



## UvA-DARE (Digital Academic Repository)

### Improving privacy protection in the area of behavioural targeting

Zuiderveen Borgesius, F.J.

**Publication date**

2014

**Document Version**

Final published version

[Link to publication](#)

**Citation for published version (APA):**

Zuiderveen Borgesius, F. J. (2014). *Improving privacy protection in the area of behavioural targeting*.

**General rights**

It is not permitted to download or to forward/distribute the text or part of it without the consent of the author(s) and/or copyright holder(s), other than for strictly personal, individual use, unless the work is under an open content license (like Creative Commons).

**Disclaimer/Complaints regulations**

If you believe that digital publication of certain material infringes any of your rights or (privacy) interests, please let the Library know, stating your reasons. In case of a legitimate complaint, the Library will make the material inaccessible and/or remove it from the website. Please Ask the Library: <https://uba.uva.nl/en/contact>, or a letter to: Library of the University of Amsterdam, Secretariat, Singel 425, 1012 WP Amsterdam, The Netherlands. You will be contacted as soon as possible.

## 1 Introduction

Behavioural targeting involves the monitoring of people's online behaviour. It uses the collected information to show people individually targeted advertisements. To give a simplified example, a person who frequently visits websites about cars and soccer might be profiled as a male sports enthusiast. If that same person books a flight to Amsterdam on a website, advertising for tickets for a game of the local football club, Ajax, may be shown.

Behavioural targeting could benefit firms and individuals. Advertising funds an astonishing amount of internet services. Without paying with money, people can use online translation tools, access online newspapers, use email accounts, watch videos, and listen to music. Many people prefer targeted ads to random ads, and appreciate the book recommendations by online bookstores based on earlier interactions with the store. But behavioural targeting also raises privacy concerns. For instance, data collection can cause chilling effects. Using cookies or other technologies, firms compile detailed profiles based on what internet users read, what videos they watch, what they search for, etc. 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. People have little control in relation to what happens to information concerning them. Many different types of firms are involved in behavioural targeting, which results in a complicated system where information about people is combined, analysed, and auctioned off in almost real time. Furthermore, behavioural targeting enables discriminatory practices. A firm can exclude people from its advertising campaign, based on their individual profiles. Ads and websites can be personalised for each visitor.

This study examines ways in which the law could improve privacy protection in this area. Broadly speaking, this study explores two primary ways in which privacy can be defended. The first focuses on *empowering* the individual, for example by requiring firms to obtain the individual's consent before they collect data. This empowerment approach is present in current data protection law. Under the data protection regime, personal data “must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law.”<sup>1</sup> The phrase “on the basis of the consent of the person concerned” appears to be a strong requirement, but is undermined in practice, due to the fact that many people click “I agree” to any statement that is shown on the web. Behavioural studies cast doubt on the potential of informed consent as a means to defend privacy.

The second approach focuses on *protecting* rather than empowering the individual. This approach is also present in data protection law. Many data protection rules can protect privacy in the area of behavioural targeting, even if people agree to consent requests. For instance, firms must always secure the data they process, and can't use data for new purposes at will. Such requirements should mitigate the chance that personal information may be used in unexpected ways that harm people. But the data protection regime should be supplemented with additional rules. The study concludes with recommendations on how to improve privacy protection.

## 1.1 Research question

This study aims to answer to following question.

How could European law improve privacy protection in the area of behavioural targeting, without being unduly prescriptive?

---

<sup>1</sup> Article 8 of the EU Charter of Fundamental Rights. See for the full titles of the legal texts: Legal texts, at the end of this study.

Some remarks about the research question and the terminology. In this study, behavioural targeting is analysed 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.

The study focuses in particular on three privacy problems regarding behavioural targeting: chilling effects, the lack of individual control over personal information, and the risk of discriminatory or manipulative practices.<sup>2</sup> Privacy is notoriously difficult to define. Three privacy perspectives are distinguished in this study, as discussed in the next section.

The phrase European law as used in the research question, refers to regulation by the European Union. The study also takes the norms into account that follow from the European Convention on Human Rights and the related case law.<sup>3</sup> To protect privacy in the area of behavioural targeting, the EU lawmaker mainly relies on the e-Privacy Directive,<sup>4</sup> and the Data Protection Directive.<sup>5</sup> The e-Privacy Directive requires firms to ask the user's consent for using tracking cookies and similar technologies.

