Improving privacy protection in the area of behavioural targeting

Zuiderveen Borgesius, F.J.

Publication date
2014
Document Version
Final published version

10 Summary and conclusion

This chapter summarises the study's main findings, draws conclusions, and answers the research question: how could European law improve privacy protection in the area of behavioural targeting, without being unduly prescriptive?

To protect privacy in the area of behavioural targeting, the EU lawmaker mainly relies on the consent requirement for the use of tracking technologies in the e-Privacy Directive, and on general data protection law. With informed consent requirements, the law aims to empower people to make choices in their best interests. But behavioural studies cast doubt on the effectiveness of the empowerment approach as a privacy protection measure. Many people click "I agree" to any statement that is presented to them. Therefore, to mitigate privacy problems such as chilling effects and the lack of individual control over personal information, this study argues for a combined approach of protecting and empowering the individual. Compared to the current approach, the lawmaker should focus more on protecting people.

The chapter is structured as follows. Section 10.1 gives an overview of how behavioural targeting works, and section 10.2 outlines privacy problems in the area of behavioural targeting. Section 10.3 discusses current data protection law. Section 10.4 discusses practical problems with informed consent to behavioural targeting, through the lens of behavioural economics. Section 10.5 gives suggestions to improve

empowerment of the individual, and section 10.6 to improve protection of the individual. Section 10.7 concludes.[1962]

10.1 Behavioural targeting

In a common arrangement for online advertising, advertisers only pay if somebody clicks on an ad. Click-through rates are low: in the order of 0.1 % to 0.5 %. In other words, when an ad is shown to a thousand people, on average between one and five people click on it. Behavioural targeting was developed to increase the click-through rate on ads, and involves monitoring people's online behaviour to target ads to specific individuals.

In a simplified example, behavioural targeting involves three parties: an internet user, a website publisher, and an advertising network. Advertising networks are firms that serve ads on thousands of websites, and can recognise users when they browse the web. An ad network might infer that a person who often visits websites about fishing is a fishing enthusiast. If that person visits a news website, the ad network might display advertising for fishing rods. When simultaneously visiting that same website, another person who visits a lot of websites about cooking might see ads for pans.

This study analyses the behavioural targeting process by distinguishing five phases: (1) data collection, (2) data storage, (3) data analysis, (4) data disclosure, and (5) the use of data for targeted advertising. In phase 1 firms collect information about people's online activities. People's behaviour is monitored, or tracked. Information captured for behavioural targeting can concern many online activities: what people read, which videos they watch, what they search for, etc. Individual profiles can be enriched with up-to-date location data of users of mobile devices, and other data that are gathered on and off line.

[1962] Roughly, section 10.1 summarises chapter 2. Section 10.2 summarises chapter 3 and chapter 7, section 1. Section 10.3 summarises chapter 4 to 6. Section 10.4 summarises chapter 7. Section 10.5 and 10.6 summarise chapter 8 and 9.

A commonly used technology for behavioural targeting involves cookies. A cookie is a small text file that a website publisher stores on a user's computer to recognise that device during subsequent visits. Many websites use cookies, for example to remember the contents of a virtual shopping cart (first party cookies). Ad networks can place and read cookies as well (third party cookies). As a result, an ad network can follow an internet user across all websites on which it serves ads. Third party tracking cookies are placed through virtually every popular website. A visit to one website often leads to receiving third party cookies from dozens of ad networks.

In addition to cookies, firms can use many other technologies for data collection, such as flash cookies and other "super cookies", which are usually harder to delete than conventional cookies. Other tracking methods don't rely on storing an identifier on a device. For example, passive device fingerprinting involves recognising a device by analysing the information it transmits.

In phase 2, firms store the information about individuals, usually tied to identifiers contained within cookies, or via similar technology. Some firms have profiles on hundreds of millions of people. Many behavioural targeting firms can tie a name or an email address to the data they have on individuals.

In phase 3 the data are analysed. A firm could construct a predictive model, for instance along the following lines: if a person visits website A, B, C and D, there's a 0.5 % chance the person clicks on ads for product E. For behavioural targeting to be useful, a predictive model doesn't have to be accurate when applied to an individual. If a behaviourally targeted ad has a click-through rate of 0.5 %, this is a major improvement compared to a 0.1 % click-through rate of non-targeted ads.

With behavioural targeting and other types of profiling, a predictive model based on information about a group of people can be applied to somebody who isn't part of that group. Suppose an online shop obtains the consent of thousands of people to analyse their shopping habits over time. Based on the information it collected, the shop constructs a predictive model that says that 95% of the women who buy certain

products will give birth within two months. Alice is a customer, but wasn't among the people who consented to data collection that formed the basis of the predictive model. When Alice buys certain products, the shop can infer with reasonable accuracy that she's pregnant. Hence, the shop can predict something about Alice, based on other people's information.

In phase 4, data disclosure, firms make data available to advertisers or other firms. For example, a social network site can enable advertisers to target specific persons with ads based on their behavioural profiles. Or a firm can sell copies of data to other firms. Firms can combine information from different sources to enrich profiles. Many types of firms are involved in behavioural targeting, and the resulting data flows are complicated. For example, an ad network that displays ads on a website can allow other ad networks to bid in an automated auction for the possibility to show ads to individuals. Data about individuals are auctioned off within milliseconds, and billions of such auctions take place every day. Such practices are referred to as real time bidding, or audience buying. A website publisher often doesn't know in advance who will serve ads on its website, and may not have a direct business relationship with the advertiser.

In phase 5 firms show targeted ads to specific individuals. Firms can personalise ads and other website content for each visitor. A firm might also refrain from showing an ad to certain people, based on their profiles. Behavioural targeting enables advertisers to reach a user, wherever he or she is on the web.

