding behavioural targeting is characterised by large information asymmetries.[1341] Many firms track people for behavioural targeting without them even being aware. When one sees releasing personal data as "payment" for services, it's clear that there are information asymmetries. As Cranor & McDonald put it, "people understand ads support free content, but do not believe data are part of the deal."[1342] To make an informed choice, people must realise they are making a choice.

Research shows that most people are only vaguely aware that data are collected for behavioural targeting. For instance, Ur et al. found in interviews that participants were

---

[1339] See e.g. Luth 2010, p. 15, p. 69; Howells 2005, p. 352; Grundmann 2002, p. 279.
[1340] See Ramsay 1985, p. 369. The European Court of Justice combines the two views: "the [Unfair Contract Terms] Directive is based on the idea that the consumer is in a weak position vis-à-vis the seller or supplier, as regards both his bargaining power and his level of knowledge" (ECJ, C-243/08, Pannon GSM, 4 June 2009, par. 22). See on paternalism chapter 6, section 6.
[1341] Acquisti & Grossklags 2007.
[1342] Cranor & McDonald 2010, p. 21.

"surprised to learn that browsing history is currently used to tailor advertisements."[1343] In a survey, Cranor & McDonald found that 86% of respondents were aware that behavioural targeting takes place.[1344] But they also find that people know little about how data relating to their online behaviour is collected: "it seems people do not understand how cookies work and where data flows."[1345] Furthermore, only 40% of respondents thought that providers of email services scan the contents of messages for the purpose of targeted advertising. 29% thought this would never happen, either because the law prohibits it, or because the consumer backlash would be too great. Almost half of Gmail users didn't know about the practice,[1346] while Gmail has been scanning emails for advertising since 2004.[1347] Research in Europe also suggests that many people are unaware of behavioural targeting.[1348] Cranor & McDonald conclude that people generally lack the knowledge needed to make meaningful decisions about privacy in the area of behavioural targeting.[1349] In addition, people who have learned how to defend themselves against tracking must update their knowledge constantly.[1350] For example, many firms used flash cookies to re-install cookies that people deleted. Hoofnagle et al. summarise: "advertisers are making it impossible to avoid online tracking."[1351]

But if firms did ask for consent for behavioural targeting, information asymmetry would still be a problem, notes Acquisti.[1352] First, there are many firms involved in serving behaviourally targeted ads, and the underlying data flows are complicated. It's almost impossible for people to find out what happens to their data. Will their name

---

[1343] Ur et al. 2012, p. 4.
[1344] However, only 51% of the respondents though that this happens a lot at present (Cranor & McDonald 2010, p. 21).
[1345] Cranor & McDonald 2010, p. 16.
[1346] Cranor & McDonald 2010, p. 21.
[1347] Battelle 2005, chapter 8.
[1348] Helberger et al. 2012, p. 70.
[1349] Cranor & McDonald 2010.
[1350] Acquisti and Grossklags 2007 make a similar point, giving other examples.
[1351] Hoofnagle et al. 2012, p. 273. See on tracking technologies chapter 2, section 2.
[1352] Acquisti 2010b, p. 15-16; Acquisti 2010a, p. 38. Acquisti doesn't explicitly present these three categories.

be tied to the profile of their surfing behaviour? Will their data be shared with other firms? If a firm goes bankrupt, will its database be sold to the highest bidder?[1353]

Second, even if people knew what firms did with their data, it would be difficult to predict the consequences.[1354] If a firm shares data with another firm, will the data be used for price discrimination? Will visits to a website with medical information lead to higher health insurance costs? If there's a data breach at a firm, will this lead to identity fraud?

Third, it's difficult for people to attach a monetary value to information about their behaviour, so they don't know how much they "pay." For instance, people may not know how much profit a firm makes with their information, or what the costs are of a possible privacy infringement. The value of the so-called "payment", that is the piece of personal information, depends on the question of what the receiving parties do with the personal information.[1355] Put differently: the "price" paid by the website visitor only becomes clear when firms exploit the personal information. "To what, then," asks Acquisti, "is the subject supposed to anchor the valuation of her personal data and its protection?"[1356]

As Vila at al. note, if the privacy-friendliness of websites is seen as a product feature, the web has characteristics of a lemons market.[1357] It's hard for people to determine how much of their personal information is captured during a website visit and how the information will be used. And website publishers rarely use privacy, or the absence of tracking, as a competitive advantage. Virtually every popular website tracks the

---

[1353] See e.g. the Toysmart case in the US (In re Toysmart.com, LLC, Case no. 00-13995-CJK, in the United States Bankruptcy Court for the District of Massachusetts 2000), and the Broadcast Press case in the Netherlands (Voorzieningenrechter Rechtbank Amsterdam, 12 February 2004, ECLI:NL:RBAMS:2004:AO3649 (Broadcast Press)).
[1354] Acquisti & Grossklags 2007, p. 365.
[1355] See Schwartz 2000a, p. 775; Strandburg 2013, in particular p. 130-165.
[1356] Acquisti 2010a, p. 39.
[1357] Vila et al. 2004. A similar conclusion is drawn by Pasquale 2013; European Data Protection Supervisor 2014, p. 33.

behaviour of visitors for behavioural targeting, or allows third parties to track the visitors.[1358]

"This situation looks like the classic market for lemons problem", says Strandburg about behavioural targeting. "Consumers cannot recognize quality (here, absence of data collection for advertising) and hence will not pay for it. As a result, the market spirals downward."[1359] After interviewing people in the online marketing business, Turow concludes that competition pushes firms towards privacy invasive marketing practices, which seems to confirm the lemons situation.[1360] Furthermore, many website publishers don't have much power in negotiations with ad networks. There also seems to be a lemons problem in the market for smartphone applications and social network sites.[1361]

There are firms, such as a few search engine providers, that use privacy-friendliness as a selling point.[1362] But it's difficult for a firm to distinguish itself from others by offering privacy-friendly services. Virtually every privacy policy begins with phrases along the lines of: "the privacy of our users is and will continue to be a top priority for us."[1363] (In many cases, website publishers firms say later in the privacy policy that they allow third party tracking.) Therefore, it's difficult for a website publisher to use the fact that it doesn't allow third party tracking as an incentive for potential visitors to use its website. At first glance, its privacy policy wouldn't look much different than privacy policies of other websites that do allow third party tracking.[1364]