Data protection law can be seen as a means, a legal instrument, to protect privacy, fairness, and related interests. This study agrees with De Hert & Gutwirth, who characterise the legal right to privacy as an “opacity tool”, and data protection law as a “transparency tool.”<sup>6</sup> They say that the right to privacy in the European Convention on Human Rights prohibits intrusions into the private sphere.<sup>7</sup> This right aims to give the individual the chance to remain shielded, or to remain opaque. This prohibition isn't absolute. Exceptions to the prohibition are possible under strictly defined

---

<sup>2</sup> This study uses the phrases “data” and “information” interchangeably, and uses “risk” and “uncertainty” interchangeably.

<sup>3</sup> The norms that follow from the European Convention on Human Rights and the related case law form an integral part of the general principles of law for the EU (see e.g. CJEU, C-131/12, Google Spain, 13 May 2014, par. 68).

<sup>4</sup> Directive 2002/58/EC (amended by Directive 2009/136/EC). This study uses the consolidated text.

<sup>5</sup> Directive 95/46/EC.

<sup>6</sup> De Hert & Gutwirth 2006.

<sup>7</sup> Article 8(1) of the European Convention on Human rights.

conditions, for instance for national security, or for the protection of the rights of others.<sup>8</sup>

Data protection law takes a different approach than the legal right to privacy. 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 by requiring firms to be transparent about personal data processing. It's a legal tool that aims to ensure that the processing of personal data happens fairly and transparently.<sup>9</sup>

In January 2012 the European Commission presented a proposal for a Data Protection Regulation,<sup>10</sup> which should replace the Data Protection Directive from 1995. 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.<sup>11</sup> The proposed Regulation is based on the same principles as the Directive.

The study looks for regulatory responses to protect privacy, “without being unduly prescriptive.” The lawmaker shouldn't take measures that are excessive or unreasonable. For this study, the “without being unduly prescriptive” requirement implies that the lawmaker must respect certain boundaries. First, in line with positive law, the study assumes that some legal paternalism is acceptable, but that the lawmaker should stay away from boundless paternalism. Second, regulation shouldn't impose unreasonable costs on society. The use of the word unduly illustrates that law isn't an exact science.

## 1.2 Methodology

This is a legal study, which is situated in the field of information law. Information law is “the law relating to the production, marketing, distribution and use of information

---

<sup>8</sup> Article 8(2) of the European Convention on Human rights.

<sup>9</sup> See in more detail on De Hert & Gutwirth 2006, opacity tools and transparency tools: chapter 4, section 3, and chapter 9, section 2.

<sup>10</sup> European Commission proposal for a Data Protection Regulation (2012).

<sup>11</sup> See: European Council 2014, p. 2.

goods and services. Information law comprises a wide set of legal issues at the crossroads of intellectual property, media law, telecommunications law, freedom of expression and right to privacy.”<sup>12</sup> More specifically, this is a study in the field of data protection law, as Europeans might say, or information privacy law, as Americans might say.<sup>13</sup>

The study contains normative and descriptive research. The research question is normative, and concerns what the law ought to be, rather than what the law is. One of the goals of European data protection law is to “protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.”<sup>14</sup> This study agrees with the argument that data protection law doesn’t achieve this goal in the area of behavioural targeting.<sup>15</sup> Parts of this study take a primarily descriptive approach, and provide an analysis of current law.<sup>16</sup>

The study considers different options, and maps out strengths and weaknesses of different regulatory strategies. According to Rubin, “[c]ontemporary legal scholars are now generally aware that their work consists of recommendations addressed to legal decision-makers, recommendations that are ultimately derived from value judgments rather than objective truth.”<sup>17</sup> Whether or not this is true for legal scholars in general, this study proceeds on that basis.<sup>18</sup> Answering the research question necessarily entails making “legal-political choices.”<sup>19</sup>

---

<sup>12</sup> Institute for Information Law 2013.

<sup>13</sup> Information privacy “concerns the collection, use and disclosure of personal information” (Schwartz & Solove 2009, p. 1). Chapter 5 shows that the concept of “personal information” raises questions in the area of behavioural targeting.