A website publisher can increase its income by allowing ad networks to track its visitors and to display behaviourally targeted ads. But in the long term behavioural targeting may decrease ad revenues for some website publishers. For example, an ad network doesn't have to buy expensive ad space on a large professional news website to advertise to a reader of that website. The ad network can show an ad to that person when he or she visits a random website, where advertising space is cheaper. One

marketer summarises: “advertisers are buying audiences with data, rather than using content as a proxy to reach the people they want to reach.”[1963]

10.2 Privacy and behavioural targeting

Surveys show that most people don’t want behaviourally targeted advertising, because they find it creepy or privacy-invasive. A small minority says it doesn’t mind the data collection and prefers behaviourally targeted advertising because it can lead to more relevant ads.

Privacy is notoriously difficult to define. Borrowing from Gürses, three privacy perspectives were distinguished in this study: privacy as limited access, privacy as control over personal information, and privacy as the freedom from unreasonable constraints on identity construction. The three perspectives partly overlap, and highlight different aspects of privacy.

The privacy as limited access perspective concerns a personal sphere, where people can be free from interference. The limited access perspective is similar to approaches of privacy as confidentiality, seclusion, or a right to be let alone. This perspective implies that too much access to a person interferes with privacy. For instance, if somebody wants to keep a website visit confidential, there’s a privacy interference if others learn about the visit. A second privacy perspective focuses on the control people should have over information concerning them. Seeing privacy as control is common since the 1960s, when state bodies and other large organisations started to amass increasing amounts of information about people, often using computers. The control perspective has deeply influenced data protection law. Privacy as control is interfered with, for example, if personal information is collected surreptitiously. Third, privacy can be seen as the freedom from unreasonable constraints on identity construction. The privacy as identity construction perspective largely includes the

---

[1963] Collective 2014.

other two perspectives, but also highlights other concerns regarding modern data processing practices in the digital environment, such as profiling and behavioural targeting. There could be an interference with privacy if somebody is manipulated by the environment, which can include technology.

This study focuses on three main privacy problems of behavioural targeting: chilling effects, a lack of control over personal information, and the risk of unfair social sorting and manipulation. First, chilling effects can occur because of the massive collection of information about people's online activities. People may adapt their behaviour if they know their activities are monitored. For instance, somebody who fears surveillance might hesitate to look for medical information on the web, or to read about certain political topics.

Second, people lack control over data concerning them. The reality of current behavioural targeting practices is far removed from the ideal of privacy as control. People don't know which information about them is collected, how it's used, and with whom it's shared. The feeling of lost control is a privacy problem. And large-scale personal data storage brings risks. For instance, a data breach could occur, or data could be used for unexpected purposes, such as identity fraud.

Third, behavioural targeting enables social sorting. There's a risk of unfair discriminatory practices: firms can sort people into "targets" and "waste", and treat them accordingly.[1964] And some fear that behavioural targeting could be used to manipulate people. Personalised advertising could become so effective that advertisers have an unfair advantage over consumers. There could also be a risk of "filter bubbles" or "information cocoons", especially when behavioural targeting is used to personalise not only ads, but also other content and services.[1965] Briefly stated, the idea is that personalised advertising and other content could surreptitiously steer

---

[1964] Turow 2011.
[1965] The phrases are from Pariser 2011 and Sunstein 2006.

people's choices. In sum, from each of the three privacy perspectives, behavioural targeting is problematic.

10.3 Data protection law

The right to respect for private life, the right to privacy for short, is a fundamental right in the European legal system, and is included in the European Convention on Human Rights (1950). The European Court of Human Rights interprets the Convention's privacy right generously, and refuses to define the right's scope of protection. This way, the Court can apply the right to privacy in unforeseen situations and to new developments. For instance, the Court says information derived from monitoring somebody's internet usage is protected under the right to privacy.

To protect privacy in the area of behavioural targeting, the main legal instrument in Europe is the Data Protection Directive, coupled with the e-Privacy Directive's consent requirement for tracking technologies. Data protection law is a legal tool, which aims to ensure that the processing of personal data happens fairly and transparently. Data protection law grants rights to people whose data are being processed (data subjects), and imposes obligations on parties that process personal data (data controllers, limited to and referred to as firms in this study). Since its inception in the early 1970s, data protection law has evolved into a complicated field of law. Borrowing from Bygrave, the core of data protection law can be summarised in nine principles: the fair and lawful processing principle, the transparency principle, the data subject participation and control principle, the purpose limitation principle, the data minimisation principle, the proportionality principle, the data quality principle, the security principle, and the sensitivity principle.

The right to data protection and the right to privacy aren't the same. The EU Charter of Fundamental Rights (2000) includes a right to privacy, and a separate right to the protection of personal data. This study agrees with De Hert & Gutwirth, who characterise the right to privacy as an "opacity tool", and data protection law as a

"transparency tool."[1966] The right to privacy in the European Convention on Human Rights prohibits intrusions into the private sphere. The right to privacy aims to give the individual the chance to remain shielded, or to remain opaque. This prohibition isn't absolute; privacy must often be balanced against other interests, such as the rights of others. Data protection law takes a different approach than the legal right to privacy, say De Hert & Gutwirth. In principle data protection law allows data processing, if the data controller complies with a number of requirements. Data protection law aims to ensure fairness, and one of the means to foster fairness is requiring firms to be transparent about personal data processing. Hence: a transparency tool.

