Consent to Behavioural Targeting in European Law - What are the Policy Implications of Insights from Behavioural Economics?

Zuiderveen Borgesius, F.

DOI
10.2139/ssrn.2300969

Publication date
2013

Document Version
Submitted manuscript

UNIVERSITY OF AMSTERDAM

CONSENT TO BEHAVIOURAL TARGETING IN EUROPEAN LAW - WHAT ARE THE POLICY IMPLICATIONS OF INSIGHTS FROM BEHAVIOURAL ECONOMICS?

Frederik Zuiderveen Borgesius

Amsterdam Law School Legal Studies Research Paper No. 2013-43

Institute for Information Law Research Paper No. 2013-02

CONSENT TO BEHAVIOURAL TARGETING IN EUROPEAN LAW

WHAT ARE THE POLICY IMPLICATIONS OF INSIGHTS FROM BEHAVIOURAL ECONOMICS?

Frederik Zuiderveen Borgesius[1]
IViR - Institute for Information Law - University of Amsterdam

Draft for Privacy Law Scholars Conference, 7 June 2013 Berkeley
This is a rough working draft, so please don't cite. Contact me for the latest version. I'd love to receive your comments at F.J.ZuiderveenBorgesius[at]uva.nl. Thanks!

Abstract

Behavioural targeting is the monitoring of people's online behaviour to target advertisements to specific individuals. European law requires companies to obtain informed consent of the internet user before they use tracking technologies for behavioural targeting. Other jurisdictions also emphasise the importance of choice for internet users. But many people click 'I agree' to any statement that is presented to them. This paper discusses insights from behavioural economics to analyse problems with informed consent to behavioural targeting from a regulatory perspective. What are the policy implications of insights from behavioural economics in the context of behavioural targeting? Two approaches to improve regulation are explored. The first focuses on empowering the individual, for example by making informed consent more meaningful. The second approach focuses on protecting the individual. If aiming to empower people is not the right tactic to protect privacy, maybe specific prohibitions should be introduced.

[1] I am grateful for comments from Axel Arnbak, Oren Bar-Gill, Stefan Kulk, Aleecia McDonald, Florencia Marotta-Wurgler, Alessio Pacces, Joost Poort, Omer Tene, Nico van Eijk, Joris van Hoboken, and participants to the workshop during the 6th Annual Privacy Law Scholars Conference (Berkeley, 7 June 2013). Any errors are my own.

TABLE OF CONTENTS

1. Introduction

Behavioural targeting is the monitoring of people's online behaviour, to target advertisements to specific individuals.[2] Behavioural targeting can have benefits for marketers and internet users, but it also raises privacy concerns.

Using cookies or other techniques, companies can compile detailed profiles of internet users, based on what they read, what videos they watch, what they search for etc. Much of the collection of personal information on the internet is related to behavioural targeting. It forms the core of many privacy related questions on the internet. Behavioural targeting could be seen as an early example of ambient intelligence, technology that senses and anticipates people's behaviour to adapt the environment to their needs.[3]

Many laws that aim to protect privacy emphasise the importance of informed consent. For instance, the Charter of Fundamental Rights of the European Union says that 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".[4] But insights from behavioural economics cast doubt on the effectiveness of the informed consent approach as a privacy protection measure. The paper concerns the following question. *What are the policy implications of insights from behavioural economics in the context of consent to behavioural targeting?*

This paper discusses practical problems with informed consent. It reviews law and economics literature, behavioural law and economics literature, and empirical research on how people make privacy choices. Law and economics provides a tool to analyse certain problems people encounter when choosing whether to consent to behavioural targeting. The main problems are that people don't have enough information (information asymmetry) and that informing themselves would take too much time (transaction costs).

Behavioural economics uses findings from for example psychology to predict human behaviour. There's a growing body of empirical research on how people make privacy choices in the context of behavioural targeting, by for example Acquisti, Cranor and McDonald.[5] The research suggests that people don't make decisions in their own best interests when confronted with information asymmetries. Moreover, even when assuming that people have enough information to base their decisions on, they might

[2] For descriptions of behavioural targeting also: Article 29 Working Party, 'Opinion 2/2010 on Online Behavioural Advertising' (WP 171), 22 June 2010, p 3; Interactive Advertising Bureau. 'Glossary of Interactive Advertising Terms v. 2.0' <www.iab.net/media/file/GlossaryofInteractivAdvertisingTerms.pdf> accessed on 5 April 2013.
[3] Hildebrandt M, 'Privacy en Identiteit in Slimme Omgevingen [Privacy and Identity in Smart Environments]' (2010)(6) Computerrecht 272, 276.
[4] Article 8 of the Charter of Fundamental Rights of the European Union.
[5] See section 5.

make decisions that are contrary to their own stated interests, and contrary to their own best interests.

For the analysis in this paper, it's assumed that consenting to behavioural targeting is somewhat comparable to entering a contract, or to exchanging personal data against the use of a service. In practice people often appear to "pay" with their personal data for the use of internet services.[6] Legal scholars don't agree on the question of whether consent in data protection law should be seen as agreeing to a contract.[7] This study doesn't suggest that consenting to data processing *should* be seen as entering a contract. For ease of reading the paper sometimes refers to data subjects as consumers.[8] However, the right to privacy protects much more than merely consumer interests.

Some remarks about the scope of this paper. Broadly speaking, three categories of reasons to limit contractual freedom can be distinguished in European legal systems. (i) Sometimes contractual freedom is limited because of public values. National laws use a variety of terms, such as unconscionability, or contracts contrary to bona mores, to public policy, or to good faith.[9] (ii) Sometimes contractual freedom is limited to protect parties other than the contract parties. (iii) Sometimes there are limits to protect contract parties themselves, because they are not expected to enter contracts in their own best interests, for instance in consumer law.[10]

Law and economics and behavioural law and economics literature usually focus on category (ii) and (iii).[11] The main subject of this paper is category (iii), people having problems entering contracts in their own interests. This paper largely ignores category (i). Many dimensions of privacy are not dealt with. For instance, requirements that follow from privacy's status as a human right receive little attention in this paper.

The paper doesn't aim to improve economic theory. The analysis is meant as an addition to legal discourse. The paper focuses on European data protection law, but

---

[6] A popular phrase in this context is: "If you are not paying for it, you're not the customer; you're the product being sold." It appears the phrase was first used on the discussion forum Metafilter (Blue_beetle (26 August 2010) < www.metafilter.com/95152/Userdriven-discontent#3256046> accessed on 5 April 2013).

[7] See e.g. Verhelst EW, *Recht Doen aan Privacyverklaringen: een Juridische Analyse van Privacyverklaringen op Internet [A Legal Analysis of Privacy Policies on the Internet] (Ph.D thesis University of Tilburg)* (Academic version 2012); Van der Sloot B, 'De Privacyverklaring als Onderdeel van een Wederkerige Overeenkomst [The Privacy Policy as a Part of a Reciprocal Agreement]' (2010) 13(3) Privacy & Informatie 106.

[8] This paper uses "consumer" as a broad term, not as a legal category.

[9] Howells GG, 'Introduction' in Howells GG, Micklitz HW and Wilhelmsson T (eds), *European Fair Trading Law: The Unfair Commercial Practices Directive* (Ashgate Publishing Company 2006), 4. See about limits on contractual freedom based on fundamental rights: Mak C, *Fundamental Rights in European Contract Law: A Comparison of the Impact of Fundamental Rights on Contractual Relationships in Germany, the Netherlands, Italy, and England (Ph.D thesis University of Amsterdam)* (Kluwer Law International 2008).

[10] See for similar distinctions: Cserne P, *Freedom of Contract and Paternalism: Prospects and Limits of an Economic Approach (Ph.D thesis University of Hamburg)* (Academic version 2008), 41; Grundmann S, Kerber W and Weatherill S, 'Party Autonomy and the Role of Information' in Grundmann S, Kerber W and Weatherill S (eds), *Party Autonomy and the Role of Information in the Internal Market* (De Gruyter 2001), 6.

[11] If a well-functioning market or a high level of social welfare were seen as a public value, it could also be argued that economics mainly looks at (i), public values. See section 3.1.

the conclusions can be relevant outside Europe too, as "informed consent" plays a large role in many laws that aim to protect privacy.

The paper gives suggestions to improve regulation. Two regulatory techniques are explored. The first focuses on empowering the individual, for example by aiming to make informed consent more meaningful. The second approach focuses on protecting rather than empowering the individual. If aiming to empower people is not the right tactic to protect privacy, maybe specific prohibitions should be introduced.

The paper is structured as follows. Section 2 provides background information to the discussion. The section introduces the practice of behavioural targeting, people's attitudes toward this practice, European data protection law, the consent requirement for tracking technologies, and discussions about a Do Not Track standard. Section 3 introduces law and economics, the economics of privacy, and the limits of an economic analysis of privacy. Then attention shifts to problems with informed consent. Section 4 takes a law and economics approach, and discusses information asymmetries, transaction costs, externalities, and market power. Section 5 focuses on insights from behavioural economics, discussing biases such as myopia and the status quo bias. Section 6 discusses policy implications of the findings, and gives suggestions to improve regulation. Section 7 concludes.

2. Behavioural targeting and data protection law

2.1 Behavioural targeting

This section introduces behavioural targeting, the monitoring of people's online behaviour, to target advertisements to specific individuals. In a simplified example, behavioural targeting involves three parties: an internet user, a website publisher, and an advertising network. An internet user visits a website, and an advertising network serves advertising on that website. Advertising networks serve advertisements on thousands of websites, and can recognise internet users when they surf the web.

An advertising network might assume that an internet user who often visits websites about recipes is a food enthusiast. If the user visits a news website, the advertising network might show advertising for restaurants or cookbooks. When visiting that same news website, somebody who reads many legal blogs might see advertising for law books.

A commonly used technology for behavioural targeting involves cookies. A cookie is a small text file that a website stores on a computer of an internet user to recognise that device during subsequent visits. Many website publishers use cookies, for example to remember the contents of a shopping cart ("first party cookies").

Advertising networks can place and read cookies as well ("third party cookies"). As a result, an advertising network can follow the online behaviour of an internet user across all sites on which it serves advertisements.

In addition to cookies, companies can use many other technologies for tracking and behavioural targeting. Tracking technologies that rely on storing information on a user's device, such as flash cookies and HTML5 local shared objects, are sometimes called "super cookies". These are often harder to delete than conventional cookies. Other technologies include device fingerprinting and deep packet inspection. Therefore, deleting cookies from one's browser isn't always sufficient to prevent being tracked. Some speak of an arms race between companies doing behavioural targeting and internet users.[12]

Data collection for behavioural targeting is widespread. For instance, in 2010 the 50 most popular websites except one (Wikipedia) in the United States all used tracking technologies.[13] In October 2012, Hoofnagle & Good found that a visit to the most 100 popular websites lead to receiving 5493 third party cookies, from 457 different third parties. Super cookies are placed through the top 100 websites as well. Moreover, the researchers found a trend towards more tracking.[14]

Many behavioural targeting companies can tie a name or an email address to the data they have on individuals. Providers of social network sites like Facebook generally know the name of many of their users. A provider of an email service that does behavioural targeting could tie an email address to the data it has on individuals. Companies can enrich profiles by merging data sets from different sources. Many companies add data gathered offline (in the real world) to online profiles. Some providers of email services also analyse people's communication for behavioural targeting.[15]

In sum, to present people with targeted advertising, many companies collect large amounts of data for behavioural targeting, and can compile highly detailed profiles of people.

---

[12] Hoofnagle CJ and others, 'Behavioral Advertising: The Offer You Cannot Refuse' (2012) 6(2) Harvard Law & Policy Review 273, 291.

[13] Angwin J, 'The Web's New Gold Mine: Your Secrets, A Journal Investigation Finds that one of the Fastest-growing Businesses on the Internet is the Business of Spying on Consumers (Wall Street Journal)' (30 July 2010) <http://online.wsj.com/article/SB10001424052748703940904575395073512989404.html> accessed on 7 April 2013.

[14] Hoofnagle CJ and Good N, 'The Web Privacy Census (UC Berkeley)' (October 2012) <http://law.berkeley.edu/privacycensus.htm> accessed on 5 April 2013.

[15] See e.g. Google. 'Ads in Gmail. How Gmail Ads work' (29 March 2013) <http://support.google.com/mail/answer/6603> accessed on 11 April 2013.