<sup>14</sup> Article 1(1) of the Data Protection Directive.

<sup>15</sup> See the references in chapter 8, section 1. See for an evaluation of the current regime also chapter 7.

<sup>16</sup> See for instance, chapter 3, section 2, and chapter 4, 5 and 6. See on the merits of descriptive legal research Posner 2007, p. 437.

<sup>17</sup> Rubin 1988, p. 1904.

<sup>18</sup> See for criticism on such “policy-driven research” Van Gestel & Micklitz 2013, p. 10.

<sup>19</sup> The phrase is borrowed from Vranken 2006, p. 123. See also Hesslink 2009.

There's no commonly agreed upon privacy definition. The European Court of Human Rights says that the right to private life, the right to privacy for short, is "a broad term not susceptible to exhaustive definition."<sup>20</sup> Borrowing from Gürses, this study distinguishes three privacy perspectives in order to bring some structure to the discussion.<sup>21</sup> The first perspective focuses on limited access to the private sphere. The second focuses on individual control over personal information. The third perspective focuses on privacy as the freedom from unreasonable constraints on identity construction. The three perspectives highlight different privacy aspects of behavioural targeting.

In order to analyse the appropriate regulatory response to behavioural targeting, the study focuses in particular on three privacy problems. First, the massive collection of information on user behaviour can cause chilling effects. People may adapt their behaviour if they suspect their behaviour is monitored. For instance, they might hesitate to look for medical information, or to read about certain political topics on the web. Second, people lack control over data concerning them. The online behaviour of hundreds of millions of people is tracked, without their knowledge or consent. The data flows behind behavioural targeting are complicated, and people have scant knowledge of what happens to their data. Third, there's a risk of unfair social sorting or discriminatory practices. And some fear behaviourally targeting could be used to manipulate people. Firms can personalise ads and other website content to each individual visitor, and personalised ads could be used to exploit people's weaknesses. In sum, this study takes a broad view of privacy related problems.<sup>22</sup>

Legal scholars often use several methods in one study to answer a research question.<sup>23</sup> This research follows that tradition. For example, this study draws inspiration from the field of consumer law and general contract law. In these fields, certain problems

---

<sup>20</sup> ECtHR, *S. and Marper v. The United Kingdom*, No. 30562/04 and 30566/04.

<sup>21</sup> Gürses 2010. The three perspective are based on Warren & Brandeis 1890; Westin 1970; Agre 1998. See chapter 3, section 1.

<sup>22</sup> See chapter 3, and especially section 3.

<sup>23</sup> Herweijer 2003.

are comparable to those in data protection law: how should the balance be struck between empowering and protecting people? Taking inspiration from other areas of law could be seen as an internal comparative law method.<sup>24</sup>

Research from other disciplines provides valuable insights for this study. The study draws on law and economics and behavioural economics research. Law and economics provides a tool to analyse certain problems with informed consent to behavioural targeting.<sup>25</sup> Behavioural economics aims to improve economic theory by including findings from psychology and behavioural studies. Empirical research by scholars such as Acquisti, Cranor and McDonald provides information on how people make privacy choices in practice.<sup>26</sup> On paper, current data protection law looks better than it operates in practice. Salter & Mason might characterise the approach of this study as follows:

Such research, from the start, expressly advocates a reform in law. (...) Such proposals will (...) be supported by evidence that changes in social patterns, lifestyles, attitudes and economic circumstances now mean that the policy underlying a particular area of legal regulation has become outdated and anachronistic, even if it fully meets the aspirations of the black-letter model.<sup>27</sup>

It's emphasised that this is legal research. The study primarily takes an internal legal viewpoint, rather than an external viewpoint, which would be the case in legal sociology, or in law and economics.<sup>28</sup> Arguments have to fit in the European legal

---

<sup>24</sup> Vranken 2006, 88; Herweijer 2003.

<sup>25</sup> Law and economics can be described as the “economic analysis of legal rules and institutions” (Posner 2011, xxi). See chapter 7, section 2 for an introduction to the field.

<sup>26</sup> See chapter 7.

<sup>27</sup> Salter & Mason 2007, p. 162-163.