A hypothetical fully rational person would know how to deal with information asymmetry and uncertainty. For instance, the person could base his or her decision on what happens to people's personal data on average, and he or she wouldn't be

---

[1358] See chapter 2, section 3.
[1359] Strandburg 2013, p. 156.
[1360] Turow 2011, p 199.
[1361] See on social network sites and information asymmetry Bonneau & Preibusch 2010.
[1362] Two examples are: <www.duckduckgo.com> and <www.startpage.com>. See also Willis 2013a, p. 128-130.
[1363] This phrase is taken from the blog post in which Yahoo said it wouldn't honour Do Not Track signals (Yahoo 2014). See on Do Not Track chapter 8, section 5.
[1364] See Marti 2014.

optimistic about quality in a lemons situation. But people don't tend to deal with information asymmetry in a "rational" way (see section 4 of this chapter).

One caveat: most authors that apply law and economics to behavioural targeting discuss the American situation. In the US, there's no general data protection law; online privacy is mostly governed by self-regulation, the Federal Trade Trade's Commission norms on unfair business practices, and narrowly tailored sector-specific statutes.[1365] In theory, the information asymmetry problems should be less severe if all firms complied with European data protection law. For instance, if firms would always comply with the purpose limitation principle, unexpected data uses should be rare. In practice compliance with data protection law is not a given, partly because many popular services are from American origin.[1366]

Transaction costs

The obvious reaction to information asymmetries is requiring firms to provide information to data subjects. But this runs into problems as well, because of transaction costs among other reasons. "Transaction costs are any costs connected with the creation of transactions themselves, apart from the price of the good that is the object of the transaction."[1367] Examples are the time a consumer spends on reading contracts, or searching for a product. Transaction costs aren't a market failure, but they can help to explain why the information asymmetry problem is difficult to solve.[1368]

Transaction costs and behavioural targeting

In the behavioural targeting area, the time it would take people to inform themselves is a transaction cost. Hence, because of transaction costs the information asymmetry

---

[1365] See Schwartz & Solove 2009.
[1366] See on the purpose limitation principle chapter 4, section 3. See on the (lack) of compliance chapter 8 section 1, and chapter 9, section 1.
[1367] Luth 2010, p. 20 (emphasis omitted). The classic article on transaction costs is Coase 1960.
[1368] See Dahlman 1979.

problem is likely to persist. Law and economics literature on consumer law suggests that consumers don't read standard contracts, partly because of the transaction costs. As consumers don't read standard contracts, there's information asymmetry, and firms don't compete on the quality of standard contracts. This can lead to a lemons situation, with contracts that are unfavourable to consumers.[1369] The situation is similar for behavioural targeting.

As noted, the transparency requirements in European data protection law should be distinguished from the obligation to obtain consent for data processing, or for using tracking technologies.[1370] In practice, many firms seek consent in their terms and conditions, or in their privacy policies. But hardly anyone reads privacy policies or consent requests. To illustrate, an English computer game store obtained the soul of 7500 people. According to the website's terms and conditions, customers granted "a non transferable option to claim, for now and for ever more, your immortal soul," unless they opted out. By opting out, people could save their soul and could receive a five pound voucher. But few people opted out. The firm later said it wouldn't exercise its rights.[1371]

Marotta-Wurgler researched the readership of end user license agreements (EULAs) of software products. She analysed the click streams of almost 50,000 households, and found an "average rate of readership of EULAs (…) on the order of 0.1 percent to 1 percent." On average, those readers didn't look long enough at EULA to read them.[1372] "The general conclusion is clear: no matter how prominently EULAs are disclosed, they are almost always ignored."[1373] There's little reason to assume the readership of privacy policies is much higher.

[1369] See e.g. Faure & Luth 2011, p. 342; Wagner 2010, p. 61-62; Schäfer & Leyens 2010, p. 105, p. 108.
[1370] See chapter 4, section 3.
[1371] Fox News 2010.
[1372] Marotta-Wurgler 2011, p 168.
[1373] Marotta-Wurgler 2011, p. 182.

There are several reasons why people don't read privacy policies. First, life is too short. Cranor & McDonald calculate that it would cost the average American 244 hours per year to read the privacy policies of the websites she visits. This would be about 40 minutes a day, or about half of the time that the average American spent online every day (in 2006). Expressed in money, this cost would be around 781 billion dollars, in lost productivity and lost value of leisure time, if people actually were to read privacy policies.[1374] The costs for individuals to inform themselves exceeded the revenues from the ad industry they might try to protect themselves from. All online advertising income in the US was estimated to be 21 billion dollar in 2007.[1375] Moreover, people have better things to do than reading privacy policies. In daily life, people encounter information everywhere. For instance, many services and products come with terms and conditions. And the law often requires firms to disclose information to people. For example, European consumer law also relies heavily on information requirements.[1376]

Privacy policies are often long and difficult to read. In one study, more than half of the examined privacy policies were too difficult for a majority of American internet users.[1377] A quarter of Europeans say privacy policies are too difficult.[1378] And privacy policies are often vague, and fail to make data processing transparent.[1379] (The author of this study often has trouble deducing from a privacy policy what a firm plans to do with personal data.)

And if people understood a privacy policy, it's questionable whether they'd realise the consequences of the combination and analysis of their data. A user might only release scattered pieces of personal data here and there, but firms could still construct detailed

---

[1374] It would be more correct to speak of the "opportunity costs" for the individual.
[1375] Cranor & McDonald 2008. The study only looked at the time to read first party notices, with no time estimates for third party privacy policies.
[1376] Luth 2010.
[1377] Jensen & Potts 2004.
[1378] European Commission 2011 (Eurobarometer), p 112-114.
[1379] Verhelst 2012, p. 221.

profiles by combining data from different sources.[1380] In addition, even if somebody manages to decipher a privacy policy, his or her quest might not be over. A website's privacy policy often refers to the privacy policies of ad networks or other firms. Hence, people might have to consult dozens of privacy policies to learn about data collection on one website. Some firms change their privacy policies without notice, so people would have to check a privacy policy regularly. All these transaction costs hinder meaningful decisions regarding behavioural targeting.