In January 2012 the European Commission presented a proposal for a Data Protection Regulation, which should replace the 1995 Data Protection Directive. At the time of writing, it's unclear whether the proposal will be adopted. The most optimistic view seems to be that the Regulation could be adopted in 2015.[1967] While based on the same principles as the Directive, the proposal would bring significant changes. For instance, unlike a directive, a regulation has direct effect and doesn't have to be implemented in the national laws of the member states, so it should lead to a more harmonised regime in the EU. The proposal introduces new requirements for data controllers, such as the obligation to implement measures to ensure and demonstrate compliance. The proposal also aims to make it easier for people to delete their data from the web, and to transfer their personal data from one service provider to another. The proposal's preamble emphasises the ideal of data subject control. "Individuals should have control of their own personal data."[1968]

[1966] De Hert & Gutwirth 2006.
[1967] See European Council, 2014, p. 2.
[1968] Recital 6.

Material scope of data protection law

Whether data protection law applies to behavioural targeting is hotly debated. Data protection law only applies when "personal data" are processed: data that relate to an identifiable person. For behavioural targeting, firms often process individual but nameless profiles. Many behavioural targeting firms claim they only process "anonymous" data, and that data protection law thus doesn't apply. While the European Court of Justice, the highest authority on the interpretation of EU law, hasn't ruled on behavioural targeting yet, its case law is relevant. The discussion about nameless behavioural targeting profiles resembles the one about IP addresses. In a decision about IP addresses in the hands of an internet access provider, the Court said that those IP addresses were personal data.[1969] Furthermore, European Data Protection Authorities, cooperating in the Article 29 Working Party, say behavioural targeting generally entails personal data processing, even if a firm can't tie a name to the data it has on an individual. If a firm aims to use data to "single out" a person, or to distinguish a person within a group, these data are personal data, according to the Working Party.[1970] Although not legally binding, the Working Party's opinions are influential. National Data Protection Authorities often follow its interpretation.

The 2012 proposal for a Data Protection Regulation stirred up the debate about the material scope of data protection law. There has been much lobbying to make the proposal less burdensome for businesses. Many firms say that pseudonymous data, such as nameless behavioural targeting profiles, should be outside the scope of data protection law, or should be subject to a lighter regime. In March 2014, the European Parliament adopted a compromise text, which the Parliament's LIBE Committee prepared on the basis of the 3999 amendments by the members of parliament. This LIBE Compromise introduces a new category of personal data, pseudonymous data, and the rules are less strict for such data. Under certain conditions, the LIBE

[1969] ECJ, Sabam/Scarlet (C-70/10)
[1970] See e.g. Article 29 Working Party 2010, WP 171, p. 9.

Compromise allows firms to use behavioural targeting with pseudonymous data without the data subject's consent.

This study argues that data protection law should apply to behavioural targeting, and argues against a lighter regime for pseudonymous data. First, many risks remain, regardless of whether firms tie a name to the information they hold about a person. For instance, surveillance can cause a chilling effect, including if firms collect pseudonymous data. And a cookie-based profile that says a person is handicapped or from a poor neighbourhood could be used for unfair social sorting. Second, a name is merely one of the identifiers that can be tied to data about a person, and is not even the most practical identifier for behavioural targeting. For an ad network that wants to track somebody's browsing behaviour, or wants to target somebody with online advertising, a cookie works better than a name. Third, the behavioural targeting industry processes large amounts of information about people, and this brings risks. If data protection law didn't apply, this industry could operate largely unregulated. For these reasons, data that are used to single out a person should be considered personal data. In addition, it's often fairly easy for firms to tie a name to pseudonymous data.

Informed consent

Informed consent plays a central role in the current regulatory framework for behavioural targeting. Therefore, this study examined the role of informed consent in data protection law, and its value for regulating privacy in the area of behavioural targeting. The Data Protection Directive only allows firms to process personal data if they can base the processing on consent or on one of five other legal bases. The European Commission proposal for a Regulation duplicates the same legal bases without major revisions. For the private sector, the most relevant legal bases are: a contract, the balancing provision, and the data subject's consent.[1971]

[1971] The legal bases are listed in article 7 of the Data Protection Directive, and in article 6 of the European Commission proposal for a Data Protection Regulation.

A firm can process personal data if the processing is necessary for the performance of a contract with the data subject. For instance, certain data have to be processed for a credit card payment, or for a newspaper subscription. The "necessary" requirement sets a higher threshold than useful or profitable. Some internet companies suggest a user enters a contract by using their services, and that it's necessary for this contract to track the user for behavioural targeting. This interpretation seems incorrect. According to the Working Party, a firm can only rely on the legal basis contract if the processing is genuinely necessary for providing the service. The Working Party's view implies that, in general, firms can't rely on this legal basis for behavioural targeting. In any case, the practical problems with informed consent to behavioural targeting which are discussed below would be largely the same if firms could base the processing for behavioural targeting on a contract.

The balancing provision allows data processing when it's necessary for the firm's legitimate interests, except where such interests are overridden by the data subject's interests or fundamental rights. When weighing the interests of the firm and the data subject, all circumstances have to be taken into account, such as the sensitivity of the data and the data subject's reasonable expectations. The balancing provision is the appropriate legal basis for innocuous standard business practices. For example, a firm can generally rely on the balancing provision for postal direct marketing for its own products to current or past customers. If a firm relies on the balancing provision for direct marketing, data protection law grants the data subject the right to stop the processing: to opt out. The Data Protection Directive doesn't say explicitly whether behavioural targeting can be based on the balancing provision. But the most convincing view is that behavioural targeting can't be based on this provision, in particular when it involves tracking a person over multiple websites. In most cases the data subject's interests must prevail over the firm's interests, as behavioural targeting involves collecting and processing information about personal matters such as people's browsing behaviour. Indeed, the Working Party says firms can almost never rely on the balancing provision to process personal data for behavioural targeting.