2.2 People's attitudes towards behavioural targeting

This section discusses studies on people's attitudes towards behavioural targeting. Research suggests that, while some like the idea, most people don't want targeted advertising based on their online behaviour. Most relevant research comes from the United States. Turow et al. found in a nationally representative phone survey that 66% of adult Americans don't want to receive advertisements that are tailored to their interests (the number is 55% for the age group between 18 and 24). When people were told that tailored advertisements would be based on their browsing behaviour, 87% didn't want targeted advertising. People were also asked whether they would allow marketers to "follow you online in an anonymous way in exchange for free content." 68% said they definitely wouldn't allow it, and 19% probably wouldn't.

The researchers conclude: "Contrary to what marketers say, Americans reject tailored advertising (…). Whatever the reasons, our findings suggest that if Americans could vote on behavioural targeting today, they would shut it down."[16] The TRUSTe Company found similar results in 2011: only 15% of the respondents would "definitely or "probably" consent to tracking for more relevant advertising.[17]

In a non-representative survey, Cranor & McDonald found that 18% of the respondents want behaviourally targeted advertising because it leads to more relevant advertising. 12% doesn't mind being tracked. On the other hand, 46% finds it "creepy" when advertisements are based on their browsing behaviour. 64% agrees with the statement "Someone keeping track of my activities online is invasive."[18] Overall, the study found mostly negative reactions to behavioural targeting.

The researchers also questioned people about companies analysing the contents of email messages for targeted advertising. This is a common practice for free email services such as Gmail and Yahoo.[19] 4% likes their email being scanned because it leads to more relevant advertising. About one in ten says "it's ok as long as the email

[16] Turow J and others, 'Americans Reject Tailored Advertising and Three Activities that Enable it' (29 September 2009) <http://ssrn.com/abstract=1478214> accessed on 5 April 2013, 4.
[17] TRUSTe Research in partnership with Harris Interactive, '2011 Consumer Research Results. Privacy and Online Behavioural Advertising' (25 July 2011) <www.eff.org/sites/default/files/TRUSTe-2011-Consumer-Behavioural-Advertising-Survey-Results.pdf> accessed on 14 February 2013.
[18] McDonald AM and Cranor LF, 'Beliefs and Behaviors: Internet Users' Understanding of Behavioral Advertising' (Telecommunications Policy Research Conference) (2 October 2010) <http://ssrn.com/abstract=1989092> accessed on 5 April 2013, 23.
[19] Yahoo said in July 2012: "Yahoo! now automatically identifies items such as words, links, people and subjects from your email to learn what matters to you so that we can deliver exciting new product features and relevant ads" (Gallagher B, 'Welcome To The New And Improved Yahoo Mail. And It's Crashing' (31 July 2012) <http://techcrunch.com/2012/07/31/welcome-to-the-new-and-improved-yahoo-mail-and-its-crashing/#> accessed on 13 April 2013).

service is free".[20] But 62% says advertising based on email content is creepy.[21] A study under university students in Toronto found similar results in 2011.[22]

Some studies find less negative attitudes to behavioural targeting. Hastak and Culnan found that 48% felt uncomfortable about their browsing behaviour being used for advertising. 23% was comfortable with it. That number would grow to 40% if websites would give information about behavioural targeting and would offer an opt-out system.[23] Some, but not all, industry sponsored surveys find more positive attitudes towards behavioural targeting.[24]

Ur et al. report on 48 in-depth interviews about online behavioural advertising. After being informed what behavioural targeting is, people saw disadvantages and benefits. Almost half of the participants liked the idea of more relevant advertising. On the other hand, a majority mentioned privacy when asked whether there were downsides to behavioural targeting.[25] "Participants commonly said they were scared about being tracked and monitored."[26] Most participants didn't like the idea of behavioural targeting. "However, this attitude seemed to be influenced in part by beliefs that more data is collected than actually is."[27] The researchers conclude that people find behavioural targeting "smart, useful, scary, and creepy at the same time."[28]

Results by European researchers are largely consistent with the American results. In a large study (26,574 people) in the European Union[29] the researchers explained that advertising pays for free email accounts and free search engines. Then they asked: "How comfortable are you with the fact that those websites use information about your online activity to tailor advertisements or content to your hobbies and interests?"

---

[20] McDonald AM and Cranor LF, 'Beliefs and Behaviors: Internet Users' Understanding of Behavioral Advertising' (Telecommunications Policy Research Conference) (2 October 2010) <http://ssrn.com/abstract=1989092> accessed on 5 April 2013, 22.

[21] Idem, 21.

[22] Foster M, West T and Levin A, 'The Next Frontier. Targeted Online Advertising and Privacy (Ted Rogers School of Management/Ryerson University)' (September 2011) <www.ryerson.ca/content/dam/tedrogersschool/privacy/Targeted_Online_Advertising_and_Privacy.pdf> accessed on 17 November 2012.

[23] Hastak, M and Culnan MJ, 'Online Behavioral Advertising "Icon" Study (Future of Privacy Forum)' (January 2010) <http://futureofprivacy.org/final_report.pdf> accessed on 18 November 2012.

[24] For instance, a report by Annalect says: "Most consumers (84%) state they would *not* pay for access to online content that is free now, and instead, they would rather receive targeted advertising in exchange for free access to online content" (emphasis original). On the other hand: "Nearly all (93%) Internet users would use or already use the DNT button, however, only 22% of users are aware of this function" (Annalect, 'Internet Users' Response to Consumer Online Privacy' (14 March 2012) <http://annalect.com/wp-content/uploads/2012/06/Consumer_Online_Privacy_Whitepaper.pdf> accessed on 10 April 2013).

[25] Ur B and others, 'Smart, Useful, Scary, Creepy: Perceptions of Online Behavioral Advertising' (Proceedings of the Eighth Symposium on Usable Privacy and Security ACM, 2012) 4, 6.

[26] Idem, p. 7.

[27] Idem, p. 11.

[28] Idem, p. 6.

[29] European Commission. 'Special Eurobarometer 359: Attitudes on Data Protection and Electronic Identity in the European Union' (2011) <http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf> accessed on 18 November 2012.

54% felt uncomfortable.[30] (The question could be read as concerning only tracking within one website.) The study also found that seven out of ten people are concerned that companies might use data for new purposes such as targeted advertising without informing them.[31] 22% trust search engines, social network sites or email services with their data.[32]

In interviews in the United Kingdom, Brown et al. find that people strongly opposed to companies sharing data with third parties. "There was a strongly negative, almost emotional reaction in every group to the idea of third parties collecting data across a range of different devices and activities to develop an understanding of every aspect of consumers' lives."[33]

Bartlett reports on a representative study in the United Kingdom in 2012. 8% is comfortable with advertising based on their browsing history.[34] 10% is conformable with Gmail scanning the contents of emails for targeted advertising. Around eight out of ten people worry about companies using their data without consent and selling data to third parties.[35]

Helberget et al. report on interviews in the Netherlands that suggest that few people are aware of behavioural targeting. People expressed privacy concerns after being told about it.[36] In a 2011 study by the Dutch Dialogue Marketing Association, 21% of the respondents felt that they had nothing to hide and that therefore companies didn't infringe their privacy. But 70% didn't want behavioural advertising.[37]

People often act differently in practice than might be expected from them based on survey results. This is the case for privacy choices as well. People that say they care deeply about privacy, often disclose personal information in exchange for minimal benefits. We will return to this "privacy paradox" below, in section 5.6.[38]

It's impossible to generalise findings from different regions and from studies that use different methods. But two common themes seem to emerge. A small minority prefers

---

[30] Idem, 74.
[31] Idem, 146.
[32] Idem, 138.
[33] Marks P and others, 'Future of Advertising Technology: Final Report' (January 2010) A Report for Ofcom (leaked document), 83.
[34] Bartlett J, 'The Data Dialogue (Demos, 2012)' <www.demos.co.uk/files/The_Data_Dialogue.pdf?1347544233> accessed on 18 November 2012, 36-37.
[35] Idem, 39.
[36] Helberger N and others, 'Online Tracking: Questioning the Power of Informed Consent' (2012) 14(5) Info 57, 70.
[37] Boogert E, 'Meeste Nederlanders: 'Persoonlijke Online Reclame is Ongewenst [Majority Dutch People: 'Personalised Advertising Is Unwanted']' (Emerce) (15 November 2011) <www.emerce.nl/nieuws/meeste-nederlanders-persoonlijke-online-reclame-ongewenst> accessed on 16 November 2012.
[38] Acquisti speaks of a "privacy paradox: people want privacy, but do not want to pay for it, and in fact are willing to disclose sensitive information for even small rewards." Acquisti A, 'The Economics of Personal Data and the Economics of Privacy (preliminary draft)' (2010) <www.heinz.cmu.edu/~acquisti/papers/acquisti-privacy-OECD-22-11-10.pdf> accessed on 4 February 2013, 37.

behaviourally targeted advertising because it leads to more relevant advertising, and doesn't mind their browsing behaviour being tracked. But a majority says it doesn't want behavioural targeting.

2.3 The Data Protection Directive and consent

This section introduces European data protection law, and its application to behavioural targeting. Data protection law is a legal tool that aims to ensure that the processing of personal data happens fairly and transparently. The Data Protection Directive requires the European Union member states to implement data protection laws.[39] This paper focuses on the Directive, rather than the national laws.

Sometimes the paper refers to opinions of the Article 29 Working Party, an advisory body to the European Commission on data protection matters.[40] The Working Party's opinions are not legally binding. But they are influential, since the Working Party consists of representatives of the Data Protection Authorities of the European Union member states and the European Data Protection Supervisor,[41] and usually takes decisions by consensus.[42] Judges and national Data Protection Authorities often follow its interpretation.[43]

Data protection law is triggered when a company processes "personal data", information relating to an identified or identifiable person ("data subject").[44] If a company doesn't process "personal data", data protection law doesn't apply.[45] The definition of "processing" is broad and almost everything that can be done with personal data falls within this definition.[46]

Behavioural targeting often entails the processing of personal data. The Working party says that pseudonymous data, for example tied to a cookie, are personal data because they "enable data subjects to be 'singled out', even if their real names are not

---

[39] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (L 281, 23 November 1995, 0031-0050) (hereafter: Data Protection Directive).
[40] Article 29 and 30 of the Data Protection Directive.
[41] <www.edps.europa.eu> accessed on 9 April 2013.
[42] Gutwirth S and Poullet Y, 'The Contribution of the Article 29 Working Party to the Construction of a Harmonised European Data Protection System: an Illustration of 'Reflexive Governance'?' in Asinari VP and P Palazzi (eds), *Défis du Droit à la Protection de la Vie Privée. Challenges of Privacy and Data Protection Law* (Bruylant 2008).
[43] See e.g. the Sabam judgment of the Court of Justice of the European Union. The Court largely follows the Advocate General, and the Advocate General relies mainly on opinions of the Article 29 Working Party (CJU, 24 November 2011, C-70/10 (Sabam/Scarlet).
[44] Article 2(a) of the Data Protection Directive.
[45] The Data Protection Directive distinguishes a data "controller", who determines the purposes and means of the processing, from the data "processor", who processes data for a controller. For ease of reading, this paper refers to both actors as "companies" (article 2(d) and 2(e) of the Data Protection Directive).
[46] Article 2(b) of the Data Protection Directive.

known".[47] This is compatible with case law of the Court of Justice of the European Union.[48] Moreover, companies are often able to tie a name to a behavioural targeting profile. Many, although not all,[49] commentators agree that data protection law generally applies to behavioural targeting.[50] European data protection law is currently under revision. There's much debate on the question of whether pseudonymous data should be subject to a lighter regime.[51]

The data protection principles, sometimes called the fair information principles,[52] form the core of the data protection regime.[53] Most important is the transparency principle. Surreptitious data collection isn't allowed. A company must provide people whose data it processes all information that is needed to guarantee fair processing. The data quality principle requires companies to take reasonable steps to ensure they erase or rectify inaccurate data. It follows from the data minimisation principle that parties shouldn't collect excessive amounts of data. The security principle requires an appropriate level of security for databases.[54] Data protection law has a stricter regime for "sensitive data", such as data revealing racial or ethnic origin, religious beliefs, and data concerning health or sex life.[55]

The purpose limitation principle says that personal data must be collected for specified, explicit and legitimate purposes. Furthermore, data that are collected for one goal shouldn't be used for incompatible purposes.[56] A company needs a legitimate basis to process personal data. Personal data may be processed on the basis of the consent of the person concerned or another basis laid down by law. Below this is discussed in more detail.