<sup>28</sup> See Hart 1961.

system.<sup>29</sup> For example, law and economics can help to analyse problems, but in the European legal system economic arguments don't trump other arguments.<sup>30</sup> The economic analysis is meant as an addition to legal discourse, and doesn't aim to improve economic theory. Chapter 2, which describes the facts regarding behavioural targeting, uses literature from the fields of marketing, computer science, and media studies. In summary, this is legal research with a small degree of interdisciplinarity.<sup>31</sup>

Some methods that are common in legal research are absent or less prominent in this study. For example, the systemisation and analysis of case law plays a minor role in this study, because case law on behavioural targeting is scarce.<sup>32</sup> External comparative law, the comparison of national legal systems, doesn't play a role in this study. While a comparison of the regulation of behavioural targeting in the United States and in Europe would be an interesting research topic, this study doesn't adopt that approach, in order to keep the scope of the study manageable. That said, the study does take inspiration from American scholars.<sup>33</sup>

This study relies on desk research, and uses several types of sources, such as the usual sources for legal research: regulation, case law, legislative history and legal literature. Research libraries and the usual databases were used to find literature. The study mainly refers to sources in English. If there was a choice between a source in English and a source in another language, usually the English source was chosen. Literature tips were asked from specialists in the various disciplines and fields of law that are present in this study. For this study, in addition to his education in information law,

---

<sup>29</sup> Hesselink 2009, p. 39; Smits 2009, p. 54.

<sup>30</sup> See chapter 7, section 2.

<sup>31</sup> See Schrama 2011, p. 161, Smits 2009, p. 51-54. In the taxonomy of Siems, this study might be called "basic interdisciplinary research" (Siems 2009).

<sup>32</sup> The analysis of case law does play a role, especially in chapter 3, section 2, and chapter 6. Furthermore, the study refers to opinions of Data Protection Authorities, in a way that resembles how many studies refer to case law.

<sup>33</sup> See for a comparison between European and US privacy regulation Blok 2002 (Dutch and US law); Hoofnagle 2010; Purtova 2011 (focusing on property rights on personal data); Tene & Polenetsky 2012 (focusing on behavioural targeting). See also Korff, D. et al. 2010, comparing eleven countries.

the author did coursework in behavioural economics, and in law and economics.<sup>34</sup> During the research, preliminary results were discussed with academics from various disciplines from many countries. Conversations with firms doing behavioural targeting, regulators, and lawyers also provided valuable insights. Any errors in the study are mine.

This study aims to be reasonably pragmatic, and relevant for policy discussions. The study doesn't examine whether data protection law should be completely abolished, so the lawmaker can start again with a clean slate to develop a new privacy regime. This would be an interesting thought experiment, but it's unlikely that the EU would abolish data protection law.<sup>35</sup> More generally, the European legal system is accepted as the background for this study. The study doesn't consider solutions that would require completely reforming the legal and political system, or resigning from the European Convention on Human Rights.

The choice to take a European perspective for this study, as opposed to a Dutch perspective for instance, is also largely pragmatic. If a EU member state would adopt regulation regarding behavioural targeting, it would likely be less effective than if the EU did so. The author is aware that the choice of a European perspective is also a political choice. Another political choice is this study's implicit assumption that the harmonisation of European laws is desirable. In data protection scholarship it's relatively common to assume that harmonisation is desirable, as many legal data protection instruments aim at both protecting fundamental rights and protecting the free cross border flow of personal data.<sup>36</sup> The European (rather than national) focus influences this study's style. For instance, the study gives a relatively large amount of

---

<sup>34</sup> At the University of Amsterdam I followed the courses "Behavioural Economics" by Prof. J. Sonnemans, and "Law and Economics" by Prof. Dari-Mattiacci. At New York University I followed the courses "Economic Analysis of Law" by Prof. L.A. Kornhauser, "Comparative Law and Economics of Contracts", by Prof. F.L. Gomez, and "Consumer Contracts" (behavioural law and economics) by Prof. O. Bar-Gill and Prof. F. Marotta-Wurgler.

<sup>35</sup> This is unlikely for many reasons. One reason is that the EU Charter of Fundamental Rights includes a right to the protection of personal data in article 8.

<sup>36</sup> See González Fuster 2014, p. 130.

attention to the opinions of the Article 29 Working Party, an advisory body in which national Data Protection Authorities cooperate.<sup>37</sup> While not legally binding, the Working Party's opinions are influential. They give an idea of the views of European national Data Protection Authorities.