If firms want to process personal data, and can't base the processing on the balancing provision or another legal basis, they must ask the data subject for consent. With consent, the data subject can allow data processing that would otherwise be prohibited. The Working Party says consent is generally the required legal basis for personal data processing for behavioural targeting. It follows from the Data Protection Directive's consent definition that consent requires a free, specific, informed indication of wishes. People can express their will in any form, but mere silence or inactivity isn't an expression of will. This is also the predominant view in general contract law. During the drafting of the Data Protection Directive in the early 1990s, firms have argued that opt-out systems should be sufficient to obtain "implied" consent for direct marketing. But the EU lawmaker rejected this idea.

A number of larger behavioural targeting firms offer people the chance to opt out of targeted advertising on a centralised website: youronlinechoices.com. However, participating firms merely promise to stop showing targeted ads, so they may continue to track people who have opted out. In short, the website offers the equivalent of Do Not Target, rather than Do Not Collect. But even if the firms stopped collecting data after somebody opts out, they couldn't use the website's opt-out system to obtain valid consent. Valid consent requires an expression of will, which generally calls for an opt-in procedure.

In line with the transparency principle, consent has to be specific and informed. Consent can't be valid if a consent request doesn't include a specified processing purpose and other information that's necessary to guarantee fair processing. Furthermore, consent must be "free." Negative pressure would make consent invalid, but positive pressure is generally allowed. In most circumstances, current data protection law allows firms to offer take-it-or-leave-it choices.

Hence, in principle website publishers are allowed to install "tracking walls" that deny entry to visitors that don't consent to being tracked for behavioural targeting. But a tracking wall could make consent involuntary if people must use a website. For

instance, say people are required to file their taxes online. If the tax website had a tracking wall that imposed third party tracking, people's consent to tracking wouldn't be voluntary. Similarly, if students must use a university website, a tracking wall would make consent involuntary. According to the Dutch Data Protection Authority, the national public broadcasting organisation isn't allowed to use a tracking wall, because the only way to access certain information online is through the broadcaster's website. The Working Party emphasises that consent should be free, but doesn't say that current data protection law prohibits tracking walls in all circumstances.

Since 2009, article 5(3) of the e-Privacy Directive requires any party that stores or accesses information on a user's device to obtain the user's informed consent. Article 5(3) applies regardless of whether personal data are processed, and applies to many tracking technologies such as tracking cookies. There are exceptions to the consent requirement, for example for cookies that are strictly necessary for a service requested by the user, and for cookies that are necessary for transmitting communication. Hence, no prior consent is needed for cookies that are used for a digital shopping cart, or for log-in procedures.

Recital 66 of the 2009 directive that amended the e-Privacy Directive has caused much discussion: "in accordance with the relevant provisions of [the Data Protection Directive], the user's consent to processing may be expressed by using the appropriate settings of a browser or other application."[1972] Many marketers suggest that people who don't block tracking cookies in their browser give implied consent to behavioural targeting. For instance, the Interactive Advertising Bureau UK, a trade organisation, says "default web browser settings can amount to 'consent'."[1973] But this doesn't seem plausible. As the Working Party notes, the mere fact that a person leaves his or her browser's default settings untouched doesn't mean that the person expresses his or her will to be tracked.

[1972] Directive 2009/136, recital 66.
[1973] Interactive Advertising Bureau United Kingdom 2012, p. 2..

In sum, firms are required to obtain consent for most tracking technologies that are used for behavioural targeting. Therefore, firms must usually obtain the data subject's consent for behavioural targeting, regardless of the legal basis of ensuing personal data processing. Hence, even if, under rare circumstances, a firm could rely on the balancing provision to process personal data for behavioural targeting, the firm would generally need consent for using the tracking technology. Article 5(3) isn't widely enforced yet, among other reasons because the national implementation laws are rather new. Many member states missed the 2011 implementation deadline. The approaches in the member states vary. For example, the Netherlands requires, in short, opt-in consent for tracking cookies. In contrast, the UK appears to allow firms to use opt-out systems to obtain "implied" consent. However, the Working Party insists that the data subject's inactivity doesn't signify consent.

A limited but important role for consent

While consent plays an important role in data protection law, its role is limited at the same time. Consent can provide a legal basis for personal data processing. But if a firm has a legal basis for processing, the other data protection provisions still apply. Those provisions are mandatory. The data subject can't waive the safeguards or deviate from the rules by contractual agreement. For example, the security principle requires an appropriate level of security for personal data processing. And it follows from the purpose limitation principle that personal data must be collected for specified purposes, and should not be used for incompatible purposes. Hence, a contract between a firm and a data subject wouldn't be enforceable if it stipulated that the firm doesn't have to secure the personal data, or can use the data for new purposes at will. Data protection law thus limits the data subject's contractual freedom. On the other hand, data protection law leaves some important choices to the data subject. For instance, the data subject can give or withhold consent, and has the right to stop data processing for direct marketing which is based on the balancing provision. In sum, data protection law embodies an inherent tension between protecting and empowering the data subject.

10.4 Informed consent and behavioural economics insights

For this study the choice was made to incorporate insights from other disciplines than law. 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 in practice. The analysis shows that there are reasons for more regulatory intervention. Informed consent largely fails as a privacy protection measure.

Economics

From an economic perspective, it's unclear whether behavioural targeting leads to a net benefit or a net loss for society. The benefits include profit for ad networks and other firms. And income from online advertising could be used to fund so-called "free" web services. People gain utility from using a search engine or reading an online newspaper. As an aside, it's unclear whether behavioural targeting is needed to fund "free" websites. Advertising that doesn't require monitoring people's behaviour is also possible, such as contextual advertising: ads for cars on websites about cars.