---

[47] Article 29 Working Party, 'Opinion 2/2010 on Online Behavioural Advertising' (WP 171), 22 June 2010, 9. See also Article 29 Working Party, 'Opinion 4/2007 on the Concept of Personal Data' (WP 136), 20 June 2007, 12-20.

[48] CJU, 24 November 2011, C-70/10 (Sabam/Scarlet.

[49] Zwenne G, 'Over Persoonsgegevens en IP-adressen, en de Toekomst van Privacywetgeving [On Personal Data and IP addresses, and the Future of Privacy Legislation]' in Mommers L and others (eds), *Het Binnenste Buiten. Liber Amicorum ter Gelegenheid van het Emiritaat van Prof. dr. Aernout H.J. Schmidt, Hoogleraar Recht en Informatica te Leiden [The Inside Out. Liber Amicorum for Retirement of Prof. Dr. Aernout H. J. Schmidt, Professor of Law and Computer Science in Leiden]* (eLaw@Leiden 2010). See also Zwenne's soon to be published Inaugural lecture, which includes a translation to English. See in the American context: Schwartz PM and Solove DJ, 'The PII Problem: Privacy and a New Concept of Personally Identifiable Information' (2011) 86 New York University Law Review 1814.

[50] See e.g. Leenes R, 'Do They Know Me? Deconstructing Identifiability' (2008) 4(1-2) University of Ottawa Law and Technology Journal 135; De Hert P and Gutwirth S, 'Regulating Profiling in a Democratic Constitutional State', and Schreurs W and others, 'Cogitas, Ergo Sum. The Role of Data Protection Law and Non-discrimination Law in Group Profiling in the Private Sector' in Hildebrandt M and Gutwirth M (eds), *Profiling the European citizen: Cross-Disciplinary Perspectives* (Springer 2008).

[51] See e.g. Tene O and Wolf C, 'The Definition of Personal Data: Seeing the Complete Spectrum (Future of Privacy forum white paper)' (January 2013) <www.scribd.com/doc/121642913/The-Definition-of-Personal-Data-Seeing-the-Complete-Spectrum> accessed on 11 April 2013.

[52] See e.g. United States Department of Health, Education, and Welfare, 'Records, Computers, and the Rights of Citizens' (1973).

[53] The principles are also called "principles relating to data quality" (see article 6 of the Data Protection Directive).

[54] Article 17 of the Data Protection Directive.

[55] Article 8 of the Data Protection Directive.

[56] Article 6(1)(b) of the Data Protection Directive. The first requirement is sometimes called the purpose specification principle (Article 29 Working Party, 'Opinion 03/2013 on Purpose Limitation (WP 203), 2 April 2013).

European data protection law applies when a company is established in the European Union. Many American companies, such as Facebook, Apple and Google, are formally established in Europe, and must comply. Among other situations, the law also applies if a company isn't based in Europe, but uses equipment in Europe for data processing.[57] European Data Protection Authorities say that if a company uses cookies to track people within the European Union, the law also applies.[58] Data protection law contains many more rules, such as rules regarding the export of data to outside the European Union and rules to establish which national data protection law within the European Union applies.

As noted, the Directive requires a company to have a legitimate basis to process personal data. Personal data may be processed on the basis of the consent of the person concerned or another basis laid down by law. For the private sector, the most important legal bases are a contract, a legitimate business interest that overrides the fundamental rights of the data subject, and consent.

First, data processing is allowed when it's "necessary for the performance of a contract to which the data subject is party (…)". This is for example the case when one pays with a credit card: certain personal data have to be processed. In some cases companies can also rely on this ground prior to entering a contract.[59] Whether companies can ground the processing of personal data for behavioural targeting on a contract isn't completely clear. Search engine providers have suggested that the use of their service implies a contract on the basis of which they can process personal data for targeted advertising. But the Article 29 Working Party doesn't accept this reasoning. The Working Party says that companies might be able to rely on this ground under certain circumstances, if people register for an account.[60]

Many behavioural targeting companies, such as advertising networks, don't have a direct relation with internet users, and don't ask them to sign up for an account. Therefore it's hard to see how they could enter a contract with the user. (For some companies, such as providers of social network sites, this might be different.) In sum, it's probably rare that companies can ground data processing for behavioural targeting on a contract.

Second, under the balancing provision, data processing is allowed when the "processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where

---

[57] Article 4 of the Data Protection Directive. See on jurisdiction in detail: Moerel L, *Binding Corporate Rules: Corporate Self-regulation of Global Data Transfers (Ph.D thesis University of Tilburg)* (Academic version 2012), chapter 2-5 with further references.

[58] Article 29 Working Party, 'Opinion 1/2008 on Data Protection Issues Related to Search Engines' (WP 148), 4 April 2008, 11.

[59] Article 7(b) of the Data Protection Directive.

[60] Article 29 Working Party, 'Opinion 1/2008 on Data Protection Issues Related to Search Engines' (WP 148), 4 April 2008, 17.

such interests are overridden by the interests for fundamental rights and freedoms of the data subject (…)". In short, a company can rely on this provision when its legitimate business interests outweigh the privacy interests of the data subject. For instance, under certain conditions, Google could ground the processing of personal data (pictures with people on them) for Street View on the balancing provision.[61]

If a company relies on the balancing provision for direct marketing, people have the right to stop the processing of their personal data.[62] Behavioural targeting is a kind of direct marketing.[63] So if a company could base personal data processing for behavioural targeting on the balancing provision, people would have the right to opt out. Hence, if a company could rely on the balancing provision, this would essentially mean that an opt-out system is sufficient.

When balancing the interests of the controller and the data subject, it has to be taken into account that the right to privacy and data protection are fundamental rights. Relevant questions are whether the processing of data is proportional to the purpose and whether there's another way of pursuing the purpose. Because the tracking of online behaviour can paint a highly detailed picture of the data subject, which is often regarded as an invasion of privacy, the data subject's interests should probably prevail in most cases.[64]

It has also been argued that in some circumstances, companies could ground data processing for behavioural targeting on the balancing provision. For instance, it has been suggested that tracking within one website could be based on the balancing provision, because it's less privacy invasive than tracking over multiple sites.[65]

---

[61] Van der Sloot B and Zuiderveen Borgesius FJ, 'Google's Dead End, or: On Street View and the Right to Data Protection: An Analysis of Google Street View's Compatibility with EU Data Protection Law' (2012)(4) Computer Law Review International 103.

[62] Article 14(b) of the data Protection Directive contains the right to object to direct marketing. Korff explains: "The Framework Directive [i.e. the Data Protection Directive] speaks of a right to "object to" rather than a right to prevent or stop the processing in question, but it is clear that the latter is intended. If a data subject exercises the right to object to direct marketing (…), the controller in question must comply with that objection." Korff D, *Data Protection Laws in the European Union* (Federation of European Direct Marketing and Direct Marketing Association 2005), 100.

[63] Direct marketing can be defined as: "The communication by whatever means (including but not limited to mail, fax, telephone, on-line services etc…) of any advertising or marketing material, which is carried out by the Direct Marketer itself or on its behalf and which is directed to particular individuals." This definition is taken from the European code of conduct of FEDMA for the use of personal data in direct marketing. A later FEDMA code of conduct makes clear that behavioural targeting is a kind of direct marketing: "Direct Marketing in the On-line environment refers to one-to-one marketing activities where individuals are targeted" The Working Party approved the codes in Article 29 Working Party, 'Opinion 3/2003 on the European Code of Conduct of FEDMA for the Use of Personal Data in Direct Marketing' (WP 77), 13 June 2003, and 'Opinion 4/2010 on the European Code of Conduct of FEDMA for the Use of Personal Data in Direct Marketing' (WP 174), 13 July 2010.

[64] Article 29 Working Party, 'Opinion 03/2013 on Purpose Limitation (WP 203), 2 April 2013, 46. Antic M, 'De Nieuwe Cookieregels, Onduidelijk, Onjuist en Ineffectief [The New Cookie Rules: Unclear, Incorrect, and Ineffective]' (2012)(2) Ars Aequi 103; Van der Sloot B and Zuiderveen Borgesius FJ, 'Google and Personal Data Protection' in Lopez-Tarruella, A. (ed), *Google and the Law. Empirical Approaches to Legal Aspects of Knowledge-Economy Business Models* (T.M.C. Asser Press/Springer 2012).

[65] Koëter J, 'Behavioral Targeting en Privacy: een Juridische Verkenning van Internetgedragsmarketing [Behavioural Targeting and Privacy: a Legal Exploration of Behavioural Internet Marketing]' (2009)(4) Tijdschrift voor internetrecht 104.

In a 2013 Opinion, the Working Party says that the balancing provision can almost never be used for behavioural targeting.[66] In 2010, the English Information Commissioner's Office (ICO) still appeared to have another view. The ICO said that behavioural targeting generally entails the processing of personal data. But the ICO added: "there are alternatives to consent".[67] This seems to imply that the ICO would allow companies to rely on the balancing provision for behavioural targeting. But the ICO isn't very explicit. In any case, the Working Party has expressed a different opinion in a later document. In sum, the most convincing view is that behavioural targeting can't be based on the balancing provision in most cases.

Third, a company may process personal data for behavioural targeting if people give their "unambiguous consent".[68] As companies can rarely rely on a contract or on the balancing provision, in most circumstances the only possible ground to legitimise the processing of personal data for behavioural targeting is unambiguous consent. The Working Party and several authors agree on this.[69] Consent is defined as "any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed."[70] Data subjects can always withdraw their consent; in such cases the company must stop processing of the data.[71] Sensitive personal data, such as medical data, can only be processed for marketing after a data subject has given her "explicit consent". Member states can also choose not to allow the processing of sensitive data based on consent.[72]

The Working Party has elaborated on the requirements for consent.[73] Consent must be freely given, so consent given under pressure isn't valid. As consent has to be specific, consent 'to use personal data for commercial purposes' wouldn't be acceptable. In line with the transparency principle, consent has to be informed. Companies shouldn't hide relevant information in the fine print of a privacy policy.

In principle, consent can be given implicitly, but inactivity is almost never an indication of one's wishes. Case law of the European Court of Justice confirms that mere silence doesn't signify consent.[74] Likewise, in general contract law, mere silence

---

[66] Article 29 Working Party, 'Opinion 03/2013 on Purpose Limitation (WP 203), 2 April 2013, 46.

[67] Information Commissioner's Office. 'Personal Information Online Code of Practice' (July 2010) <www.ico.gov.uk/~/media/documents/library/data_protection/detailed_specialist_guides/personal_information_online_cop.pdf> accessed on 2 February 2013, 22.

[68] Article 7(a) of the Data Protection Directive.

[69] See e.g. Traung P, 'EU Law on Spyware, Web Bugs, Cookies, etc. Revisited: Article 5 of the Directive on Privacy and Electronic Communications' (2010) 31 Business Law Review 216. Antic says that the processing of personal data for behavioural targeting can only be based on consent, but also argues that behavioural targeting often doesn't entail the processing of personal data (Antic M, 'De Nieuwe Cookieregels, Onduidelijk, Onjuist en Ineffectief [The New Cookie Rules: Unclear, Incorrect, and Ineffective]' (2012)(2) Ars Aequi 103).

[70] Article 2(h) of the Data Protection Directive.

[71] Kotschy W, 'Directive 95/46' in Büllesbach A and others (eds), *Concise European IT Law (second edition)* (Kluwer Law International 2010), 56.

[72] Article 8(2)(a) of the Data Protection Directive.

[73] Article 29 Working Party, 'Opinion 15/2011 on the Definition of Consent' (WP 187), 13 July 2011.

[74] The Court of Justice of the European Union has discussed the requirements for consent on many occasions. For

doesn't constitute an indication of will. "Silence or inactivity does not in itself amount to acceptance", says the Vienna Sales Convention. Several international texts on contract law use a similar phrase.[75] In sum, in most circumstances companies can only lawfully process personal data for behavioural targeting after the unambiguous consent of the data subject.

Consent in data protection law can be seen as an instrument to promote control of data subjects over their data. While data protection law doesn't give people full control over data concerning them, it's deeply influenced by the notion of privacy as control over personal information.[76] Transparency is a precondition for data subjects to have some control over how their personal data are used.

The Data Protection Directive doesn't allow the data subject to waive the other data protection rules.[77] For instance, the following declaration wouldn't be enforceable.