The topic of this thesis is a moving target, in various ways. For example, firms develop new tracking technologies all the time. The legal landscape is also subject to change. While the thesis was in progress, proposals to amend European data protection law were presented by the European Commission and discussed and amended in Brussels. The research was concluded on 1 November 2014. Developments after that date aren't taken into account, with a few minor exceptions. Parts of the thesis build on and include parts of the earlier work of the author.<sup>38</sup>

### **1.3 Societal and scientific relevance**

Research shows that many people worry about their online privacy, and that many find behavioural targeting to be a privacy invasion.<sup>39</sup> Vast amounts of information about hundreds of millions of people is collected for behavioural targeting. European regulation of cookies and proposals to amend European data protection law have been the topic of much policy discussion. There's a constant stream of articles in the academic and popular press on behavioural targeting. The idea that privacy protection in the area of behavioural targeting leaves something to be desired is widely shared in literature.<sup>40</sup>

No national regulator has come up with a definitive answer in relation to how to regulate behavioural targeting, a practice that started in the mid-1990s, and grew into a major business during the last decade. Everywhere in the world, behavioural

---

<sup>37</sup> Article 29 of the Data Protection Directive. See for more details on the Working Party: chapter 4, introduction.

<sup>38</sup> See in particular Van Der Sloot & Zuiderveen Borgesius 2012; Zuiderveen Borgesius 2011; Zuiderveen Borgesius 2013; Zuiderveen Borgesius 2013a; Zuiderveen Borgesius 2014.

<sup>39</sup> See for research on people's attitudes regarding behavioural targeting chapter 7, section 1.

<sup>40</sup> See chapter 7, chapter 8, section 1, chapter 9, section 1.

targeting is a relatively new phenomenon. As scholars and regulators worldwide are struggling to come up with answers, this study might be relevant outside Europe as well. Roughly a hundred countries have laws that are based on the same principles as European data protection law.<sup>41</sup> Hence, certain problems, for instance regarding consent in the online environment, also arise outside Europe.

What does this study add to existing scholarship? This study is among the first to discuss the implications of behavioural economics research for European data protection policy.<sup>42</sup> The topic of whether data protection law should apply to pseudonymous data is discussed in depth in the study. The study contains a detailed analysis of the role of informed consent in data protection law. And the study gives much attention to the tension between protecting and empowering the individual within data protection law.

Legal scholars have discussed online privacy problems since the 1990s. In recent years, many authors have expressed scepticism about the potential of informed consent as a privacy protection measure.<sup>43</sup> The complicated data flows behind behavioural targeting make transparency and informed choices especially difficult.<sup>44</sup> Kosta analysed consent in European data protection law, using mainly legal-historical analysis and external comparative law.<sup>45</sup> This study could be seen as a next step after her thesis.

De Hert & Gutwirth characterisation of data protection law as a legal “transparency tool” influences this study.<sup>46</sup> The choice of the three privacy perspectives in this study

---

<sup>41</sup> In September 2013, Greenleaf counted 101 countries in the world with a data protection law (Greenleaf 2013a, Greenleaf 2013b).

<sup>42</sup> Other studies that take behavioural economics insights into account when discussing European data protection law include Brown 2011; Brown 2013; Helberger et al. 2012.

<sup>43</sup> See e.g. Bygrave & Schartum 2009; Blume 2012. See also the references in chapter 7, section 3 and 4.

<sup>44</sup> See e.g. Helberger et al. 2012; Kosta 2013a. See further chapter 7. US scholars are often even more pessimistic about “informed consent” as a privacy protection tool; see e.g. Barocas & Nissenbaum 2009; Nissenbaum 2011; Tene & Polenetsky 2012; Solove 2013.

<sup>45</sup> Kosta 2013a.