Behavioural targeting can also decrease welfare. For instance, it can be costly for people if their information ends up in the wrong hands. People could receive invasive marketing such as spam, or they could fall victim to identity fraud. Personalised ads could be used to exploit people's weaknesses or to charge people higher prices. And it's costly if people invest time in evading tracking. Furthermore, it may hamper electronic commerce if people don't trust that their personal information is adequately protected when they buy online, or when they use internet services. Other privacy related costs are harder to quantify, such as annoyance, chilling effects, and the long term effects on society. In sum, it seems unlikely that economics could offer a definitive answer to the question of whether more or less legal privacy protection would be better in the behavioural targeting area. Apart from that, the European legal system doesn't give precedence to economic arguments. Nevertheless, economics

provides a useful tool to analyse practical problems with consent to behavioural targeting.

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 are generally able to choose the best way to maximise their welfare. In economics, 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. But there may be reason for the lawmaker to intervene when the market doesn't function as it ideally should. From an economic perspective, the law should aim at reducing market failures, such as information asymmetries, externalities, and market power. However, legal intervention brings costs and economic distortions as well, which must be taken into account.

Through an economic lens, consenting to behavioural targeting can be seen as entering into a market transaction with a firm. But this "transaction" is plagued by information asymmetries. Research shows that many people don't know to what extent their behaviour is tracked, so their "choice" to disclose data in exchange for using a service can't be informed. Even 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 difficult to predict the consequences of future data usage. Information asymmetry is a form of market failure. Firms won't compete on quality if people can't assess the quality of products. This can lead to low quality products. Websites rarely compete on privacy, as illustrated by the fact that people are tracked for behavioural targeting on virtually every popular website. There seems to be a comparable situation on the market for smart phone apps.

Data protection law aims to reduce the information asymmetry by requiring firms to disclose certain information to data subjects. The law obliges firms to provide data subjects with information about their identity and the processing purpose, and all other information that's necessary to guarantee fair processing. Website publishers

can use a privacy policy to comply with data protection law's transparency requirements. These requirements also apply if a firm doesn't seek the data subject's consent, but relies on another legal basis for data processing.

However, the information asymmetry problem is hard to solve because of transaction costs for data subjects, and again, information asymmetries regarding the meaning of privacy policies. Reading privacy policies would cost too much time, as they're often long, difficult to read, and vague. It would take people several weeks per year if they read the privacy policy of every website they visit. The language in privacy policies is too difficult for many. It's thus not surprising that almost nobody reads privacy policies. In practice, data protection law thus doesn't solve the information asymmetry problem.

Externalities are another example of market failure. Economists refer to costs or damage suffered by third parties as a result of economic activity as negative externalities. Externalities occur because parties that aim to maximise their own welfare don't let costs for others influence their decisions. An example of a negative externality is environmental pollution from traffic or industry. Many legal rules, such as those in environmental law, can be seen as responses to an externalities problem. If the lawmaker wants to reduce negative externalities resulting from a contract, it generally needs to use mandatory rules. If the lawmaker used non-mandatory default rules, the contract parties would set the rules aside. After all, the externality is a result of the fact that contract parties don't take the interests of non-contract parties into account.

At first glance there are no negative externalities if somebody consents to sharing his or her data with a behavioural targeting firm. 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 can be illustrated with the example of a shop that uses a predictive model to predict the pregnancy of Alice, while the model is based on other people's data. This could be seen as an externality imposed on Alice,

which is a result of the fact that people consented to having their personal information processed.

Market power, such as a monopoly situation, is a third example of market failure. Whether a firm has too much market power depends on the specifics of a particular market. The conclusion would be different for search engines, social network 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. In any event, even in a market without market power problems, the practical problems with consent resulting from information asymmetries could persist.

Behavioural economics

Behavioural economics aims to improve the predictive power of economic theory, by including insights from psychology and behavioural studies. Behavioural economics suggests that people act structurally different than rational choice theory predicts. Because of their bounded rationality, people often rely on rules of thumb, or heuristics. Usually such mental shortcuts work fine, but they can also lead to behaviour that is not in people's self-interest. Systematic deviations from rational choice theory are called biases. Several biases influence privacy choices, such as the status quo bias and the present bias.

The status quo bias, or default bias, describes people's tendency to stick with default options. People are less likely to consent under an opt-in regime that requires an affirmative action for valid consent, than under an opt-out regime where people are assumed to consent if they don't object. In this light, the continuous opt-in/opt-out discussion about behavioural targeting and other types of direct marketing concerns the question of who benefits from the status quo bias, the firm or the data subject.

Present bias, or myopia, suggests that people often choose for immediate gratification and disregard future costs or disadvantages. For example, many find it hard to stick

with a diet, or to save money for later. If a website has a tracking wall, and people can only use the site if they agree to behavioural targeting, they're likely to consent, thereby ignoring the costs of future privacy infringements. Behavioural economics can thus help to explain 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. It's only a slight exaggeration to say: people don't read privacy policies; if they were to read, they wouldn't understand; if they understood, they wouldn't act.

In conclusion, an economic analysis doesn't dictate the ideal level of legal privacy protection. It's not straightforward whether more or less legal privacy protection in the area of behavioural targeting would be better from an economic perspective. Therefore, it remains unclear whether legal limits on behavioural targeting would be too costly for society. In any case, the lawmaker shouldn't act too bluntly. Just like environmental law doesn't aim to undo the industrial revolution (and is unlikely to do so), legal privacy protection shouldn't undo the advantages of information technology (and is unlikely to do so).

The economic analysis does show that if consenting to behavioural targeting were compared to entering into market transaction, this transaction would take place in a market plagued by market failures. There also seems to be a behavioural market failure in the behavioural targeting area. If all competitors exploit people's biases, a firm has to do the same to stay in business. In sum, insights from economics and behavioural economics suggest more regulatory intervention is needed in the area of behavioural targeting.