> I hereby consent to the use of my personal data in every way you see fit, and I waive all my rights under the data protection regime, including, but not limited to, my right to seek redress when you experience a data breach, and my rights to access, correction and erasure. This waiver is also valid to whomever you sell my data to.

Hence, even when a company may process personal data based on the consent of the data subject, the data subject should still be protected by data protection law's requirements.

Obtaining consent of a data subject should be distinguished from data protection law's transparency obligations. From a European legal perspective, the reason website publishers post privacy policies can be found in the Data Protection Directive. Article

---

instance, in a trademark case the Court says "implied consent (…) cannot be inferred from (…) mere silence" (ECJ, 20 November 2001, C-414/99 to C-416/99 (Zino Davidoff), par. 55). The Court sets the bar for consent at least as high in data protection cases. The Court says that merely informing somebody that data processing will take place "thus does not seek to base the personal data processing (…) on the consent" of the data subject (CJU, 9 November 2010, C-92/09 and C-93/09 (Volker und Markus Schecke), par. 63). See also the opinion of the Advocate General (17 June 2010, C-92/09 and C-93/09 (Volker und Markus Schecke), par 79). See for more case law on consent: Traung P, 'The Proposed New EU General Data Protection Regulation: Further Opportunities' (2012)(2) Computer Law Review international 33, 38-39, note 48.

[75] See e.g. article 18(1) of the Vienna Convention on international sale of goods: "A statement made by or other conduct of the offeree indicating assent to an offer is an acceptance. Silence or inactivity does not in itself amount to acceptance." The same phrase is used in article II. 4:204(2) of the Draft Common Frame of Reference (Principles, Definitions and Model Rules of European Private Law), and article 34 (of Annex 1) of European Commission. 'Proposal for a regulation of the European Parliament and of the Council on a Common European Sales Law (COM(2011) 635 final)'.

[76] Bennett CJ, *Regulating Privacy: Data Protection and Public Policy in Europe and the United States* (Cornell University Press 1992), 153-154.

[77] De Hert P and Gutwirth S, 'Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power' in Claes E, Duff A and Gutwirth S (eds), *Privacy and the criminal law* (Intersentia 2006), 68, note 19; Article 29 Working Party, 'Opinion 15/2011 on the Definition of Consent' (WP 187), 13 July 2011, 7. Some authors argue that it would be better if more rules could be waived. See e.g. Cuijpers C, 'A Private Law Approach to Privacy; Mandatory Law Obliged?' (2007) 4(4) SCRIPT-ed.; See for a critique of Cuijpers' article: Purtova N, *Property Rights in Personal Data* (Information Law Series, Kluwer Law International 2012), 207-220

10 and 11 require a company to provide at least information regarding its identity and the purposes of the processing, and more information when this is necessary to guarantee fair processing.

A privacy policy can be defined as follows (adapted from Verhelst): an instrument which the data controller can use to comply with his obligation to provide information pursuant to article 10 and 11 of the Data Protection Directive.[78] A privacy policy should thus contain a factual description of what a company does with personal data. Companies must always be transparent about the processing of personal data, regardless of whether they rely on consent or not.

In practice, many companies don't ask prior consent from European internet users for behavioural targeting. How is this possible? First, some companies may believe that data protection law doesn't apply. They might assume that they don't process personal data, if they don't process "personally identifiable information", such as a name, email address or social security number.[79] Second, enforcement of the law is insufficient. Data Protection Authorities don't have enough manpower to enforce the law against all wrongdoers. Enforcement is hard because many behavioural targeting companies are based outside the European Union. And until a few years ago behavioural targeting happened largely below the radar.

In sum, companies can rely on a contract, the balancing provision, or on unambiguous consent for the processing of personal data. But in the case of behavioural targeting, companies are usually required to obtain the data subject's consent. Apart from that: if a company could rely on a contract or on the balancing provision, the practical problems regarding informed consent that are described later in this paper would remain relevant. Moreover, we will see in the next section that the e-Privacy Directive requires consent for most tracking technologies for behavioural targeting.

2.4 The e-Privacy Directive and consent

The European Union has a separate directive for the protection of privacy and personal data in the electronic communications sector. Since 2009 this e-Privacy Directive requires companies to obtain consent of the internet user before they use tracking technologies such as cookies. This rule should have been implemented in national legislation by May 2011.[80] For ease of reading this paper speaks of 'cookies',

[78] His definition is as follows: "A privacy statement is an instrument which the data controller can use to comply with his obligation to provide information pursuant to Articles 33 and 34 Wbp [Dutch Data Protection Act]. The data controller can formalise the content and therefore the implementation of the obligation to provide information by means of this privacy policy." Verhelst EW, *Recht Doen aan Privacyverklaringen: een Juridische Analyse van Privacyverklaringen op Internet [A Legal Analysis of Privacy Policies on the Internet]* (Ph.D thesis University of Tilburg) (Academic version 2012), 244.

[79] See on the American concept of "personally identifiable information": Schwartz PM and Solove DJ, 'The PII Problem: Privacy and a New Concept of Personally Identifiable Information' (2011) 86 New York University Law Review 1814.

[80] Article 4(1) of the Citizens' Rights Directive (2009/136/EC).

but the provision is technology neutral, and applies to anyone that wants to store or access information in the device of an internet user. This rule also applies if a company doesn't process personal data.[81]

The general rule can be summarised as follows. Companies that want to store or access a cookie on a user's device must (a) give the user clear and complete information about the purposes of the cookie, and (b) obtain consent of the user. Certain functional cookies are exempted from the consent requirement.[82] For example, no consent is needed for a cookie for a digital shopping cart.

For the definition of consent, the e-Privacy Directive refers to the definition in the Data Protection Directive: a free, informed, specific indication of one's will. It's somewhat unclear what "free" consent means in this context. Some websites use a "tracking wall", or "cookie wall", and deny entrance to visitors that don't accept third party tracking cookies. One could question whether a user gives "free" consent in such cases.[83] But the e-Privacy Directive's preamble says that "[a]ccess to specific website content may still be made conditional on the well-informed acceptance of a cookie or similar device, if it is used for a legitimate purpose."[84] It's unclear whether the European lawmaker foresaw that some website publishers would block visitors that don't accept third party tracking cookies.[85]

It could be argued that in some cases cookie walls render consent not sufficiently free. For instance, the Dutch Data Protection Authority says that the Dutch public broadcaster isn't allowed to use a tracking wall.[86] Because people can only obtain certain information online from the public broadcaster, it has a "situational monopoly", thereby making consent involuntary.[87] But such a situation seems exceptional. If there are alternative service providers, data protection law probably allows companies to make the use of a service dependant on the acceptance of tracking cookies, if they clearly explain this.[88]

---

[81] Article 29 Working Party, 'Opinion 2/2010 on Online Behavioural Advertising' (WP 171), 22 June 2010, 9.

[82] Article 5.3 of the e-Privacy Directive (Directive 2002/58/EC, amended by the Citizens' Rights Directive (2009/136/EC), consolidated version).

[83] Kosta E, *Consent in European Data Protection Law (Ph.D thesis University of Leuven)* (Martinus Nijhoff 2013), 321. "The intuitive answer would be that in such a case the user does not have a real choice, thus the consent is not freely given. However, the explicit reference on the conditionality of access in Recital 25 complicates the situation."

[84] Recital 25 of the e-Privacy Directive.

[85] Recital 25 also says that "so-called 'cookies', can be a legitimate and useful tool, for example, in analysing the effectiveness of website design and advertising." This would suggest that tracking cookies might be legitimate cookies in the lawmaker's opinion.

[86] See about the Dutch tracking walls: Helberger N, 'Freedom of expression and the Dutch cookie-wall', conference paper MIT 8 Public Media Private Media Conference, Boston, 3-5 May 2013, <www.ivir.nl/publications/helberger/Paper_Freedom_of_expression.pdf> accessed on 20 July 2013.

[87] College Bescherming Persoonsgegevens [Dutch Data Protection Authority]. 'Brief aan de staatssecretaris van Onderwijs, Cultuur en Wetenschap, over beantwoording Kamervragen i.v.m. cookiebeleid [Letter to the State Secretary of Education, Culture and Science, on answers to parliamentary questions about cookie policy]' (31 January 2013) <www.cbpweb.nl/downloads_med/med_20130205-cookies-npo.pdf> accessed on 4 February 2013.

[88] See Kosta E, Consent in European Data Protection Law (Ph.D thesis University of Leuven) (Martinus Nijhoff 2013), 256, 312.

A company must at least explain the purpose of the cookie. The information provided to users must be "clear and comprehensive", and must be in accordance with the Data Protection Directive, which requires more information if this is necessary to guarantee fair processing.[89] The Working Party gives several examples of how a website publisher could obtain consent, including a pop-up window.[90]

To summarise, companies that place tracking cookies have to ask consent of the internet user. But a sentence from recital 66 of the amending directive has caused much confusion and discussion:

> Where it is technically possible and effective, in accordance with the relevant provisions of [the Data Protection Directive], the user's consent to processing may be expressed by using the appropriate settings of a browser or other application.

Most browsers offer users the possibility to block first party cookies, third party cookies, or all cookies.[91] Some conclude from recital 66 that *default* browser settings could express consent for tracking cookies, perhaps because the e-Privacy Directive doesn't require consent to be "unambiguous".[92] These opposite views have led to much debate.

However, people that don't tweak their browser may be unaware of accepting tracking cookies. Therefore it's hard to see how there could be consent. The Working Party says: "consent based on the lack of individuals' action, for example, through pre-ticked boxes, does not meet the requirements of valid consent under the [Data Protection Directive]. The same conclusion applies to browser settings which would accept by default the targeting of the user (through the use of cookies)."[93]

Regulators and commentators in the United Kingdom seem to be more inclined to accept a system that allows people to object – an opt-out system – as a way to obtain "implied" consent.[94] For instance, the English Information Commissioner's Office (ICO), the regulator that oversees compliance with the e-Privacy Directive, drops cookies through its website as soon as a visitor arrives, and explains in a banner that it

---

[89] Article 5.3 of the e-Privacy Directive; article 10 and 11 of the Data Protection Directive.

[90] Article 29 Working Party, 'Opinion 16/2011 on EASA/IAB Best Practice Recommendation on Online Behavioural Advertising' (WP 188), 8 December 2011, 9-11.

[91] A web browser is software to browse the web, such as Chrome, Firefox, Internet Explorer, or Safari.

[92] The Interactive Advertising Bureau United Kingdom says: "We believe that default web browser settings can amount to 'consent' (…)" (emphasis original) (Interactive Advertising Bureau United Kingdom, 'Department for Business, Innovation & Skills consultation on implementing the revised EU electronic communications framework, IAB UK Response' (1 December 2012) <www.iabuk.net/sites/default/files/IABUKresponsetoBISconsultationonimplementingtherevisedEUElectronicCommunicationsFramework_7427_0.pdf> accessed on 10 April 2013).

[93] Article 29 Working Party, 'Opinion 15/2011 on the Definition of Consent' (WP 187), 13 July 2011, 32.

[94] Kosta E, *Consent in European Data Protection Law (Ph.D thesis University of Leuven)* (Martinus Nijhoff 2013), 192.

did. The ICO seems to suggest that explaining how a user can delete cookies is enough to obtain "implied consent".[95]

The English view of an opt-out system as sufficient to obtain consent has been met with criticism in literature.[96] According to Kosta for instance, "there is no such thing as 'opt-out consent'".[97] She adds: "reference to 'opt-out' consent is a misnomer. An 'opt-out' regime refers to the right of a data subject to object to the processing of his personal data and does not constitute consent."[98]

A number of larger behavioural targeting companies offer people the chance to opt out of targeted advertising. Many of those companies stop showing targeted advertising after people object, but continue to track people.[99] Whatever the results of objecting are, it's hard to see how such a system could meet data protection law's requirements for consent.

Member states of the European Union should have implemented the e-Privacy Directive in their national laws by May 2011, but many member states missed this deadline. The consent requirement for tracking cookies isn't widely enforced yet, among other reasons because the national laws implementing the consent rule are rather new. Discussions about a Do Not Track standard may have delayed enforcement as well (more on this in the next section). It's unclear how the e-Privacy Directive will be applied in the European Union member states. The approaches seem to vary. For instance, the United Kingdom appears to accept a kind of opt-out system. The Netherlands requires unambiguous consent for tracking cookies (an opt-in system).[100]

The interplay between the consent requirements from the e-Privacy Directive and the Data Protection Directive is somewhat complicated. An analysis of the Data Protection Directive suggests that companies that process personal data for

---

[95] The banner says: "We have placed cookies on your computer to help make this website better. You can change your cookie settings at any time. Otherwise, we'll assume you're OK to continue" (Information Commissioner's Office. 'Changes to Cookies on Our Website' (31 January 2013) <www.ico.org.uk/news/current_topics/changes-to-cookies-on-our-website> accessed on 5 April 2013).