The accepting without reading problem isn't unique to the privacy field. Most consumers don't read (other) contracts either.[1381] Some have argued that an "informed minority" of consumers disciplines the market by reading contracts. The idea is that firms adapt their contracts to the few people who read contracts.[1382] But many authors are sceptical about the informed minority argument. If an informed minority is too small, it won't discipline the market.[1383] It seems there aren't enough people who read privacy policies to discipline the market in the behavioural targeting area. True, a change in a firm's privacy policy could lead to media attention, and sometimes firms react to that.[1384] But such cases are rare.

If somebody read and understood a privacy policy, transaction costs could still be a problem. Moving to another service often involves transaction costs for the user. For instance, transferring emails and contacts to another email provider costs time. Furthermore, "when the costs of switching from one brand of technology to another are substantial, users face *lock-in*."[1385] If iTunes changes its privacy policy, many people might just accept. And when all one's friends are on Facebook, it makes little

---

[1380] Barocas & Nissenbaum 2009, p. 6.
[1381] EU consumer law makes certain contract terms invalid, which makes it, to some extent, safe for consumers not to read contracts (see for instance the Unfair Contract Terms Directive).
[1382] Schwartz & Wilde 1978, p. 638.
[1383] See e.g. Luth 2010, p. 149; Bakos et al. 2009.
[1384] For instance, after attention in the press, Facebook offered people a way to opt out of their "Beacon" service (Debatin et al. 2009).
[1385] Shapiro & Varian 1999, p. 104.

sense to join another social network site.[1386] In addition, there might not be any privacy friendly competitors, especially since there's information asymmetry in the market. As noted, most popular websites allow third parties to track their visitors for behavioural targeting. To illustrate, it's hard to find a tracking-free news website.

Some firms use transaction costs strategically. Firms can discourage people from opting out, by requiring multiple mouse clicks for an opt-out. For instance, people face transaction costs when they want to opt out of receiving behaviourally targeted ads on the website Youronlinechoices, managed by the Interactive Advertising Bureau. It takes three clicks and a waiting period to opt out of receiving behaviourally targeted ads.[1387] Opting out of Google's advertising cookies takes five mouse clicks from its search page.[1388]

Lastly, reading privacy policies doesn't guarantee that somebody knows what will happen with his or her data. For instance, some firms don't act according to their privacy policy. Google said on a website that people who used the Safari browser on certain devices were effectively opted out of tracking, because Safari blocks third party cookies. But Google bypassed Safari's settings.[1389] It would take people too much time to keep track of whether firms actually comply with their privacy policies. Furthermore, things can go wrong. A firm could experience a data breach for example.

Because of transaction costs, there may be an economic argument for having policymakers set standards. As Baldwin et al. note, "if information disclosure rules were employed instead of [other] regulation in relation to food safety, a visit to the

---

[1386] The European Commission proposal introduces a right to data portability to mitigate the problem of lock-in. See article 18 and recital 55 of the European Commission proposal for a Data Protection Regulation (2012).
[1387] In a non-scientific test, I had to wait forty-five seconds. First I had to choose a country (click 1), then I had to click on "your ad choices" (click 2). Next I had to wait until the website contacted the participating ad networks. Then I could opt out of receiving targeted advertising (click 3). For several ad networks the website gave an error message. (See Interactive Advertising Bureau Europe - Youronlinechoices.) See Leon et al. 2012 for a more academic discussion of the (non) user friendliness of industry opt-out systems.
[1388] College bescherming persoonsgegevens (Dutch DPA) 2013 (Google), p. 82.
[1389] Felten 2012; Mayer 2012. See chapter 2, section 2.

supermarket would involve a very lengthy process of scrutinizing labels."[1390] Therefore, there could be an economic rationale for having regulators ensuring a reasonable level of food safety. "It might, in many circumstances, be far more efficient for consumers to rely on the expertise and protection of public regulators and inspectorates, rather than depend on their own individual assessments of risks.[1391] A similar argument can be made in the area of behavioural targeting.

Outside data protection law, rules that require firms to disclose information to people are ubiquitous as well. Lawmakers often choose this regulatory technique in the hope people will make decisions in their own best interests. In European consumer law, for instance, this is the predominant approach.[1392] But there's little evidence that providing information helps to steer people towards decisions in their own best interests. Many scholars are sceptical.[1393] Ben-Shahar & Schneider summarise: "[n]ot only does the empirical evidence show that mandated disclosure regularly fails in practice, but its failure is inevitable."[1394]

Privacy policies fail to inform people who use computers, and it's even more difficult to inform people who use mobile devices with smaller screens. Soon it may become even harder to make data processing transparent, if more objects will be connected to the internet. Common phrases in this context are the Internet of Things, ubiquitous computing, and ambient intelligence.[1395] It's hard to give people effective information about behavioural targeting when they use computers and smart phones, but transparency would be even harder to achieve if firms use objects without a screen for

---

[1390] Baldwin et al. 2011, p. 120.
[1391] Baldwin et al. 2011, p. 120. See also Helberger 2013a, p. 37.
[1392] Grundmann et al. 2001; Luth 2010, p. 228. See on the US: Ben-Shahar & Schneider 2011.
[1393] See for an overview, with references Luth 2010.
[1394] Ben-Shahar & Schneider 2011, p. 651.
[1395] See chapter 2, section 2.

data collection. And it's not straightforward how informed consent could work in such an environment.[1396]

The foregoing doesn't imply that data protection law's transparency principle is useless. The transparency requirements can help to make behavioural targeting controllable for Data Protection Authorities and lawmakers. Without data protection law more problems might remain hidden. If problems are brought to light, the lawmaker could intervene.[1397] Hence, data protection law's transparency requirements could serve an important purpose, even if they fail to empower the individual.

Externalities

From an economic viewpoint, one reason for legal intervention in markets is when an activity has negative effects on people other than the contract parties. Economists refer to costs or damage suffered by third parties as a result of economic activity as negative externalities. Externalities occur because contract parties that aim to maximise their own welfare don't let costs for others influence their decisions.