<sup>46</sup> De Hert & Gutwirth 2006.

is deeply influenced by the work of Gürses.<sup>47</sup> Surveillance scholars such as Gandy and Lyon inform the discussion on social sorting and discrimination.<sup>48</sup> Scholars such as Hildebrandt et al., Solove, and Zarsky distinguish different phases of personal data processing.<sup>49</sup> The analysis of behavioural targeting in this study builds on their work. The work by media scholars, such as Turow and Bermejo, provides information for this study's discussion of the behavioural targeting practice.<sup>50</sup> Computer science researchers such as Krishnamurthy, Mayer, Soltani, and Van Eijk provide insights into behavioural targeting practices.<sup>51</sup> Such research is sometimes referred to as “web privacy measurement.”<sup>52</sup>

Several authors in North America analyse consent to data processing through a law and economics lens, and consider the implications of behavioural economics for online privacy.<sup>53</sup> In Europe, authors such as Cserne, Howells, and Luth examine the implications of behavioural economics for consumer law, without, however, discussing privacy.<sup>54</sup> A couple of European authors, such as Brown, take behavioural economics into account when discussing data protection law.<sup>55</sup>

#### **1.4 Scope of the study**

The research question concerns behavioural targeting, the monitoring of people's online behaviour to use the collected information to show people individually targeted advertisements. Behavioural targeting enables more possibilities than targeted

---

<sup>47</sup> Gürses 2010

<sup>48</sup> Gandy 1993; Lyon 2002. Surveillance studies can be described as follows. “The contribution of surveillance studies is to foreground empirically, theoretically and ethically the nature, impact and effects of a fundamental social-ordering process. This process comprises the collection, usually (but not always) followed by analysis and application of information within a given domain of social, environmental, economic or political governance” (Lyon et al. 2012, p. 1).

<sup>49</sup> Hildebrandt et al. 2008; Solove 2006; Solove 2008; Zarsky 2004.

<sup>50</sup> Turow 2011.

<sup>51</sup> Mayer & Mitchell 2012; Gomez et al. 2009; Hoofnagle et al. 2012; Krishnamurthy & Wills 2009; Van Eijk 2011.

<sup>52</sup> Berkeley Law 2012.

<sup>53</sup> E.g. Kerr et al. 2009; Nehf 2005.

<sup>54</sup> Luth 2010; Cserne 2008; Howells 2005.

<sup>55</sup> Brown 2011; Brown 2013; See also Helberger et al. 2012.

advertising, such as personalised content and personalised prices (a type of price discrimination). Such topics are mentioned in passing, but aren't the main focus of this study. In the long term behavioural targeting may decrease ad revenues for some website publishers. The changing power relations in the media landscape resulting from behavioural targeting are not an independent topic of inquiry in this study.<sup>56</sup>

The scope of this study is limited to the EU. When examining legal privacy protection in Europe, one automatically ends up looking at data protection law. As noted, data protection law is the main legal instrument to protect information privacy in Europe. Considering their specific relevance for behavioural targeting, a couple of themes within data protection law were selected for this study.<sup>57</sup> The study doesn't aim to give an overview of all data protection provisions that could be relevant for behavioural targeting. For example, the question of which national data protection law applies to firms based in or outside Europe falls outside the study's scope, as do trans-border data flows.<sup>58</sup> Whether special rules are needed for children isn't discussed in this study.<sup>59</sup> A discussion of the so-called right to be forgotten and the problematic interplay between data protection law and freedom of speech falls outside this study's scope.<sup>60</sup> The study doesn't examine the competence of the EU to adopt data protection rules.<sup>61</sup>

This isn't a handbook listing all European regulation and case law that might be relevant for behavioural targeting.<sup>62</sup> For example, advertising law, non-discrimination

---

<sup>56</sup> See on that topic chapter 2, section 2; chapter 7, section 2. See in more detail Turow 2011.

<sup>57</sup> See chapter 4, 5 and 6.

<sup>58</sup> On the territorial scope of data protection law, see Moerel 2011, chapter 1-4; Kuner 2010; Kuner 2010a; Piltz 2013. On transborder data flows see Moerel 2011; Kuner 2013.

<sup>59</sup> See on children and data protection law Van Der Hof et al. 2014.

<sup>60</sup> See on a right to be forgotten Ausloos et al. 2012 (mostly positive); Van Hoboken 2013 (more critical); Mayer-Schönberger 2009 (US focused). See also CJEU, C-131/12, Google Spain, 13 May 2014, and on that case Kulk & Zuiderveen Borgesius 2014.