10.5 Improving empowerment

Considering the limited potential of informed consent as a privacy protection measure, this study argues for a combined approach of empowering and protecting the individual. The study concludes that certain practices simply shouldn't be allowed

(see below). But it doesn't seem feasible to define all beneficial or all harmful data processing activities in advance. Apart from that, the EU Charter of Fundamental Rights lists consent as a legal basis for personal data processing. Relying on informed consent, in combination with data protection law's other safeguards, will probably remain the appropriate approach in many circumstances. For those cases, transparency and consent should be taken seriously. While fostering individual control over personal information won't suffice to protect privacy in the area of behavioural targeting, some improvement must be possible, compared to the current situation of almost complete lack of control by individuals over their own data.

To improve privacy protection in the area of behavioural targeting, data protection law should be more strictly enforced, and needs amendments. The European Commission has realised that compliance with data protection law is lacking, and aims for better enforcement. For instance, under the proposal for a Data Protection Regulation, Data Protection Authorities could impose high penalties, and organisations could take a firm to court on behalf of data subjects if the firm breaches data protection law. An important avenue for further research is how compliance with the rules could be improved. One option that should be examined is the introduction of collective action procedures that enable groups of people to sue a firm if it breaches privacy or data protection rights. Another topic for further research is enforcement of European data protection law against firms that are based outside Europe, a topic that was outside this study's scope.

How could the law improve *empowerment* of the individual? To reduce the information asymmetry in the area of behavioural targeting, the transparency principle should be enforced. In line with European consumer law, the lawmaker should require firms to phrase privacy policies and consent requests in a clear and comprehensible manner. The European Commission proposal for a Data Protection Regulation requires firms to have easily accessible privacy policies "in an intelligible form, using

clear and plain language."[1974] Codifying the clear language requirement could discourage firms from using legalese in privacy policies. And the requirement would make it easier for Data Protection Authorities to intervene when a firm uses a privacy policy or a consent request that is too vague. The rule wouldn't be enough to ensure actual transparency, but it could help to lower the costs of reading privacy policies. Also, interdisciplinary research is needed to develop tools to make data processing transparent in a meaningful way.

Regarding consent, the existing rules should be enforced. Requiring informed consent for tracking wouldn't guarantee transparency, but at least a consent request would alert people to the tracking, unlike an opt-out system. And because of the default bias, requiring opt-in consent for tracking could nudge people towards disclosing fewer data. The European Commission proposal reaffirms that consent must be expressed "either by a statement or by a clear affirmative action."[1975] The proposal also codifies the Working Party's view that a consent request may not be hidden in a privacy policy or in terms and conditions.

Human attention is scarce and too many consent requests can overwhelm people. Therefore, the scope of article 5(3) of the e-Privacy Directive is too broad. Article 5(3) requires consent for storing or accessing information on a user's device. This means consent is also required for some cookies that pose few privacy risks and that aren't used to collect detailed information about individuals, such as certain types of cookies that are used for website analytics. But there's little reason to seek consent for truly innocuous practices. The Data Protection Directive contains the balancing provision for such innocuous practices.

It would probably be better if the lawmaker phrased the consent requirement for tracking in a more technology neutral way. The law could require consent for the collection and further processing of personal data, including pseudonymous data, for

---

[1974] Article 11 of the European Commission proposal for a Data Protection Regulation (2012).
[1975] Article 4(8) of the European Commission proposal for a Data Protection Regulation (2012).

behavioural targeting and similar purposes – regardless of the technology that's used. Phrasing the rule in a more technology neutral way could also mitigate another problem. In some ways the scope of article 5(3) is too narrow. For instance, it's unclear to what extent article 5(3) applies if firms use device fingerprinting for behavioural targeting.

A user-friendly system should be developed to make it easier for people to give or refuse consent. Work is being done in this area, among others by the World Wide Web Consortium, an organisation that works on the standardisation of web technologies. The Consortium's Tracking Protection Working Group (DNT Group) is trying to develop a Do Not Track standard, which should enable people to signal with their browser that they don't want to be tracked. This way, people could opt out of tracking with a few mouse clicks. The system could thus lower the transaction costs of opting out of data collection by hundreds of firms.

It's not immediately apparent how Do Not Track – an opt-out system – could help firms to comply with the e-Privacy Directive's consent requirement for tracking technologies. But an arrangement along the following lines could be envisaged. Firms should refrain from tracking European internet users that haven't set a Do Not Track preference. If somebody signals to a firm "Yes, you can track me" after receiving sufficient information, that company may track that user. Hence, in Europe not setting a preference would have the same legal effect as setting a preference for "Do not track me." In Europe, Do Not Track would thus be a system to opt in to tracking.

At the time of writing, after almost three years of discussion, the DNT Group still hasn't reached consensus in relation to some major issues. The most contentious topic is what firms should do when they receive a "Do not track me" signal. Many firms that participate in the DNT Group want to continue to collect data from people who signal they don't want to be tracked. In brief, the firms want to offer Do Not Target, rather than Do Not Collect. Some firms even want to continue targeting ads to people who signal "Do not track me." The firms offer to delete people's browsing history,

while retaining the inferred interest categories tied to people's profiles. There's no agreement in the DNT Group about which data uses should still be allowed when people signal "Do not track me."