An example of an externality is environmental pollution. Suppose a firm produces aluminium, and sells it to another party. If producing aluminium causes pollution, it imposes costs on others. Rational producers and buyers ignore these costs. When the costs of pollution for others are taken into account, too much aluminium is produced from a social welfare perspective. Global warming could be seen as an enormous externality problem. Externalities can also be positive. If somebody hires a gardener to craft a beautiful garden in front of her house, other people in the street might enjoy

---

[1396] See Article 29 Working Party 2014, WP 223. There's research on how to enable informed consent in a ubiquitous computing environment. See e.g. Le Métayer & Monteleone 2009.

[1397] This is one of the rationales for the obligation for data controllers to notify Data Protection Authorities of processing operations (article 18-21 of the Data Protection Directive). The 2012 proposals abolish this requirement.

the sight. These neighbours gain welfare from the garden without paying for it; they enjoy a positive externality.[1398]

Many legal rules, such as the rules in environmental law, can be explained as a response to an externalities problem. Even a rule that makes a contract to commit a murder void could be seen in this light. The rule protects a third party, namely the intended victim. Similarly, a prohibition of falsely yelling "fire" in a crowded theatre could be seen as a response to an externality problem.[1399] Legal responses to externalities often limit an individual's freedom. Generally speaking, if the lawmaker wants to reduce negative externalities resulting from contracting practices, the rules have to be mandatory. If the lawmaker would use non-mandatory default rules, the contract parties would set the rules aside.[1400] After all, the externality is caused by the fact that the contract parties don't take the interests of non-contract parties into account.[1401] Legal responses to externalities have nothing to do with paternalism, as the rules don't aim to protect people against themselves.

Externalities and behavioural targeting

Are externalities relevant for consent to behavioural targeting? If somebody consents to sharing his or her data with a firm, there are no negative externalities at first glance. The person merely gives up an individual interest. But people's consent to behavioural targeting may lead to the application of knowledge to others. This could be seen as an externality imposed on others.[1402] For instance, say a supermarket can track the shopping behaviour of thousands of customers that joined a loyalty programme and consented to having their data analysed. The supermarket constructs the following predictive model: 90% of the women who buy certain products will give birth within two months. Out of privacy considerations, Alice didn't join the

---

[1398] See on externalities Coase 1960; Dahlman 1979; Trebilcock 1997, chapter 3; Luth 2010, p. 22.
[1399] See US Supreme Court, Schenck v. United States - 249 U.S. 47 (1919).
[1400] See on the difference between mandatory rules and default rules chapter 6, section 5.
[1401] Wagner 2010, p. 53.
[1402] See MacCarthy 2011; Brown 2013; Hildebrandt et al. 2008. See also Hirsch 2006, who compares negative externalities in the context of environmental law and privacy law.

loyalty programme. But when she buys certain products, the shop can predict with reasonable accuracy that she's pregnant.[1403] This could be seen as an externality imposed on Alice, which is a result from the fact that people consented to having their personal information processed. Hence, firms can also learn information about people who do not agree to data collection. This topic is completely separate from the issue of people tending to click "I agree" to many requests.[1404]

Moreover, if almost everybody consents to being tracked, *not* consenting could make somebody conspicuous. Does he or she have something to hide? Sometimes not divulging information, or not participating, can raise suspicion.[1405] Osama Bin Laden was found, partly because it was suspicious that his large compound didn't have internet access.[1406] And some intelligence services find it suspicious if internet users use privacy enhancing technologies.[1407]

There may be positive externalities when people consent to behavioural targeting. For instance, firms might use behavioural targeting data that are collected with consent for innovative products that other people can use. It could be seen as a positive externality if innovative products benefit other parties than the firm and the person that consented.[1408] An oft-cited example of a positive externality resulting from commercial data collection is Google Flu trends. In short, Google uses people's search behaviour to deduce information about the spread of flu.[1409] However, the usefulness of the service has been questioned.[1410]

[1403] The example is based on a news report on the US supermarket Target, which reportedly found that a woman was pregnant, based on the products she bought (see chapter 2, section 5).
[1404] See Barocas 2014, p. 159.
[1405] See Posner 2011, p. 25. Peppet 2011.
[1406] Ambinder 2011.
[1407] See for instance Greenwald & Ball 2013.
[1408] New uses of personal data may breach the purpose limitation principle, but we'll leave that topic aside for now (see chapter 4, section 3). Some might argue that so-called "free" websites are a positive externality, enjoyed by web users, of contracts between website publishers and advertisers (see Strandburg 2013, p. 108, who is critical of that claim).
[1409] Ginsberg et al. 2009.
[1410] Ohm 2013, p. 342. Furthermore, research suggests that Flu Trends isn't very accurate (Hodson 2014; Lazer et al. 2014).

The phrase "big data" has become a buzzword. There's no commonly accepted definition, but "big data" roughly refers to the analysing large data sets. Some have high hopes for "big data", and speak of "a revolution that will transform how we live, work and think."[1411] Others are sceptical.[1412] According to Arnbak for instance, "the concept of 'big data' [is] a carefully constructed frame by proponents of systematic surveillance for commercial purposes."[1413] As an aside, legal limits on the use of personal data don't imply that all advantages of large-scale data analysis are lost. Many positive externalities could also be generated by using aggregated data, rather than personal data. And not all large-scale data analysis ("big data") relies on data about individuals.

In this chapter, the focus is on externalities resulting from an individual consenting to a firm processing his or her personal data. Another example of a negative privacy externality is a firm that sells Alice's contact information to other firms, thereby increasing the chance that Alice is subjected to invasive marketing, such as spam.[1414] And privacy invasive tracking that results from a contract between an ad network and a website publisher could be seen as an externality imposed on website visitors.

In conclusion, it would be difficult to assess whether the positive externalities of behavioural targeting outweigh the negative externalities or vice versa. But consent to behavioural targeting does have negative externalities. If lawmakers want to respond to negative externalities, they generally need to use mandatory rules rather than default rules.