[96] See e.g. Traung P, 'The Proposed New EU General Data Protection Regulation: Further Opportunities' (2012)(2) Computer Law Review international 33, 38; McStay A, 'I consent: An analysis of the Cookie Directive and its implications for UK behavioral advertising' (2012) New Media & Society, 1.

[97] Kosta E, *Consent in European Data Protection Law (Ph.D thesis University of Leuven)* (Martinus Nijhoff 2013), 202.

[98] Idem, 387.

[99] For example, the opt-out page of the Internet Advertising Bureau says: "Declining behavioral advertising only means that you will not receive more display advertising customised in this way" (Interactive Advertising Bureau Europe, 'Your Online Choices. A Guide to Online Behavioural Advertising. FAQ # 22.' <www.youronlinechoices.com/ma/faqs#22> accessed on 10 April 2013. See also Komanduri S and others, 'AdChoices? Compliance with Online Behavioral Advertising Notice and Choice Requirements' (2011) 7 I/S: A Journal of Law & Policy for the Information Society 603.

[100] Article 11.7a of the Dutch Telecommunications Act (version 1 January 2013). See for a translation of the provision: Zuiderveen Borgesius, FJ, 'Behavioral Targeting. Legal Developments in Europe and the Netherlands (position paper for W3C Workshop: Do Not Track and Beyond)' (2012) <www.w3.org/2012/dnt-ws/position-papers/24.pdf> accessed on 7 April 2013, 5.

behavioural targeting have to obtain prior "unambiguous consent" of the internet user in most cases. Apart from this requirement, the e-Privacy Directive requires consent for tracking cookies, whether personal data are processed or not. The Working Party suggests that a company doesn't need separate consent for the processing of personal data, if it obtained proper consent for a tracking cookie.[101] For ease of reading the rest of this paper sometimes speaks of 'consent', without specifying whether it concerns consent in the sense of the e-Privacy Directive or the Data Protection Directive.

In sum, the e-Privacy Directive requires companies to obtain informed consent of the internet user for most tracking technologies for behavioural targeting. How consent should obtained is contentious. Even if consent to tracking technologies could be given by mere silence (quod non), the Data Protection Directive would still require unambiguous consent for behavioural targeting in most cases.

2.5 Do Not Track

Since September 2011, a Tracking Protection Working Group of the World Wide Web Consortium has been engaged in a discussion about a Do Not Track standard.[102] The Consortium is an international community where member organisations cooperate to develop web standards.[103]

Euro Commissioner Kroes has suggested that a Do Not Track system could enable companies to comply with the e-Privacy Directive's consent requirement.[104] A Do Not Track option should allow people to use their browser to signal to websites that they don't want to be tracked. It's a system to opt out of certain kinds of tracking.

It's not immediately apparent how Do Not Track – an opt-out system – could help companies to comply with the e-Privacy Directive's consent rule. But perhaps an arrangement along the following lines would be possible. Companies should refrain from tracking European internet users that haven't set a Do Not Track preference. If somebody signals to a specific company 'Yes, You Can Track Me' after receiving sufficient information, that company may place a cookie to track that user. Hence, in Europe not setting a preference would have the same effect as setting a preference for 'Do Not Track Me'. In other words, in Europe Do Not Track would be an opt-in system. In countries without a data protection law, such as the United States, companies might be free to track people that don't set a Do Not Track preference.[105] It would thus be an opt-out system in the United States.

---

[101] Article 29 Working Party, 'Opinion 2/2010 on Online Behavioural Advertising' (WP 171), 22 June 2010, p 16.
[102] W3C Tracking Protection Working Group <www.w3.org/2011/tracking-protection> accessed on 7 April 2013.
[103] W3C, About W3C <www.w3.org/Consortium> accessed on 7 April 2013.
[104] Kroes, N, 'Reinforcing Trust and Confidence (speech/11/461), Online Tracking Protection & Browsers Workshop Brussels ' (22 June 2011) <http://europa.eu/rapid/press-release_SPEECH-11-461_en.htm> accessed on 7 April 2013.
[105] See the discussion on the public mailing list of the Do Not Track Working Group of the World Wide Web consortium: <http://lists.w3.org/Archives/Public/public-tracking/> accessed 7 April 2013.

The proposals for a Do Not Track standard exclude tracking within one website. Therefore, the standard would allow companies like Amazon or Facebook to analyse people's behaviour within their own website, even if people signal 'Do Not Track Me'. In contrast, the e-Privacy Directive's consent rule also applies to first party tracking cookies.

One of the main points of disagreement is whether Do Not Track means 'Do Not Collect' (and therefore, not use any tracking technologies) or merely 'Do Not Target' (continue the use of tracking technologies without showing targeted advertisements to users). Another point of discussion is whether a browser that is set to 'Do Not Track Me' by default should be respected. Some companies suggest that default Do Not Track signals don't express a user's choice, and could thus be ignored.[106] At the time of writing the Tracking Protection Working Group hasn't reached consensus.[107]

To sum up, the e-Privacy Directive requires consent for tracking technologies that are used for behavioural targeting. This rule is currently not widely enforced yet, among other reasons because some hope that a Do Not Track standard could make it possible to comply with the consent requirements. The following sections analyse certain problems with informed consent.

3. Economics of privacy

3.1 Law and economics

This section briefly introduces law and economics, described by Posner as the "economic analysis of legal rules and institutions".[108] Economics can be defined as "the science which studies human behaviour as a relationship between ends and scarce means which have alternative uses."[109]

---

[106] For instance, Yahoo said it would ignore the Do Not Track signals from Microsoft Internet Explorer if those were set by default. (Yahoo! Public Policy Blog, 'In Support of a Personalized User Experience' (26 October 2012) <www.ypolicyblog.com/policyblog/2012/10/26/dnt/> accessed on 10 April 2013).

[107] See for a history of the Do Not Track Working Group and an overview of some of the main disagreements: Schunter, M, & Swire, P, 'Explanatory Memorandum for Working Group Decision on "What Base Text to Use for the Do Not Track Compliance Specification"', 16 July 2013, <http://lists.w3.org/Archives/Public/public-tracking/2013Jul/att-0395/Explanatory_memorandum.as_issued.pdf> accessed on 26 July 2013.

[108] Posner RA, *Economic Analysis of Law* (Aspen/Wolters Kluwer 2010), xxi. This paper uses the phrases "economic analysis of law" over "law and economics" interchangeably. Some authors prefer the phrase 'economic analysis of law'. Kornhauser L, 'The Economic Analysis of Law' in Zalta, Edward N. (ed), The Stanford Encyclopedia of Philosophy (Fall 2011 Edition) <http://plato.stanford.edu/archives/fall2011/entries/legal-econanalysis> accessed 5 April 2013).

[109] Robbins L, *An Essay on the Nature and Significance of Economic Science* (The Mises Institute 2007 (facsimile of 1932 edition)), 15.

In economics, it's usually assumed that parties want to maximise their own welfare, or their own utility. For example, a company maximises profit. Welfare concerns not only money or things that are usually given a monetary value. A consumer maximises utility, which may include happiness, satisfaction, psychological well-being, and privacy.[110] Economics concerns the question of how parties make decisions when trying to maximise their preferences, with the limited means at their disposal.

In economics, rational choice theory is often used to predict human behaviour. Rational choice theory analyses behaviour assuming that people generally want to maximise their utility, and that people are able to choose the best way to maximise their utility. In short, it's assumed that people act "rationally" on average. Kahneman summarises: "[r]ational agents are expected to know their tastes, both present and future, and they are supposed to make good decisions that will maximize their interests."[111]

Rational choice theory is a tool to predict human behaviour and doesn't aim to fully describe reality.[112] Rational choice theory doesn't imply that people always maximise their utility, or that people always act rationally. But the theory can still be used to predict human behaviour, and to reflect on how to regulate behaviour.[113] For example, say a lawmaker raises the fines for speeding to deter people from driving too fast. The lawmaker assumes that people weigh the benefit of quick arrival against the potential cost of paying a fine. Even though some people might still drive too fast, on average the measure could lead to less speeding.

Law and economics often analyses which rule leads to the highest aggregate welfare for society. In economics, it's often assumed that a (hypothetical) perfectly functioning free market would lead to the highest aggregate welfare, if there are no market failures such as externalities, monopoly, or information asymmetry. The assumption is thus that private exchanges lead to the highest social welfare. People are assumed to enter contracts only when they expect to gain something from it, because they maximise their expected utility. In theory, unrestricted trade in a market without market failures leads to the highest aggregate welfare. Therefore economists are sometimes sceptical of laws that interfere with the free market, or that interfere with freedom of contract.[114]

In reality, the ideal type of a perfectly functioning free market is rare. When the market doesn't function as it ideally should, there may be reason for the lawmaker to intervene from an economic perspective. Examples of problems with the market are

---

[110] Cooter R and Ulen T, *Law & Economics (6th edition)* (Addison-Wesley 2012), 12.
[111] Kahneman D, *Thinking, Fast and Slow* (Allen Lane/Pinguin 2011), 98.
[112] Posner RA, *Economic Analysis of Law* (Aspen/Wolters Kluwer 2010), 4.
[113] Posner RA, 'Rational Choice, Behavioral Economics, and the Law' (1998) 50(5) Stanford Law Review,1551.
[114] Trebilcock MJ, *The Limits of Freedom of Contract* (Harvard University Press 1997 (paperback)), 7; Hermalin BE, Katz AW and Craswell R, 'Contract Law' in Polinsky, AM and Shavell S (eds), *Handbook of law and economics* (North Holland (Elsevier) 2007), 24.

externalities, information symmetries and transaction costs. Such problems, or market failures, are discussed in section 4.4.[115]

Sometimes the law implicitly seems to be based on a kind of rational choice model. Put differently, sometimes the law appears to assume that people make choices in their own best interests, as long as they have enough information to base their decisions on.[116] In Europe for instance, contractual freedom, or party autonomy, is often seen as the basis of contract law. Grundmann summarises: "party autonomy dominates and the limits are seen as exceptions."[117] (The exceptions are many, for example to protect consumers or employees.) The notion of "informed consent" in data protection law also seems to be based on the idea that data subject make "rational" choices.

3.2 The economics of privacy

This section introduces the economic analysis of privacy.[118] Economic theory can be used to analyse aspects of people's choices regarding privacy. One of the leading scholars in the economics of privacy is Acquisti. He explains: "the economics of privacy attempts to understand, and sometimes measure, the trade-offs associated with the protection or revelation of personal information."[119] Some of his main conclusions are summarised below.

An example of a trade-off is the use of an unpaid email service. Many email services analyse the contents of messages for targeted advertising. The user thus discloses personal data (a cost) to gain utility: the use of a "free" service. Social network sites often offer a similar exchange. For instance, people don't pay with money for Facebook, which in turn analyses their behaviour for marketing. Another example is

[115] Market failure is "[a] general term describing situations in which market outcomes are not Pareto efficient" (Organisation for Economic Co-operation and Development. 'Glossary of Industrial Organisation Economics and Competition Law' (1993) <www.oecd.org/regreform/sectors/2376087.pdf> accessed on 12 March 2013).

[116] Ben-Shahar O and Schneider C, 'The Failure of Mandated Disclosure' (2011) 159 University of Pennsylvania Law Review 647, 650. Sunstein & Thaler say: "Whether or not they have ever studied economics, many people seem at least implicitly committed to the idea of homo economicus, or economic man – the notion that each of us thinks and chooses unfailingly well, and thus fits within the textbook picture of human beings offered by economists." Sunstein CR and Thaler RH, Nudge: Improving Decisions about Health, Wealth, and Happiness (Yale University Press 2008), 6.

[117] Grundmann S, 'Information, Party Autonomy and Economic Agents in European Contract Law' (2002) 39 Common Market Law Review 269, 271. See also article II – 1:102 of the Draft Common Frame of Reference, which contains the principle of contractual freedom: "Parties are free to make a contract or other juridical act and to determine its contents, subject to any applicable mandatory rules."