From the start, the DNT Group agreed that the Do Not Track standard should allow a website to ask somebody who signals "Do not track me" for an exception, roughly as follows. "We see your Do Not Track signal. But do you make an exception for me and my ad network partners so we can track you?" As noted, data protection law allows take-it-or-leave-it choices in many circumstances. Hence, if a Do Not Track standard were developed that complied with European law, many websites would probably respond by installing tracking walls. Therefore, even if firms provided clear information, even if people understood the information, and even if firms asked for prior consent, many people might still feel that they're forced to consent to behavioural targeting. Even if Do Not Track emerges as a W3C standard, it seems unlikely that without additional legislative support it will solve the privacy problems posed by behavioural targeting.

To conclude, a lack of individual control over personal information aptly describes many privacy problems. But this doesn't mean that aiming for data subject control is the best regulatory tactic. Enforcing and tightening the data protection principles could improve data subject control. However, aiming for individual empowerment alone won't suffice in protecting privacy in the area of behavioural targeting.

10.6 Improving protection

A second legal approach to improve privacy protection in the area of behavioural targeting involves *protecting,* rather than empowering, people. If fully complied with, the data protection principles could give reasonable privacy protection in the behavioural targeting area, even if people agreed to consent requests. But additional regulation is needed as well.

The study offers suggestions on how the law could improve privacy protection, without being unduly prescriptive. In this study, rules are considered unduly prescriptive if they impose unreasonable costs on society, or if they're unduly paternalistic. As noted, from an economic perspective it's unclear whether more or less legal privacy protection in the area of behavioural targeting would be better. Therefore, stricter rules wouldn't necessarily be too costly for society. Additionally, the existence of market failures in the area of behavioural targeting suggests a need for regulatory intervention.

A greater focus on protecting the data subject wouldn't make the law unduly paternalistic either. Paternalism involves limiting a person's contractual freedom, predominantly to protect that person. The law in Europe accepts a degree of paternalism, and this study agrees with that approach. Many rules, such as consumer protection rules and minimum safety standards for products, could plausibly be explained, at least in part, by paternalistic motives, although such rules could also be seen as a response to market failures.

Pure paternalism is only present when a legal rule only aims at protecting somebody against him- or herself. But there are other rationales for legal privacy protection than protecting people against themselves. The right to privacy and the right to data protection aim to contribute to a fair society, which goes beyond individual interests. And responding to market failures has nothing to do with paternalism. Moreover, behavioural economics insights suggest that more protective rules are needed. After all, the European Court of Human Rights requires privacy protection that's "practical and effective, not theoretical and illusory."[1976]

The data minimisation principle, if effectively enforced, is an example of a data protection principle that could protect people's privacy, even after people consent to behavioural targeting. The vast scale of data processing for behavioural targeting

---

[1976] ECtHR, Christine Goodwin v. the United Kingdom, No. 28957/95, July 11, 2002, par 74.

aggravates the chilling effects, and the lack of individual control over personal information. And large-scale data storage brings risks, such as data breaches. Compliance with the data minimisation principle could mitigate such privacy problems. Furthermore, setting limits to data collection would reduce the amount of information that's available to construct predictive models. The Data Protection Directive states that data processing must be "not excessive" in relation to the processing purpose.[1977] It follows from the Directive's structure that this requirement also applies if the processing is based on the data subject's consent. The data minimisation principle should be phrased more clearly, which the European Commission proposal for a Data Protection Regulation does. "Personal data must be (…) limited to the minimum necessary in relation to the purposes for which they are processed."[1978] The lawmaker should explicitly codify that the data subject's consent doesn't legitimise disproportionate data processing. Such a rule could remind firms that consent doesn't give them carte blanche to collect personal information at will, and that a Data Protection Authority could intervene if they did.

The transparency principle can be interpreted as a prohibition of surreptitious data processing. With some behavioural targeting practices, it would be difficult for a website publisher to comply with data protection law's transparency requirements, even if it tried its best. For example, some ad networks allow other ad networks to buy access to individuals by bidding on an automated auction. In such situations, the website publisher doesn't know in advance who will display ads on its site, and who will track its website visitors. Therefore, it's hard to see how the publisher could comply with the law's transparency requirements. If a publisher can't give data subjects the information that's required by the Data Protection Directive, the processing isn't allowed – and shouldn't be allowed. The lawmaker should make it more explicit that processing is prohibited, unless firms can comply with the transparency principle.

[1977] Article 6(1)(c) of the Data Protection Directive.
[1978] Article 5(c) of the European Commission proposal for a Data Protection Regulation (2012).

Data protection law has a stricter regime for "special categories of data", such as data revealing race, political opinions, health, or sex life.[1979] Using special categories of data for behavioural targeting and other types of direct marketing is only allowed after the data subject's explicit consent is obtained, and in some member states prohibited. Strictly enforcing the existing rules on special categories of data could reduce privacy problems such as chilling effects. For instance, people might be hesitant to look for medical information on the web if they fear leaking information about their medical conditions. Because the privacy risks involved in using health data for behavioural targeting outweigh the possible societal benefits from allowing such practices, the EU lawmaker should consider prohibiting the use of any health related data for behavioural targeting, whether the data subject gives explicit consent or not. The rules on special categories of data could be interpreted in such a way that the collection context is taken into account. For example, tracking people's visits to websites with medical information should arguably be seen as processing "special categories of data", as the firm could infer data regarding health from such tracking information.

For providers of publicly available electronic communications services, such as internet access providers or phone operators, the e-Privacy Directive contains stricter rules for certain data types. For example, such providers may only process location data and traffic data with consent, unless a specified exception applies. But many firms, such as ad networks and providers of smart phone apps, process more data of a more sensitive nature than providers of publicly available electronic communications services. This asymmetric situation calls for reconsideration.