Market power

Market power, like a monopoly situation, may be a reason for legal intervention from an economic viewpoint. In a perfectly competitive market, many firms must compete

---

[1411] Mayer-Schönberger & Cukier 2013. See also Manyika et al. 2011; Tene & Polonetsky 2012a; Tene & Polenetsky 2013; Moerel 2014; World Economic Forum 2014.
[1412] See for instance boyd & Crawford 2013; Ohm 2013; Morozov 2013.
[1413] Arnbak 2013. See on behavioural targeting as surveillance chapter 3, section 3.
[1414] Varian 2009, p. 103.

for consumers and firms have no market power. Without problems such as information asymmetries, competition should lead to products that consumers want, for prices close to the productions costs. Competition should thus lead to the highest social welfare, and to consumer-friendly services. This is the rationale for laws that aim to mitigate market power, such as competition law. The opposite of a perfectly competitive market is a monopoly situation. A monopolist has market power and can raise prices without fearing the reaction of competitors.[1415]

Market power and behavioural targeting

Privacy scholars often complain that people lack real choice if firms offer take-it-or-leave-it-choices.[1416] This is a valid concern. As noted, from a data protection law perspective, sometimes the position of a firm asking consent is such that consent wouldn't be sufficiently "free."[1417] However, data protection law and economics use different frameworks. From an economic perspective the question of whether there's too much market power depends on the specifics of that particular market. The conclusion would be different for search engines, social networks sites, online newspapers, or games for phones.

Many take-it-or-leave-it choices regarding behavioural targeting may not be an abuse of market power from the viewpoint of competition law or economics.[1418] For instance, there could be a situation of monopolistic competition, where many firms compete by differentiating similar products. This often occurs in markets for magazines or newspapers. For online services, such as websites and smart phone apps, monopolistic competition is common as well. Monopolistic competition is usually not regarded as a market power problem from an economic viewpoint. If a

---

[1415] See Bar-Gill 2012, p. 16.
[1416] See Solove 2013, p. 1898; Blume 2012, p. 29; Rouvroy & Poullet 2009, p. 50; p. 70-74; Bygrave 2002, p. 58-59.
[1417] See chapter 6, section 3 and 4, and chapter 8, section 3 and 5.
[1418] See on the interplay between competition law and data protection law European Data Protection Supervisor 2014.

user said a website doesn't give a real choice whether to allow tracking or not, an economist might counter that the user could visit another website.[1419]

Even in a perfectly competitive market, many problems described in this chapter could remain. For example, information asymmetries can lead to a lemons situation with services that offer low privacy levels, even if a market is perfectly competitive.[1420] Therefore, market power may not be the main problem for consent to behavioural targeting.

Nevertheless, market power may be relevant for consent to behavioural targeting.[1421] As noted in chapter 2, the online marketing industry is becoming increasingly centralised.[1422] If in ten years a couple of firms are responsible for all behavioural targeting in the world, this calls for different regulatory answers than if thousands of firms engage in behavioural targeting.

In conclusion, people face severe difficulties when deciding whether to consent to behavioural targeting. One of the main problems is asymmetric information. Transaction costs make this information asymmetry difficult to overcome. From an economic perspective, information asymmetry can lead to market failure, which justifies regulatory intervention, provided that legal intervention doesn't bring too many costs or economic distortions. The next section shows that there are also "behavioural market failures" in the area of behavioural targeting.[1423]

7.4 Informed consent and behavioural economics

Behavioural economics highlights more problems with informed consent to behavioural targeting. Behavioural economics aims to improve the predictive power

---

[1419] In practice, there's a good chance that the same ad networks would track people on other websites. Chapter 8, section 3 and 5, and chapter 9, section 5 and 7, return to the topic of take-it-or-leave-it-choices.
[1420] Bar-Gill 2012, p. 16.
[1421] See on privacy and market power Brown 2013; European Data Protection Supervisor 2014.
[1422] Chapter 2, section 2.
[1423] The phrase "behavioral market failure" comes from Bar-Gill 2012.

of economic rational choice theory by including findings from psychology and behavioural studies. Research shows that people structurally act differently than rational choice theory predicts.[1424]

If many people made decisions that didn't conform to rational choice theory, but did so in different ways, on average their decisions might still conform to rational choice theory. Random deviations from rational choice theory would not influence the theory's predictive power in the aggregate.[1425] But people tend to make decisions that are *systematically* different from what rational choice theory predicts. Sunstein summarises: "[p]eople are not always 'rational' in the sense that economists suppose. But it does not follow that people's behaviour is unpredictable, systematically irrational, random, rule-free or elusive to scientists. On the contrary, the qualifications can be described, used, and sometimes even modeled."[1426]

One difference between people who conform to rational choice theory and people in the real world is that people in the real world have bounded rationality. Human attention is scarce. Simon explains: "[t]he term 'bounded rationality' is used to designate rational choice that takes into account the cognitive limits of the decision maker – limitations of both knowledge and computational capacity."[1427] The human mind has limited capacity for decisions that require taking many factors into account. People tend to be bad at calculating risks and at statistics in general.

Because of their bounded rationality, people often rely on rules of thumb, or heuristics. Kahneman defines a heuristic as "a simple procedure that helps find adequate, though often imperfect, answers to difficult questions."[1428] Most of the time such mental shortcuts work fine. "Do as the others do" is often a useful heuristic, for

---

[1424] There are heated debates among economists on the question of whether behavioural economics really adds something to neoclassical economics (see e.g. Posner 1998). This study doesn't take sides in this debate. Some might argue that certain biases discussed in this section could partly be explained under neoclassical economic theory (see e.g. Cofone 2014).
[1425] Posner 1998.
[1426] Sunstein 2000, p. 1.
[1427] Simon 1997 (1987).
[1428] Kahneman 2011, p. 98.

instance. When you are in a department store and everybody starts to flee for the exit, leaving the building too might be a good idea. But sometimes, heuristics lead to decisions that people later regret. "Humans predictably err."[1429] Such systematic deviations from rational choice theory, or common mistakes, are called biases.

Biases are studied and used in marketing and advertising.[1430] As Bar-Gill explains, "competition forces sellers to exploit the biases and misperceptions of their customers."[1431] Apart from questions of fairness, this can lead to "behavioural market failures", and thus decrease social welfare.