[118] See for an overview of the field of the economics of privacy: Acquisti A, 'The Economics of Personal Data and the Economics of Privacy (preliminary draft)' (2010) <www.heinz.cmu.edu/~acquisti/papers/acquisti-privacy-OECD-22-11-10.pdf> accessed on 4 February 2013; Acquisti A and Brandimarte L, 'The Economics of Privacy' in Peitz M and Waldfogel J (eds), *The Oxford handbook of the digital economy* (Oxford University Press 2012); Hui K and Png IPL, 'The Economics of Privacy' in Hendershott T (ed), *Handbook on Economics and Information Systems*, *Volume 1* (Elsevier 2006).

[119] Acquisti A, 'From the Economics to the Behavioral Economics of Privacy: a Note' (2010) 6005 Third International Conference on Ethics and Policy of Biometrics and International Data Sharing, ICEB 2010, Hong Kong, January 4-5 (Ethics and Policy of Biometrics) 23, 23.

joining a loyalty card program of a supermarket. For an economic viewpoint, customers "trade" personal data, like their name and information about their shopping habits, for discounts.[120]

Whether people realise that they pay with their personal data is another matter. Acquisti notes that trade-offs can exist, even when people don't realise that they "pay" with their data: "the existence of such trade-offs does not imply that the economic agents are always aware of them as they take decisions that will impact their privacy."[121]

The paper doesn't aim to answer the question of whether behavioural targeting leads to a net loss or a net benefit for society. Neither economic theory nor empirical economic research has provided a definite answer to the question of whether behavioural targeting – or a law that limits behavioural targeting – leads to more or less social welfare in the aggregate. Some economists say that legal protection of personal data is good, but others argue the opposite. "Economic theory", concludes Acquisti, "has brought forward arguments both supporting the view that privacy protection *increases* economic efficiency, and that it *decreases* it."[122] Empirical economic research doesn't arrive at definitive conclusions either. Acquisti says "it would be futile to attempt comparing the aggregate values of personal data and privacy protection, in search of a 'final' economic assessment of whether we need more, or less, privacy protection."[123]

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

Some say that legal protection of privacy reduces social welfare, because it limits data flows. For example, behavioural targeting has benefits from an economic viewpoint, for companies and internet users. Behavioural targeting leads to profit for many companies. Internet users can benefit when revenue from targeted advertising is used to fund "free" internet services. (However, in the end, consumers might pay for this advertising, if companies pass on the advertising costs in product prices.) Behaviourally targeted advertising can bring products under the consumers' attention, which could save them searching costs. But it's difficult to calculate the total benefits of behavioural targeting.[124]

---

[120] Acquisti A and Brandimarte L, 'The Economics of Privacy' in Peitz M and Waldfogel J (eds), *The Oxford handbook of the digital economy* (Oxford University Press 2012), 548.
[121] Acquisti A, 'The Economics of Personal Data and the Economics of Privacy (preliminary draft)' (2010) <www.heinz.cmu.edu/~acquisti/papers/acquisti-privacy-OECD-22-11-10.pdf> accessed on 4 February 2013, 4.
[122] Idem, 34 (emphasis original).
[123] Idem, 42
[124] Idem, 42

Likewise, aggregating all costs of behavioural targeting is hard, or even impossible. Costs for companies include money spent on data processing systems. Furthermore, some estimate that billions of dollars are lost, because people would engage in more online consumption if they'd feel their privacy was better protected.[125] The European Commission says it would be good for the market if people worried less about their privacy. "Lack of trust makes consumers hesitate to buy online and adopt new services."[126]

Not protecting personal data can bring costs for data subjects. Some privacy-related costs could be calculated, at least in theory. For example, when a company experiences a data breach, the leaked data could lead to identity fraud. Such costs could materialise years after the data are collected. Or if somebody's email address is disclosed too widely, this could lead to receiving spam. The time it takes to clean one's inbox is a cost.[127] Other privacy-related costs are harder, perhaps impossible, to quantify. Such costs include annoyance and a creepy feeling. In sum, the costs of privacy infringements may only become clear after years, it's difficult to agree on which costs to count, and many privacy-related costs are impossible to quantify.

To conclude, it's unclear whether behavioural targeting leads to a net benefit or a net loss for society from an economic perspective. Likewise, whether more legal protection of personal data would lead to more or less social welfare is unknown. Hence, economic research alone doesn't dictate the ideal level of protection. As Acquisti puts it, "it may not be possible to resolve this debate using purely economic tools."[128] But economic theory can still be helpful to analyse certain problems with informed consent to behavioural targeting.

3.3 Limits of economic analysis of privacy

Law and economics and behavioural law and economics provide useful analytical tools to analyse certain practical problems with informed consent to data processing. But economic analysis has is limits, especially when discussing fundamental rights like in this study. "Evidently there is more to justice than economics", notes Posner.

---

[125] Idem, 21.

[126] European Commission, 'Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012) 11 final)', 1. See also recital 5 of the e-Privacy Directive.

[127] Acquisti A and Brandimarte L, 'The Economics of Privacy' in Peitz M and Waldfogel J (eds), *The Oxford handbook of the digital economy* (Oxford University Press 2012), 556.

[128] Acquisti A, 'The Economics of Personal Data and the Economics of Privacy (preliminary draft)' (2010) <www.heinz.cmu.edu/~acquisti/papers/acquisti-privacy-OECD-22-11-10.pdf> accessed on 4 February 2013, 34.

> But there is more to notions of justice than a concern with efficiency. It is not obviously inefficient to allow suicide pacts; to allow private discrimination on racial, religious, or sexual grounds; to permit killing and eating the weakest passenger in the lifeboat in circumstances of genuine desperation, to force people to give self-incriminating testimony; to flog prisoners; to allow babies to be sold for adoption; to permit torture to extract information; to allow the use of deadly force in defense of a pure property interest; to legalize blackmail; or to give convicted felons a choice between imprisonment and participation in dangerous medical experiments. Yet all these things offend the sense of justice of modern Americans, and all are to a greater or lesser (usually greater) extent illegal. An effort will be made in this book to explain some of these prohibitions in economic terms, but many cannot be. Evidently, there is more to justice than economics, and this is a point the reader should keep in mind in evaluating normative statements in this book.[129]

Fairness, fundamental rights, and the function of privacy in a democratic society play a marginal in the economic analysis of privacy.[130] But such considerations are important. As Acquisti notes: "the value of privacy eventually goes beyond the realms of economic reasoning and cost benefit analysis, and ends up relating to one's views on society and freedom."[131] He warns for an "extremisation" of the debate. Too much attention to economics and trade-offs may take our attention away from privacy infringements that are harder to quantify.[132] Indeed, sometimes it's suggested that there's no need to regulate behavioural targeting because the "harm" is difficult to quantify in monetary terms.[133] European data protection law applies to the processing of personal data, whether there's (quantifiable) harm or not. The question of harm is relevant where data protection law requires the balancing of different interests.

In sum, the economic analysis of privacy provides useful insights but it has its limits. With that caveat, let's see what law and economics and behavioural law and economics have to offer.

---

[129] Posner RA, *Economic Analysis of Law* (Aspen/Wolters Kluwer 2010), 35. I don't suggest that Posner finds law and economics ill equipped to discuss privacy. Posner suggests that the protection of personal information is bad from an economic perspective. See Posner RA, 'The Right of Privacy' (1977) 12(3) Georgia Law Review 393.

[130] See for an amusing text on the difficulties of combining the viewpoints of an economic approach and a European data protection approach: Kang J and Buchner B, 'Privacy in Atlantis' (2004) 18(1) Harvard Journal of Law & Technology 229.

[131] Acquisti A, 'Privacy in Electronic Commerce and the Economics of Immediate Gratification' (2004) Proceedings of the 5th ACM Conference on Electronic Commerce, Association for Computing Machinery, New York 21, 27.

[132] Acquisti A, 'Opening Keynote at the Economics of Privacy Conference, Silicon Flatirons Center at the University of Colorado Law School' (2 December 2011) <http://siliconflatirons.com/events.php?id=1005> accessed on 15 February 2013.

[133] See e.g. Lenard TM and Rubin PH, 'In Defense of Data: Information and the Costs of Privacy' 2(1) Policy & Internet 143.

4. Informed consent and insights from economics

4.1 Introduction

This section analyses problems with informed consent through a law and economics lens. American legal scholars, such as Kang and Schwartz, have applied insights from law and economics to consent to online data processing.[134] Although consent plays a different role in American law than in European data protection law, some arguments from the American discussion are relevant for Europe too.

A basic starting point in economics is that contractual freedom is desirable, because completely free trade should lead to the highest social welfare. But there may be reason for government intervention in markets under rational choice theory. The possible grounds for limiting contractual freedom can be roughly divided in two categories. First, sometimes third parties suffer costs resulting from a contract: externalities. Second, sometimes contract parties have difficulties entering a contract in their best interests, because of information asymmetries or transaction costs for instance.[135] The section is structured as follows. Sections 4.2 - 4.5 discuss information asymmetries, transaction costs, externalities, and market power. Section 4.6 concludes.

4.2 Information asymmetries

Sometimes contract parties have difficulties entering in a contract in their own best interests. In business to consumer contracts, information symmetries are common. Information asymmetry describes "a situation where one party possesses information about a certain product characteristic and the other party does not."[136] Information asymmetries can lead to market failures. It's often said that one of the main goals of European consumer law is mitigating information asymmetry.[137]

---

[134] Kang J, 'Information Privacy in Cyberspace Transactions' (1997) 50(4) Stanford Law Review 1193; Schwartz PM, 'Property, Privacy, and Personal Data' (2003) 117(7) Harvard Law Review 2056.

[135] Hermalin BE, Katz AW and Craswell R, 'Contract Law' in Polinsky, AM and Shavell S (eds), *Handbook of law and economics* (North Holland (Elsevier) 2007), 30; Luth HA, *Behavioural Economics in Consumer Policy: The Economic Analysis of Standard Terms in Consumer Contracts Revisited* (Ph.D thesis University of Rotterdam) (Academic version 2010), 15.

[136] Luth HA, *Behavioural Economics in Consumer Policy: The Economic Analysis of Standard Terms in Consumer Contracts Revisited* (Ph.D thesis University of Rotterdam) (Academic version 2010), 23.

[137] See e.g. Luth HA, *Behavioural Economics in Consumer Policy: The Economic Analysis of Standard Terms in Consumer Contracts Revisited (Ph.D thesis University of Rotterdam)* (Academic version 2010), 15, 69; Howells G, 'The Potential and Limits of Consumer Empowerment by Information' (2005) 32(3) Journal of Law and Society 349, 352; Grundmann S, 'Information, Party Autonomy and Economic Agents in European Contract Law' (2002) 39 Common Market Law Review 269, 279.

Since the 1970s economists devote much attention to markets with asymmetric information, for example where consumers have difficulties evaluating the quality of products or services. Akerlof used the market for used cars as an example of a market with asymmetric information.[138] Suppose sellers offer bad cars ("lemons") and good cars. Sellers know whether they have a bad or a good car for sale, but buyers can't detect hidden defects. A rational buyer will offer the price corresponding to the average quality of all used cars on the market.

But this means that sellers of good cars are offered a price that is too low. Many owners of good cars will therefore not offer their cars for sale. The result is that the average quality of used cars on the market decreases. Buyers will therefore offer lower prices, and fewer people offer their cars for sale. The average quality of cars on the market will drop. In short, in a market characterised by asymmetric information about quality, sellers often don't compete on quality, leading to a "race to the bottom".[139] This can lead to products or services of low quality, or to markets driven out of existence.

Information asymmetries hamper meaningful consent to behavioural targeting. Internet users have less information about behavioural targeting than companies. Many companies track people for behavioural targeting without people being aware. But even if companies would ask people consent, information asymmetries would be a problem.

Few people are aware to what extent companies collect data about their online behaviour, and of the possible consequences. When one sees the release of personal data as payment for "free" services, it's clear that there are information asymmetries. To make an informed choice, people must realise they make a choice. As Cranor & McDonald put it, "people understand ads support free content, but do not believe data are part of the deal."[140] Therefore, the current state of affairs regarding behavioural targeting is characterised by large information asymmetries.[141]

Research suggests that most people are only vaguely aware of data collection for behavioural targeting. For instance, Ur et al. found in interviews that participants were "surprised to learn that browsing history is currently used to tailor advertisements".[142] Cranor & McDonald found in a survey that 86% of respondents were aware that

---

[138] Akerlof GA, 'The Market for "Lemons": Quality Uncertainty and the Market Mechanism' (1970) 84(3) Quarterly Journal of Economics 488.