An option that should be explored is whether a separate legal instrument is needed to protect privacy in the behavioural targeting area. The current sector-specific rules in the e-Privacy Directive have major shortcomings. With a separate legal instrument for privacy protection in the area of behavioural targeting, the lawmaker could adopt appropriate rules for behavioural targeting, without imposing unnecessary burdens on

---

[1979] Article 8 of the Data Protection Directive.

other sectors. These specific rules could address the different behavioural targeting phases: (1) data collection, (2) data storage, (3) data analysis, (4) data disclosure, and (5) the use of data for targeted advertising. But specific rules could also be included in other legal instruments. For instance, rules regarding tracking and public service media could be included in media law. Other rules could be included in consumer law.

What should the lawmaker do about take-it-or-leave-it choices such as tracking walls? The law could prohibit take-it-or-leave-it choices in certain circumstances or contexts. For instance, public service broadcasters often receive public funding, and they have a special role in informing people. But if people fear surveillance, they might forego using public service media. Therefore, the lawmaker should prohibit public service broadcasters from installing tracking walls on their websites. The lawmaker could also go one step further, and prohibit all third party tracking for behavioural targeting on public service media.

More generally it's questionable whether it's appropriate for websites of state bodies to allow third party tracking for behavioural targeting – even when people consent. It's not evident why the public sector should facilitate tracking people's behaviour for commercial purposes. Therefore, the lawmaker should consider prohibiting all tracking for behavioural targeting on public sector websites.

The Data Protection Directive's provision on automated decisions could protect people against certain forms of unfair social sorting and discrimination. The provision says that a person may not be subjected to certain fully automated decisions that "significantly affect" him or her.[1980] But there are exceptions. For example, the law allows a firm to automatically refuse to enter into a contract with an individual, if there are safeguards in place for that person, which may include a possibility to ask for human intervention. By way of illustration, an insurance company that lets

---

[1980] Article 15 of the Data Protection Directive.

software automatically deny a website visitor an insurance contract could ensure that the person can ask a human to reconsider the decision. But for behavioural targeting the relevance of the automated decisions provision seems limited, as it's unclear whether one targeted ad qualifies as an automated decision that "significantly affects" somebody in the sense of the provision. However, in aggregate, behavioural targeting may well significantly affect a person. Indeed, the very point of advertising is to change views, attitudes, actions, and behaviours over time.

The successor of the automated decisions provision in the European Commission proposal is entitled "measures based on profiling."[1981] The provision introduces a new transparency requirement, which obliges a firm to tell the person concerned that a profiling measure with significant effect is taken, and to inform the person about the measure's envisaged effects. The provision should be amended. First, to improve transparency, firms should inform people about profiling measures and their underlying logic, even if no significant effects of the measure are foreseen. Also, interdisciplinary research is needed to develop tools to provide people with meaningful transparency regarding data processing and profiling. Second, profiling measures that have the effect of discriminating on the basis of special categories of data, intentional or not, should be prohibited, as proposed by the European Parliament. Such a prohibition would also apply if a firm used non-special data as a proxy for special categories of data.

10.7 Conclusion

In summary, the law could improve privacy protection in the area of behavioural targeting, by combining the empowerment and the protection approach, along with better enforcement of the existing rules. Collecting and storing fewer data, and not collecting data without meaningful consent, could reduce chilling effects. But the most effective way of preventing chilling effects is by not collecting data. Therefore,

---

[1981] Article 20 of the European Commission proposal for a Data Protection Regulation (2012).

data collection for behavioural targeting may have to be further restricted or banned in certain contexts.

To improve individual control over personal information, strictly enforcing the data protection principles would be a good start. Covert data collection is a problem from the normative perspective of privacy as control. But if behavioural targeting happens surreptitiously, this usually implies a breach of existing laws as well. The study provides suggestions on how to apply and enforce the data protection principles.

To mitigate the risk of unfair social sorting, data protection law can help as well. As long as the data aren't applied to an individual (phase 5), the sorting doesn't happen. But analysing vast amounts of data (phase 3) is a crucial step. Hence, limiting the amount of data that is available could mitigate the risks. Requiring firms to be transparent about personalisation could also mitigate the risk of manipulation. And the data protection principles can be interpreted as generally requiring firms to offer an option to opt out of personalisation. Furthermore, the legal transparency requirements can help to make data processing controllable for policymakers, as transparency can help to uncover problems that might call for regulatory intervention.

In sum, enforcing and tightening the data protection principles could help to protect privacy in the area of behavioural targeting. But this may not be enough. If society is better off if certain behavioural targeting practices don't take place, the lawmaker should consider banning them. The study shows that there are no reasons *never* to use prohibitions in the area of behavioural targeting. But it would be difficult to define prohibitions in such a way that they're not over or under inclusive. Here lies a challenge for further research. Hard questions are ahead for researchers and policymakers. The legal protection of privacy will remain a learning process. If new rules were adopted, their practical effect would have to be evaluated. The problems with the current informed consent requirements demonstrate that regulation that looks good on paper may not effectively protect privacy in practice. The way the online marketing industry evolves also has implications for the best regulatory approach. If

in ten years a couple of firms are responsible for all the behavioural targeting in the world, this calls for different regulatory answers than if thousands of firms engage in behavioural targeting.

Behavioural targeting illustrates the difficulties that privacy protection faces in the twenty-first century. Gradually more objects are being connected to the internet. Transparency and individual control over personal data are difficult to achieve when people use computers and smart phones, but will be even harder to achieve when objects without a screen are used to collect data.

In conclusion, there's no silver bullet to improve privacy protection in the area of behavioural targeting. While current regulation emphasises empowerment, without much reflection on practical issues, this study argues for a combined approach of protecting and empowering people. To improve privacy protection, the data protection principles should be more strictly enforced. But the limited potential of informed consent as a privacy protection measure should be taken into account. Therefore, the lawmaker should give more attention to rules that protect, rather than empower, people.

* * *