> The basic claim is that market forces demand that sellers be attentive to consumer psychology. Sellers who ignore consumer biases and misperceptions will lose business and forfeit revenue and profits. Over time, the sellers who remain in the market, profitably, will be the ones who have adapted their contracts and prices to respond, in the most optimal way, to the psychology of their customers.[1432]

Privacy scholars have started to take behavioural economics insights into account.[1433] Important behavioural research on how people make privacy choices is done by scholars such as Acquisti, Cranor and McDonald, who all work, or worked, at the Carnegie Mellon University in Pittsburgh. Acquisti & Brandimarte note that even fully informed people often have difficulties making privacy choices in their own interests.

[1429] Sunstein & Thaler 2008, p. 7.
[1430] Howells 2005, p. 361-362; Bar-Gill 2012.
[1431] Bar-Gill 2012, p. 2.
[1432] Bar-Gill 2012, p. 8. Luth 2010 reaches a similar conclusion (p. 81, p. 107-108, p. 288). See also Sunstein 2013a, p. 90; Sunstein 2013.
[1433] An influential paper is Acquisti & Grossklags 2007.

> As a matter of fact, the information available to individuals when making decisions regarding privacy is often incomplete (…). Moreover, due to bounded rationality, the individual cannot obtain and retain all information necessary to make a perfectly rational decision. Even if she could access all that information, and even if she had unlimited capability of information storage and processing, her choices would nonetheless be influenced by several psychological biases and heuristics (…) All these factors influence the individual's privacy decision-making processes in such a way that even if she was willing, in theory, to protect her privacy, in practice she may not do so.[1434]

Somebody who wants to make a rational choice to consent to behavioural targeting would have to take a number of factors into account. Making "rational" choices about complex matters such as privacy is difficult, and people often rely on heuristics for such choices. Relying on heuristics for privacy decisions can lead to biases, such as the status quo bias and present bias.

Status quo bias

The status quo bias, or inertia, refers to the power of the default.[1435] Most people don't change the default option. This means that the default setting will have a big impact on the dynamics between the firm and its users. A famous example of the status quo bias concerns the percentage of organ donors. Countries that use an opt-out system (people donate their organs unless they express that they don't want to donate) have many donors, while countries that use an opt-in system have few donors.[1436] The status quo bias is surprising from a rational choice perspective. Rational choice theory

---

[1434] Acquisti & Brandimarte 2012, p. 564.
[1435] See Samuelson & Zeckhauser 1988.
[1436] Johnson & Goldstein 2003.

would predict that people choose according to their preferences, regardless of the default option – assuming there are no transaction costs to changing the default.[1437]

Marketers can leverage the status quo bias. Free trial periods of newspapers can lead to subscriptions for years, because – in line with the status quo bias – people don't get around to cancelling. "Buy this pack of shampoo, and get a 2 euro refund", relies on transaction costs and the status quo bias. With such mail-in rebates, many people fail to send in the coupon. As an aside, sending in the coupon would also disclose one's name and bank account number to the firm.

The status quo bias is relevant for behavioural targeting. As Sunstein puts it, "true, we might opt out of a website policy that authorizes a lot of tracking (perhaps with a simple click) – but because of the power of inertia, many of us are not likely to do so."[1438] Few people tweak the settings of their browser or their social network site accounts.[1439] The effect of the status quo bias is aggravated if switching to another service also entails transaction costs.[1440]

Insights into the status quo bias help to understand the decades-old discussion about opt-in versus opt-out systems for direct marketing and behavioural targeting. This is basically a discussion on who profits from the status quo bias. Firms often prefer to collect personal data, unless people object. This illustrates that marketers understand the power of the default.[1441] Privacy advocates tend to prefer opt-in systems for privacy-intrusive practices.[1442] As noted, a purely dogmatic analysis of the law also leads to the conclusion that an expression of will is required for valid consent.[1443]

[1437] Of course, that assumption rarely holds in practice.
[1438] Sunstein 2013, p. 1893. See along similar lines Sunstein 2013a, p. 102.
[1439] On the settings of social media accounts Acquisti & Gross 2006.
[1440] See on transaction costs section 3 of this chapter.
[1441] As the DoubleClick ad network puts it, a default browser setting that doesn't allow third party cookies "is basically equivalent to not allowing them at all, because 99% of the population will see no reason to change the default." (Kristol p. 188.)
[1442] See Willis 2013a, especially p. 81.
[1443] See chapter 6, section 3 and 4.

Myopia and other biases

More biases are relevant for consent to behavioural targeting, such as myopia. Literally myopia means limited sight, or short sightedness. In behavioural economics, myopia refers to the effect that people tend to focus more on the present than on the future. People often pursue immediate gratification, thereby ignoring future costs.[1444] For example: "I can finish these footnotes on Sunday." People who are planning to lose weight might still eat a piece of cake, because it looks so good now, thereby forgetting they were planning to eat less sugar. Myopia also helps to explain why many people find it difficult to save money for their retirement.[1445]

People might choose immediate access to a service, even if this means they have to consent to behavioural targeting, contrary to earlier plans. Say Alice reads about behavioural targeting and decides not to accept any more tracking cookies. That night, she wants to read an online newspaper, and wants to watch the news online. Both websites deny entry to visitors that don't accept third party tracking cookies.[1446] Contrary to her earlier plans, Alice clicks "yes" on both websites. Hence, people don't always stick with default options. Sometimes this can be explained by myopia, or present bias.[1447]

Overconfidence and optimism biases are related to myopia. People tend to underestimate the risk of accidents and diseases, and overestimate the chances of a long and healthy life, or winning the lottery. Most drivers think they drive better than the average driver, and most newlywed couples think there's an almost 100% chance that they will stay together, even when they know that roughly one in two marriages

---

[1444] Luth 2010, p. 53.
[1445] Sunstein & Thaler 2008, chapter 6.
[1446] Early 2013 this was the case in the Netherlands. The National Public Broadcasting Organisation and one of the larger newspapers (Volkskrant) both installed a cookie wall (<www.publiekeomroep.nl> and <www.volkskrant.nl> accessed 15 February 2013). See chapter 6, section 4, and chapter 8, section 3 and 5.
[1447] In one Dutch survey, 30% doesn't want tracking cookies at all, and 41% only wants tracking cookies from some sites. However, 50% usually clicks "OK" to consent requests for cookies (Consumentenbond (Dutch Consumer Organisation) 2014).