[139] Grundmann S, 'Information, Party Autonomy and Economic Agents in European Contract Law' (2002) 39 Common Market Law Review 269, 279.

[140] McDonald, A. M. and L. F. Cranor. 'Beliefs and Behaviors: Internet Users' Understanding of Behavioral Advertising' (Telecommunications Policy Research Conference) (2 October 2010) <http://ssrn.com/abstract=1989092> accessed on 5 April 2013, 21.

[141] Acquisti A and Grossklags J, 'What Can Behavioral Economics Teach Us About Privacy?' in Acquisti A and others (eds), *Digital Privacy: Theory, Technologies and Practices* (Auerbach Publications, Taylor and Francis Group 2007).

[142] Ur B and others, 'Smart, Useful, Scary, Creepy: Perceptions of Online Behavioral Advertising' (Proceedings of the Eighth Symposium on Usable Privacy and Security ACM, 2012) 4, 4.

behavioural targeting happens. But they also find that people know little about how data are collected about their online behaviour: "it seems people do not understand how cookies work and where data flows."[143]

Furthermore, only 40% of respondents thought that providers of email services scan the contents of messages to serve targeted advertising. 29% thought this would never happen, because the law prohibits it, or because the consumer backlash would be too great. Almost half of Gmail users didn't know about the practice,[144] while Gmail has been doing this since 2004.[145] Research in Europe also suggests that many people are unaware of behavioural targeting.[146] In sum, internet users have incomplete information about behavioural targeting. Cranor & McDonald conclude that people generally lack the knowledge needed to make meaningful decisions about privacy and behavioural targeting.[147]

Information asymmetries are likely to persist, because technologies evolve.[148] For instance, companies use new tracking technologies. Therefore, deleting third party cookies may not be enough to avoid being tracked. For example, many companies used 'flash cookies' to re-install cookies that people deleted.[149] Hence, even people that learn how to defend themselves against tracking would have to update their knowledge constantly. Hoofnagle et al. summarise: "advertisers are making it impossible to avoid online tracking."[150]

But if companies asked consent before they collect data for behavioural targeting, information asymmetries would still be a problem. Acquisti discusses three categories of information asymmetries.[151] First, people don't know what will happen with their data. Will a company tie their name to the profile of their surfing behaviour? Will their data be shared with other companies? If a company goes bankrupt, will its database be sold to the highest bidder?[152] Moreover, it's hard to foresee how data will

---

[143] McDonald AM. and Cranor LF, 'Beliefs and Behaviors: Internet Users' Understanding of Behavioral Advertising' (Telecommunications Policy Research Conference) (2 October 2010) <http://ssrn.com/abstract=1989092> accessed on 5 April 2013, 16.

[144] Idem, 21.

[145] Battelle J, *The Search. How Google and its rivals rewrote the rules of business and transformed our culture* (Penguin Group 2005), chapter 8.

[146] Helberger N and others, 'Online Tracking: Questioning the Power of Informed Consent' (2012) 14(5) Info 57, 70.

[147] Idem, 27.

[148] Acquisti and Grossklags make a similar point, but give other examples. Acquisti A and Grossklags J, 'What Can Behavioral Economics Teach Us About Privacy?' in Acquisti A and others (eds), *Digital Privacy: Theory, Technologies and Practices* (Auerbach Publications, Taylor and Francis Group 2007), 367.

[149] Soltani A and others, 'Flash Cookies and Privacy' (10 August 2009) <http://ssrn.com/abstract=1446862> accessed 10 April 2013.

[150] Hoofnagle CJ and others, 'Behavioral Advertising: The Offer You Cannot Refuse' (2012) 6(2) Harvard Law & Policy Review 273, 273.

[151] Acquisti A, 'The Economics of Personal Data and the Economics of Privacy (preliminary draft)' (2010) <www.heinz.cmu.edu/~acquisti/papers/acquisti-privacy-OECD-22-11-10.pdf> accessed on 4 February 2013, 38. Acquisti doesn't explicitly present these three categories.

[152] See e.g. the Toysmart case in the United States (In re Toysmart.com, LLC, Case no. 00-13995-CJK, in the United States Bankruptcy Court for the District of Massachusetts), and the Broadcast Press case in the Netherlands (Voorzieningenrechter Rechtbank Amsterdam, 12 February 2004, LJN: AO3649).

be shared among companies. The system of companies involved in behavioural targeting is complicated.

Second, even if people knew what companies do with their data, it would be hard to predict the consequences.[153] If a company shares data with another company, will the data be used for price discrimination? Will visits to a website with medical information lead to higher health insurance costs? If there's a data breach at a company, will this lead to identity fraud?

A third reason that people have limited information to base their decisions on, is that it's hard for people to attach a monetary value to their online behaviour. One of the transacting parties thus rarely knows how much she "pays".[154] For instance, people might not know the possible costs of a privacy infringement. "To what, then," asks Acquisti, "is the subject supposed to anchor the valuation of her personal data and its protection?"[155] In sum, information asymmetries are a problem in the context of consent to behavioural targeting.

If one would see the privacy-friendliness of websites as a product feature, the world wide web has some characteristics of a lemons market.[156] People have difficulties judging the privacy-friendliness of websites, and website publishers rarely use privacy as a competitive advantage. Almost all popular websites allow third parties to track their visitors. Some authors suggest a similar effect with regard to standard contracts for consumers. As consumers don't read standard contracts, companies don't compete on the quality of their terms. This can lead to contracts that are unfavourable to consumers.[157]

A hypothetical fully rational person would know how to deal with information asymmetry and uncertainty. For instance, she could base her decision on what happens to people's personal data on average. And in a lemons situation she wouldn't be optimistic about the quality. But section 6 shows that this isn't how people tend to deal with information asymmetry.

---

[153] Acquisti A and Grossklags J, 'What Can Behavioral Economics Teach Us About Privacy?' in Acquisti A and others (eds), *Digital Privacy: Theory, Technologies and Practices* (Auerbach Publications, Taylor and Francis Group 2007), 365.

[154] See also: Hoofnagle CJ and Whittington JM, 'The Price of 'Free': Accounting for the Cost of the Internet's Most Popular Price (Forthcoming (2014) UCLA Law Review 61(3))' <http://ssrn.com/abstract=2235962> accessed on 5 April 2013.

[155] Acquisti A, 'The Economics of Personal Data and the Economics of Privacy (preliminary draft)' (2010) <www.heinz.cmu.edu/~acquisti/papers/acquisti-privacy-OECD-22-11-10.pdf> accessed on 4 February 2013, 39.

[156] See Vila T, Greenstadt R and Molnar D, 'Why We Can't be Bothered to Read Privacy Policies. Models of Privacy Economics as a Lemons Market.' in Camp, L. J. and S. Lewis (eds), *Economics of Information Security* (Springer 2004).

[157] See e.g.: Faure MG and Luth HA, 'Behavioural Economics in Unfair Contract Terms. Cautions and Considerations' (2011) 34(3) Journal of Consumer Policy 337, 342; Wagner G, 'Mandatory Contract Law: Functions and Principles in Light of the Proposal for a Directive on consumer rights' (2010) 3(1) Erasmus Law Review 47, 61-62.

One caveat. Acquisti discusses the American situation. In the United States, there's no general data protection law, and online privacy is mostly governed by self-regulation, coupled with narrowly tailored statutes.[158] If all companies complied with European data protection law, some of the problems discussed by Acquisti should be less severe.

A logical solution to information asymmetry appears to be requiring companies to disclose information to internet users. But this runs into problems as well, as we will see in the next section.

4.3 Transaction costs

The obvious reaction to information asymmetries is requiring companies to provide information to data subjects. This brings us to transaction costs. These can be described as "any costs connected with the creation of transactions themselves, apart from the price of the good that is the object of the transaction."[159] Examples are the time a consumer spends on reading contracts, or searching for a product. In the context of behavioural targeting, the main transaction cost is the time it would cost internet users to inform themselves. Hence, because of transaction costs the information asymmetry problem is likely to persist.

The transparency requirements in European data protection law should be distinguished from the obligation to obtain consent for behavioural targeting. In practice however, many companies seek consent in their "terms and conditions" or "privacy policy".

Hardly anyone reads privacy policies. To give an example, an English company obtained the soul of 7500 people. According to its terms and conditions, customers granted "a non transferable option to claim, for now and for ever more, your immortal soul," unless they opted out.[160] The company later said it wouldn't exercise its rights.

Marotta-Wurgler did research on the readership of end user license agreements (EULAs) of software products. She analysed the click streams of almost 50.000 households, and concludes: "the overall average rate of readership of EULAs is on the order of 0.1 percent to 1 percent." On average, those readers didn't look long enough

---

[158] Solove DJ and Schwartz PM, *Information Privacy Law* (3rd edition) (Aspen 2009).
[159] Luth HA, *Behavioural Economics in Consumer Policy: The Economic Analysis of Standard Terms in Consumer Contracts Revisited* (Ph.D thesis University of Rotterdam) (Academic version 2010), 20.
[160] Fox News, '7,500 Online Shoppers Unknowingly Sold Their Souls ' (15 April 2010) <www.foxnews.com/tech/2010/04/15/online-shoppers-unknowingly-sold-souls/> accessed on 7 April 2013.

at EULA to read them.[161] It doesn't seem plausible that the readership of privacy policies would be much higher.[162]

There are several reasons why almost nobody reads privacy policies. First, life is too short. Reading them would take too much time. Cranor & McDonald calculated that it would cost the average American 244 hours per year to read the privacy policies of the websites she visits. This would be about 40 minutes a day, or about half of the time that the average American spent online every day (in 2006). Expressed in money, this cost would be around 781 billion dollars, while all online advertising income in the United States was estimated to be 21 billion dollar in 2007.[163]

Second, privacy policies are often long and difficult to read. Jensen & Potts analysed privacy policies, and found that more than half of the policies was too difficult for a majority of American internet users.[164] A quarter of Europeans say privacy policies are too difficult.[165]

Third, privacy policies are often vague. Research in the Netherlands shows that privacy policies generally fail to make data processing transparent.[166] Lawyers sometimes have a hard time deducing from a privacy policy what a company does with data. And if people understood a privacy policy, it's questionable whether they'd realise the consequences of combining and analysing their data. A user might only disclose scattered pieces of personal data here and there, but companies could still construct detailed profiles by combining data from different sources.[167]

Fourth, if somebody deciphers a privacy policy her quest might not be over. Privacy policies often refer to other privacy policies. Hence, people might have to consult dozens of privacy policies when they visit a website. Some companies change their privacy policies without notice, so people would have to check a privacy policy

---

[161] Marotta-Wurgler F, 'Will Increased Disclosure Help? Evaluating the Recommendations of the ALI's Principles of the Law of Software Contracts' (2011) 78(1) The University of Chicago Law Review 165, 168.

[162] In a survey 58% of Europeans responded that they read privacy policies, but they might overestimate how often they do in practice (European Commission. 'Special Eurobarometer 359: Attitudes on Data Protection and Electronic Identity in the European Union' (2011) <http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf> accessed on 18 November 2012, 112-114.)

[163] McDonald AM and Cranor LF, 'The Cost of Reading Privacy Policies' (2008) 4(3) I/S: A Journal of Law and Policy for the Information Society 540.

[164] Jensen C and Potts C, 'Privacy policies as decision-making tools: an evaluation of online privacy notices' (2004), Proceedings of the SIGCHI Conference on Human Factors in Computing Systems 471.

[165] European Commission. 'Special Eurobarometer 359: Attitudes on Data Protection and Electronic Identity in the European Union' (2011) <http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf> accessed on 18 November 2012, 112-114.

[166] Verhelst EW, *Recht Doen aan Privacyverklaringen: een Juridische Analyse van Privacyverklaringen op Internet [A Legal Analysis of Privacy Policies on the Internet] (Ph.D thesis University of Tilburg)* (Academic version 2012), 221.

[167] Barocas S and Nissenbaum H, 'On Notice: the Trouble with Notice and Consent (Proceedings of the Engaging Data Forum: The First International Forum on the Application and Management of Personal Electronic Information)' (October 2009) <www.nyu.edu/pages/projects/nissenbaum/papers/ED_SII_On_Notice.pdf> accessed on 5 April 2013, 6.

regularly. The conclusion is clear: transaction costs are a problem for consent to behavioural targeting. Privacy policies fail to inform people that use computers, and it's even more difficult to inform people that access services on mobile devices with smaller screens.