<sup>61</sup> The 1995 Data Protection Directive is based on the old article 95 of the Treaty establishing the European Community, which corresponds to article 114 of the Treaty on the Functioning of the EU (consolidated version 2012). The European Commission proposal for a Data Protection Regulation (2012) is based on article 16 of the Treaty on the Functioning of the EU (consolidated version 2012).

<sup>62</sup> Good overview books about data protection law generally are Bygrave 2002; Bygrave 2014; Büllsbach et al. 2010; European Agency for Fundamental Rights 2014; Kuner 2007.

law, competition law, and consumer law are excluded from the analysis.<sup>63</sup> Having said that, the study does take some inspiration from consumer law.<sup>64</sup> Providing a new privacy definition isn't among the study's goals. This isn't a work of legal philosophy or political science.<sup>65</sup> The democratic deficit of the EU and the influence of lobbying on EU regulation are outside the study's scope.

A distinction by Baldwin et al. can help to clarify this study's scope. They distinguish six tools that the state can use to regulate behaviour.<sup>66</sup> In current data protection law, three of the tools are present: to command, to inform, and to confer protected rights. The first tool is commanding. For example, the state can prohibit or require certain activities. This strategy can be found in data protection law. For example, personal data processing is only allowed if there's a legal basis for the processing. The second tool is using information for policy goals. For instance, the law can require firms to disclose certain information to help people make decisions. Data protection law partly relies on this strategy. Firms are required to be transparent about data processing towards the data subject. This study doesn't analyse other ways of informing the data subject, such as education. The third tool is conferring protected rights. The state can grant people rights, which they can enforce themselves. Tort law and property rights could be seen as examples of this approach.<sup>67</sup> Parts of data protection law also grant people rights they can enforce themselves. People can take a firm to court when their data protection rights are infringed.<sup>68</sup> Even the rights granted to individuals by constitutions and human rights treaties, such as the right to privacy, could be seen as

---

<sup>63</sup> See for a media law angle Helberger 2013. See on non-discrimination law and profiling Hildebrandt et al. 2008; Zarsky et al. 2013; De Vries et al. 2013.

<sup>64</sup> There isn't much literature that applies European consumer protection law to behavioural targeting. See for exceptions Van Der Sloot 2012; Centre for the Study of European Contract Law (CSECL) & Institute for Information Law (IViR) 2012; European Data Protection Supervisor 2014.

<sup>65</sup> See for a legal philosophical angle on behavioural targeting Hildebrandt & Gutwirth (eds.) 2008, and for a philosophy and ethics angle Nissenbaum 2011; Bozdag & Timmersmans 2011; Bozdag & Van De Poel 2013. See on data protection law through a political science lens Bennett 1992; Regan 1995; Heisenberg 2005; Newman 2008, and specifically on the regulation of cookies Kierkegaard 2005.

<sup>66</sup> Baldwin et al. 2011, p. 106, and generally chapter 7. Baldwin et al. work in the field of "regulation studies", see chapter 8, section 1 of this study. Lessig distinguished four "modalities" of regulation: law, architecture (technology, or "code"), social norms and the market (Lessig 2006). This study focuses mostly on law.

<sup>67</sup> Baldwin et al. 2011, p. 126-128. See also Ogus 2004, p. 257-258.

<sup>68</sup> See chapter 8, section 1.

an example of this regulatory strategy.<sup>69</sup> Some authors have discussed introducing property or intellectual property rights on personal information; a discussion of such proposals falls outside this study's scope.<sup>70</sup>

Three other types of policy tools fall outside the study's cope: deploying wealth, harnessing markets, and acting directly.<sup>71</sup> First, the state could use tax or subsidies to influence behaviour. For instance, many European states fund public broadcasters. Deploying wealth has been suggested as an instrument in the area of online privacy: in France there was discussion about the possibility of taxing the use of personal data.<sup>72</sup> Second, the state can aim to guide markets, with competition law for example.<sup>73</sup> Third, the state can act directly. For instance, the state can construct a bridge or a road, or organise hospitals or a pension scheme. The state played a large role in developing the internet.<sup>74</sup> In principle, the state could also set up, or help to set up, internet services such as websites or even search engines.

## 1.5 Outline

The outline of the thesis is detailed below. The research question was introduced in this first chapter: how could European law improve privacy protection in the area of behavioural targeting, without being unduly prescriptive?