ends in divorce.[1448] The success of "buy now, pay later" deals can be partly explained by myopia and optimism bias.[1449] Research suggests people also tend to underestimate the risks of identity fraud and of re-identification of anonymised data.[1450]

The way information is presented can also influence decisions. This is known as the framing effect.[1451] For example, many people see a link to a privacy policy as a quality seal. 41% of Europeans don't read privacy policies, because they think it's enough to check whether a website has one.[1452] In a California survey, the majority thought that the mere fact that a website had a privacy policy meant that their privacy was protected by law.[1453] Turow at al. argue that the phrase "privacy policy" is misleading.[1454] Facebook speaks of a "data use policy", which seems a more apt name.[1455]

Research suggests that privacy policies with vague language give people the impression that a service is more privacy-friendly than privacy policies that give more details.[1456] Another study suggests that "any official-looking graphic" can lead people to believe that a website is trustworthy.[1457] Böhme and Köpsell find that people are more likely to consent if a pop-up looks more like an end user license agreement (EULA). The researchers varied the design of consent dialog boxes and tested the effect by analysing the clicks of more than 80,000 people. They conclude that people are conditioned to click "agree" to a consent request if it resembles a EULA.

[1448] Sunstein & Thaler 2008, p. 31-33.
[1449] Sunstein & Thaler 2008, p. 35.
[1450] Acquisti & Grossklags 2005.
[1451] For example, Kahneman found that even among doctors, "[t]he statement that 'the odds of survival one month after surgery are 90%' is more reassuring than the equivalent statement that 'mortality within one month of surgery is 10%'" (Kahneman 2011, p. 88).
[1452] European Commission 2011 (Eurobarometer), p. 118-120.
[1453] Hoofnagle & King 2008; Turow 2003; Turow et al. 2005.
[1454] Turow et al. 2007.
[1455] Facebook, 'Data Use Policy'.
[1456] Good et al. 2006.
[1457] Moores 2005.

> [U]biquitous EULAs have trained even privacy-concerned users to click on "accept" whenever they face an interception that reminds them of a EULA. This behaviour thwarts the very intention of informed consent. So we are facing the dilemma that the long-term effect of well-meant measures goes in the opposite direction: rather than attention and choice, users exhibit ignorance.[1458]

Furthermore, Acquisti et al. discuss a "control paradox." People share more information if they *feel* they have more control over how they share personal information. The researchers conclude that control over personal information is a normative privacy definition: control *should* ensure privacy. But in practice, "'more' control can sometimes lead to 'less' privacy in the sense of higher objective risks associated with the disclosure of personal information."[1459]

Several authors conclude that there's a behavioural market failure regarding online privacy. Firms wouldn't stay in business if they didn't exploit people's biases. As Strandburg puts it, "[t]he behavioral advertising business model seems almost designed to take advantage of (…) bounded rationality."[1460] Firms often have larger data sets than scientists to discover biases. For instance, some internet firms can analyse the behaviour of hundreds of millions of people to test various designs and opt-out systems. Calo warns against "the mass production of bias."[1461]

7.5 Privacy paradox

There seems to be a privacy paradox. In surveys, people say they care about privacy. But people often divulge personal data in exchange for minimal benefits or

---

[1458] Böhme & Köpsell 2010.
[1459] Acquisti et al. 2012, p. 6.
[1460] Strandburg 2013, p. 149. See along similar lines Calo 2013; Acquisti 2010a, p. 6.
[1461] Calo 2013, p. 12. See for an example of a large-scale experiment by Facebook chapter 3, section 3.

convenience, and relatively few people use technical tools to protect their privacy online. Declared preferences (what people say in surveys) are often less reliable than revealed preferences (how people act). Sometimes it's suggested that people only care about privacy when they don't have to deal with other interests. "Consumers may tell survey takers they fear for their privacy, but their behaviour belies it. People don't read privacy policies, for example."[1462]

Scholars from various disciplines counter that people do care about privacy, but have difficulties acting according to their privacy preferences.[1463] Similarly, people who care about the environment might not study the label of every supermarket product to establish if it was produced in an environmentally friendly way.[1464] Another similarity with privacy policies is that merely studying the ingredients on a package may not be enough to assess how environmentally friendly a product is.

Regarding privacy decisions, it's doubtful whether revealed privacy preferences can be used to estimate how much people value their privacy in monetary terms. It's easy to manipulate the value people attach to their personal data.[1465] For instance, in a study by Cranor & McDonald, most participants believe they wouldn't pay one dollar a month to keep a website from using behavioural targeting. At first glance, this might suggest that few value protecting their information more than one dollar a month. But 69% would *not* accept a one dollar discount in exchange for having their data collected for behavioural targeting. This suggests that most people think their personal data is worth more than one dollar a month. In short, people's willingness to pay for privacy is different to their willingness to accept (a discount) to forego privacy.[1466] If it were assumed that people make "rational" choices to maximise their own welfare, in this case their privacy, the results would be surprising.

[1462] Goldman 2002.
[1463] See for instance Trepte et al 2014; Acquisti & Grossklags 2007; Solove 2013; Cranor & McDonald 2010. See also Cofone 2014. Moreover, fundamental rights also apply if people don't care about fundamental rights.
[1464] Thanks to Lauren Willis, who pointed this out at the Privacy Law Scholars Conference in Berkeley (2013).
[1465] See Acquisti et al. 2013a.
[1466] Cranor & McDonald 2010, p. 25. The effect that people value things more when they own them is called the endownment effect. See on that effect in the privacy context Acquisti et al. 2013a.

In follow-up interviews and a survey, Cranor & McDonald "found people generally unwilling to pay for privacy, not because they do not value it, but because they believe it is wrong to pay."[1467] 69% of the respondents agreed with the statement "Privacy is a right and it is wrong to be asked to pay to keep firms from invading my privacy."[1468] 61% agreed it would be "extortion" if a firm would ask them to pay for not collecting data. The researchers suppose "that one reason people will not pay for privacy is because they feel they should not have to: that privacy should be theirs by right."[1469] This suggests that the EU legal regime comes closer to the expectations of the US respondents in this research than a free market model regarding privacy.