Chapter 2 explains what behavioural targeting is, by distinguishing five phases. During the first phase of behavioural targeting, firms track people's online behaviour. Second, firms store data about individuals. Third, firms analyse the data. Fourth, firms

---

<sup>69</sup> Human rights are typically inalienable, while, for instance, property rights usually can be transferred to others (see Calabresi & Melamed 1972).

<sup>70</sup> The most extensive discussion of property rights on personal data is Purtova 2011. She characterises such proposals as a means to improve data subject control, and suggests mandatory protective rules are needed as well (p. 244). See on introducing a type of intellectual property right on personal data Dommering 2010; Dommering 2012.

<sup>71</sup> Baldwin et al. 2011, p. 106 and further.

<sup>72</sup> Collin & Colin 2013.

<sup>73</sup> Some scholars have asked what competition law can do to protect privacy interests, but for the moment there are more questions than answers. See Geradin & Kuschewsky 2013; European Data Protection Supervisor 2014.

<sup>74</sup> Bing 2009.

disclose data to other parties. In the fifth phase, data are used to target ads to specific individuals.

Chapter 3 discusses the right to privacy in European law, and the privacy implications of behavioural targeting. Three privacy perspectives are distinguished in this study: privacy as limited access, privacy as control, and privacy as identity construction. The chapter discusses three main privacy problems of behavioural targeting. First, the massive collection of information on user behaviour can have a chilling effect. Second, people lack control over their information. Third, behavioural targeting enables social sorting and discriminatory practices. Also, some fear that personalised ads and other content could be manipulative, or could narrow people's horizons.

Chapter 4 introduces data protection law, Europe's main legal tool to protect information privacy. Data protection law aims to ensure that personal data processing happens fairly and transparently. The history of data protection law can help to understand its focus on informed consent and transparency. The chapter shows that there's a tension within data protection law between empowering and protecting the individual. This tension is a recurring theme in this study.

Chapter 5 concerns the material scope of data protection law. Many behavioural targeting firms say data protection law doesn't apply to them, because they only process "anonymous" data. The chapter makes two points. First, an analysis of current law shows that data protection law generally applies to behavioural targeting. Data protection law also applies if firms don't tie a name to individual profiles. Second, from a normative perspective, data protection law should apply.

Chapter 6 discusses the role of informed consent in the regulation of behavioural targeting. Current law regarding behavioural targeting places a good deal of emphasis on informed consent. The e-Privacy Directive requires firms to obtain informed consent for the use of most tracking technologies, such as cookies. Furthermore, in general data protection law, consent is one of the legal bases that a firm can rely on for personal data processing.

Chapter 7 analyses practical problems with informed consent in the area of behavioural targeting. The chapter reviews law and economics literature, behavioural economics literature, and empirical research on how people make privacy choices. The chapter shows that the potential of data protection law's informed consent requirement as a privacy protection measure is very limited. People generally ignore privacy policies, and click "I agree" to almost any online request.

Chapter 8 discusses measures to improve individual *empowerment*. Strictly enforcing and tightening data protection law would be a good start. For example, firms shouldn't be allowed to infer consent from mere inactivity from the individual, and long unreadable privacy policies shouldn't be accepted. User-friendly mechanisms should be developed to foster transparency and to enable people to express their choices. This study doesn't suggest that data subject control over personal information can be fully achieved. Nevertheless, some improvement must be possible, as now people's data are generally accumulated and used without meaningful transparency or consent.

Chapter 9 discusses measures to improve individual *protection*. Certain data protection principles could protect people, even if they consent to data processing. While the role of informed consent in data protection law is important, it's at the same time limited. People can't waive data protection law's safeguards, or contract around the rules. The protective data protection principles should be enforced more strictly; but this won't be enough. In addition to data protection law, more specific rules regarding behavioural targeting are needed. If society is better off if certain behavioural targeting practices don't happen, the lawmaker should consider banning them.

Chapter 10 summarises the main findings and answers the research question. There's no easy solution, but legal privacy protection can be improved in the area of behavioural targeting. The limited potential of informed consent as a privacy

protection measure should be taken into account. Therefore, the lawmaker should focus less on empowering people, and more on protecting people.

\* \* \*