Self-help tools exist to protect privacy in the area of behavioural targeting. For instance, people can install browser plug-ins that blocks ads and limit tracking, and millions of people do so.[1470] But many people find technical privacy protection tools too complicated.[1471] The time it would take people to learn to use the tools is a transaction cost. And even if a tool is easy, people might refrain from using it because they think it's difficult.[1472] In any case, so far most people seem to be losing the technological arms race. Some firms seem to be on a quest for more effective and opaque tracking technologies. For instance, it would be very difficult to detect or to protect oneself against device fingerprinting. If technology alone determined the level of online privacy, behavioural targeting firms would be likely to emerge as winners, and data subjects as losers.[1473]

This study doesn't suggest that all privacy problems can be attributed to behavioural biases. Even if people wouldn't have difficulties making decisions in accordance with

---

[1467] Cranor & McDonald 2010, p. 28.
[1468] Cranor & McDonald 2010, p. 26.
[1469] Cranor & McDonald 2010, p. 26.
[1470] The ad blocking software Adblok Plus was reportedly downloaded 200 million times (Adblock Plus 2014). Some estimate that between 9 and 23% of internet users use ad blocking software (Hill 2013). And in April 2014 there were about 2.5 million people connected users to the anonymity service Tor at any given moment (Tor 2014).
[1471] Leon et al. 2012. See for an amusing account of trying to use self-help tools Angwin 2014.
[1472] Willis 2013, p. 1164.
[1473] See chapter 2, section 2.

their declared interests, they still wouldn't be able to fully protect their privacy. For instance, it's very hard to defend oneself against group profiling.[1474] A firm that has a predictive model may need only a few data points to predict other information about somebody. Nevertheless, behavioural economics insights can help to explain the alleged privacy paradox.

Because privacy choices are context-dependent, caution is needed when drawing conclusions about the effect of biases. One bias might influence a privacy decision in one direction, while another bias might influence the same decision in another direction.[1475] Still, it would be naive to ignore behavioural economics when making laws that rely, in part, on the decisions of people whose privacy the law aims to protect.[1476]

7.6 Conclusion

This chapter analysed practical problems with informed consent, and thus with the privacy as control perspective. The chapter also discussed the economics of privacy and behavioural targeting.

As noted previously, this study offers suggestions to improve privacy protection, without being unduly prescriptive.[1477] If rules impose unreasonable costs on society, this study considers them unduly prescriptive. From an economic perspective, it's unclear whether behavioural targeting leads to a net benefit or a net loss for society. On the one hand, using personal data can increase social welfare. For instance, firms such as ad networks and website publishers profit from behavioural targeting. Income from online advertising could be used to fund so-called "free" web services. On the other hand, using personal data can decrease social welfare. For instance, if

---

[1474] Gürses 2010, p. 51. See section 3 of this chapter on externalities.
[1475] Acquisti & Grossklags 2007, p. 371. Luth 2010 arrives at a similar conclusion regarding consumer protection (p. 279-283).
[1476] Acquisti & Grossklags 2007, 374. In the context of EU consumer law Gomez reaches a similar conclusion (Gomez 2010, p. 110).
[1477] See chapter 1, section 1.

somebody's information ends up in the wrong hands, this could lead to receiving spam or to identity fraud. Other privacy related costs are harder to quantify, such as annoyance, a creepy feeling, and chilling effects. As it's unclear whether more or less privacy protection would be better from an economic perspective, more legal limits on behavioural targeting wouldn't necessarily be too costly.

From an economic perspective, consenting to personal data processing for behavioural targeting, or consenting to the use of a tracking cookie, can be seen as entering into a market transaction with a firm. But this "transaction" is plagued by information asymmetries. Many people don't know their behaviour is tracked, so their "choice" to disclose data in exchange for the use of a service isn't informed. But if firms sought consent for behavioural targeting, information asymmetry would remain a problem. People rarely know what a firm does with their personal data. And it's hard for people to predict the consequences of future data use. From an economic perspective, information asymmetry can lead to market failure, which can justify regulatory intervention. If people can't assess the quality of products or services, sellers won't compete on quality. This can lead to low quality products or services: a "lemons" market. Indeed, websites rarely compete on privacy. Virtually every popular website allows third parties to track its visitors.

Through an economic lens, data protection law's requirements for firms to be transparent about their data processing practices can be seen as an attempt to mitigate the information asymmetry. Website publishers can comply with the transparency requirements by disclosing the information in a privacy policy. But the information asymmetry problem is difficult to solve because of transaction costs. Reading privacy policies would cost too much time, as they are often long, difficult to read, and vague. "Only in some fantasy world do users actually read these notices and understand their implications before clicking to indicate their consent."[1478]

[1478] White House (Podesta J et al.) 2014, p. xi; see also p. 38.

Behavioural economics insights highlight more practical problems with informed consent. For instance, the status quo bias describes people's tendency to stick with default options. If people are assumed to consent if they fail to object, most people will "consent." With an opt-in system that requires an affirmative action for valid consent, people are less likely to consent.

Present bias, or myopia, suggests that people often choose immediate gratification and don't pay attention to future costs or disadvantages. If a website has a tracking wall, and people can only use the site if they agree to being tracked, they're likely to consent, ignoring the costs of future privacy infringements. The following chapters return to the topic of take-it-or-leave-it-choices.[1479]

In sum, behavioural economics can help to understand the alleged privacy paradox. People who say they care about their privacy often disclose information in exchange for small benefits. Part of this is conditioning: many people click "yes" to any statement that is presented to them. Exaggerating slightly: people don't read privacy policies; if they were to read, they wouldn't understand; if they understood, they wouldn't act.[1480]

* * *

[1479] See in particular chapter 8, section 3 and 5, and chapter 9, section 5 and 7.
[1480] Ben-Shahar and Schneider arrive at a similar conclusion on the regulatory technique of mandated disclosure of information in general: people "often do not read disclosed information, do not understand it when they read it, and do not use it even if they understand it" (Ben-Shahar & Schneider 2011, p. 665).