The accepting without reading problem isn't unique to the privacy field. Most consumers don't read (other) contracts either. It has been argued that an "informed minority" of consumers disciplines the market by reading contracts. The idea is that companies adapt their contracts to the few people that read contracts.[168] But many authors are sceptical about the informed minority argument.[169] If an informed minority is too small, it won't discipline the market. Sometimes a change in a company's privacy policy leads to reactions in the press, and sometimes companies react to that.[170] But such cases are relatively rare. If one percent or less reads privacy policies, there probably aren't enough people to discipline the market.[171]

If somebody read and understood a privacy policy, transaction costs could still be a problem. For some services, such as search engines, moving to a more privacy friendly competitor is relatively easy (if there is one). But moving to another service often involves transaction costs. For instance, transferring emails and contacts to another email provider costs time. Sometimes, "when the costs of switching from one brand of technology to another are substantial, users face *lock-in*".[172] If Facebook or iTunes changes its privacy policy, many people might just accept. And when all one's friends are on Facebook, it makes little sense to move to another social network site.

Lastly, reading privacy policies doesn't guarantee being informed. For instance, things can go wrong. A company could experience a data breach. And some companies don't act according to their privacy policy. For example, Google said on a website that people who used the Safari browser on certain devices were effectively opted out of tracking, because Safari blocks third party cookies. But Google bypassed

---

[168] Schwartz A and Wilde LL, 'Intervening in Markets on the Basis of Imperfect Information: A Legal and Economic Analysis' (1978) 127 University of Pennsylvania Law Review 630, 638: "if enough searchers [people who read contracts, FZB] exist, firms have incentives both to compete for their business and to offer the same terms to nonsearchers. When the preferences of searchers are positively correlated with the preferences of nonsearchers, competition among firms for searchers should tend to protect all consumers" (internal footnote omitted).

[169] Luth HA, *Behavioural Economics in Consumer Policy: The Economic Analysis of Standard Terms in Consumer Contracts Revisited* (Ph.D thesis University of Rotterdam) (Academic version 2010), 149,

[170] For instance, after attention in the press, Facebook offered people a way to opt out of their 'Beacon' service (Debatin B and others, 'Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences' (2009) 15(1) Journal of Computer-Mediated Communication 83).

[171] Bakos Y, Marotta-Wurgler F and Trossen D, 'Does Anyone Read the Fine Print? Testing a Law and Economics Approach to Standard Form Contracts (NYU Law and Economics Research Paper No. 09-40)' (2009) <http://ssrn.com/abstract=1443256> accessed on 5 April 2013,

[172] Shapiro C and Varian HR, *Information Rules. A Strategic Guide to the Network Economy* (Harvard Business School Press 1999), 104. See generally about lock-in: chapter 5 and 6.

Safari's settings.[173] Monitoring hundreds of companies that have access to their data would take internet users too much time.

Outside data protection law, rules that require companies to disclose information to people are ubiquitous as well. Lawmakers often choose for this regulatory technique in the hope people will make decisions in their own best interests.[174] In European consumer law for instance, this is the predominant approach.[175] But there's little evidence that providing information helps to steer people towards decisions in their own best interests. Many scholars are sceptical.[176] Ben-Shahar and Schneider summarise: "[n]ot only does the empirical evidence show that mandated disclosure regularly fails in practice, but its failure is inevitable."[177]

To conclude, the information asymmetry problem is likely to persist because of transaction costs. Privacy policies fail to inform people when they access the internet on a computer, and the problems are harder when people use a device with a smaller screen, such as a smart phone. Transaction costs make it hard for people that consent to behavioural targeting to make choices in their own interests. The next section discusses exchanges that impose costs on others than the contract parties.

4.4 Externalities

This section discusses externalities. From an economic viewpoint, one reason for legal intervention in markets is when an exchange has negative effects for others than the contract parties. Whether such externalities should lead to intervention in the case of consent to behavioural targeting is contentious.

Economists refer to costs or damage suffered by third parties as a result of economic activity as externalities. Externalities can occur because contract parties that aim to maximise their own welfare don't let costs for others influence their decisions. An example of an externality is environmental pollution. Say a company produces aluminium, and sells it to another party. If the production of aluminium causes pollution, it imposes costs on others. Rational producers and buyers ignore these costs. When the costs of pollution for others are taken into account, too much

---

[173] United States District Court for the Northern District of California, 16 November 2012, United States of America (For the Federal Trade Commission), Plaintiff, v. Google Inc., Defendant, Case No. 5:12-cv-04177-HRL FTC Docket No. C-4336.

[174] Ben-Shahar O and Schneider C, 'The Failure of Mandated Disclosure' (2011) 159 University of Pennsylvania Law Review 647.

[175] Grundmann S, Kerber W and Weatherill S (eds), *Party Autonomy and the Role of Information in the Internal Market* (De Gruyter 2001); Luth HA, *Behavioural Economics in Consumer Policy: The Economic Analysis of Standard Terms in Consumer Contracts Revisited* (Ph.D thesis University of Rotterdam) (Academic version 2010), 228.

[176] See for an overview, with references: Luth HA, *Behavioural Economics in Consumer Policy: The Economic Analysis of Standard Terms in Consumer Contracts Revisited* (Ph.D thesis University of Rotterdam) (Academic version 2010).

[177] Ben-Shahar O and Schneider C, 'The Failure of Mandated Disclosure' (2011) 159 University of Pennsylvania Law Review 647, 651.

aluminium is produced from a social welfare perspective.[178] Environmental law could thus be seen as a reaction to an externality. Externalities can also be positive. If somebody hires a gardener to craft a beautiful garden in front of her house, people in the street might enjoy the sight. These neighbours gain utility from the garden; they enjoy a positive externality. Many legal rules can be explained as an answer to an externalities problem.

Are externalities relevant for consent to behavioural targeting? The answer is complicated. As mentioned, some privacy harms are not only difficult, but impossible to quantify. In Acquisti's words, certain "privacy dimensions that affect individuals' well-being (…) are not merely intangible, but in fact immeasurable."[179]

If somebody consents to sharing her data with a company there are no negative externalities at first glance: she merely gives up an individual interest. But people's consent to behavioural targeting may lead to the application of knowledge to others. This could be seen as an externality imposed to others.[180] For instance, say a supermarket can track the shopping behaviour of thousands of customers that joined a loyalty program. The supermarket constructs the following predictive model: 90% of the women who buy certain products will give birth within two months.[181] Out of privacy considerations, Alice didn't join the loyalty program. But when she buys certain products, the shop can predict with reasonable accuracy that she's pregnant.[182] This could be seen as an externality imposed on Alice.

Moreover, if almost everybody consents to being tracked, *not* consenting could make somebody conspicuous. Does she have something to hide?[183] Sometimes not disclosing information, or not participating, can raise suspicion.[184] Osama Bin Laden was found, partly because it was suspicious that his large compound didn't have internet access.[185]

---

[178] Trebilcock MJ, *The Limits of Freedom of Contract* (Harvard University Press 1997 (paperback)), chapter 3.

[179] Acquisti A, 'The Economics of Personal Data and the Economics of Privacy (preliminary draft)' (2010) <www.heinz.cmu.edu/~acquisti/papers/acquisti-privacy-OECD-22-11-10.pdf> accessed on 4 February 2013, 5.

[180] MacCarthy M, 'New Directions in Privacy: Disclosure, Unfairness and Externalities' (2011) 6 I/S: A Journal of Law and Policy for the Information Society 425; Schreurs W and others, 'Cogitas, Ergo Sum. The Role of Data Protection Law and Non-discrimination Law in Group Profiling in the Private Sector' in Hildebrandt M and Gutwirth M (eds), *Profiling the European citizen: Cross-Disciplinary Perspectives* (Springer 2008).

[181] See about predictive modelling: Siegel E, Predictive Analytics: The Power to Predict Who Will Click, Buy, Lie, or Die (Wiley 2013), chapter 1.

[182] The example is based on a news report on the American supermarket Target, which reportedly found that a woman was pregnant, based on the products she bought (Duhigg, Charles. 'How Companies Learn Your Secrets' (16 February 2012) <www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=all&_r=0> accessed on 7 April 2013).

[183] Posner RA, Economic Analysis of Law (Aspen/Wolters Kluwer 2010), 25.

[184] Peppet SR, 'Unraveling Privacy: The Personal Prospectus and the Threat of a Full-Disclosure Future' (2011) 105(3) Northwestern University Law Review 1153.

[185] Ambinder M, 'The Secret Team That Killed Osama bin Laden' (2 May 2011) <www.theatlantic.com/international/archive/2011/05/the-secret-team-that-killed-osama-bin-laden/238163/> accessed on 15 February 2013.

There may be positive externalities when people consent to behavioural targeting. For instance, companies might use behavioural targeting data that are collected with consent for innovation. If innovative products benefit other parties than the company and the person that consented, there's a positive externality. In sum, consenting to behavioural targeting might have positive externalities, but how much is unclear.

In conclusion, it's unclear whether behavioural targeting's positive externalities outweigh the negative externalities or vice versa. More research is needed on the question. But whether it's possible to come to definitive answers remains to be seen.

4.5 Market power

From an economic viewpoint, market power, like a monopoly situation, may be a reason for legal intervention. But it's probably rare that market power is the main problem in the case of consent to behavioural targeting, from an economic viewpoint. The problems described in this paper could persist, even when no company has market power.

In a perfectly competitive market many companies must compete for consumers. Companies have no market power. Without problems such as information asymmetries, competition should lead to products that consumers want, for prices close to the productions costs. Competition should thus lead to the highest social welfare, and to consumer-friendly services. This is the ratio for laws that aim to mitigate market power, such as competition law. The opposite of a perfectly competitive market is a monopoly situation. A monopolist has significant market power. For instance, it can raise prices without fearing the reaction of competitors.

But in a perfectly competitive market, many of the problems described in this paper could remain. Information asymmetries can lead to market failure, even if a market is perfectly competitive.[186] Bar-Gill speaks of behavioural market failures. He explains: "competition forces sellers to exploit the biases and misperceptions of their customers."[187]

> The basic claim is that market forces demand that sellers be attentive to consumer psychology. Sellers who ignore consumer biases and misperceptions will lose business and forfeit revenue and profits. Over time, the sellers who remain in the market, profitably, will be the ones who have adapted their contracts and prices to respond, in the most optimal way, to the psychology of their customers.[188]

[186] Bar-Gill O, *Seduction by Contract: Law, Economics, and Psychology in Consumer Markets* (Oxford University Press 2012), 16.
[187] Idem, 2.
[188] Idem, 8. Luth reaches a similar conclusion (Luth HA, Behavioural Economics in Consumer Policy: The Economic Analysis of Standard Terms in Consumer Contracts Revisited (Ph.D thesis University of Rotterdam) (Academic version 2010), 81, 107-108, 288).

In the context of behavioural targeting, this might suggest that companies that don't exploit people's imperfect information and biases would not stay in business. Hence, the analysis below remains relevant, whether there's perfect competition or not.

Privacy scholars often complain that people lack real choice.[189] People have no real choice if a company offers a unique service and offers a take-it or-leave-it choice. This is a valid concern from a fundamental rights perspective. But from an economic perspective the question of whether there's too much market power depends on the specifics of a particular market. The conclusion would be different for search engines, social networks sites, online newspapers, or games for phones. Many situations that worry privacy scholars aren't a market power problem from an economics- or competition law viewpoint.

For instance, there could be a situation of monopolistic competition, where many companies compete by differentiating their products. This is often the case in markets for magazines or newspapers. Monopolistic competition is usually not regarded as a market power problem from an economic viewpoint. We return below to situations where people may feel they have to accept.[190] In sum, from an economic viewpoint market power is not the main problem in the case of consent to behavioural targeting. Even in a perfectly competitive market, the problems described in this paper could remain.

4.6 Conclusion

The analysis in this section suggests that internet users have severe difficulties entering "transactions" in their best interests. The main problem is asymmetric information, and transaction costs make this information asymmetry difficult to overcome. Bounded rationality aggravates this problem, as we will see in the next section.

[189] See e.g.: Blume P, 'The Inherent Contradictions in Data Protection Law' (2012) 2(1) International Data Privacy Law 26; Rouvroy A and Poullet Y, 'The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy' in (Springer 2009), 50-52; 70-74.
[190] Section 4.3 on transaction costs, and section 5.3 on myopia.

5. Informed consent and insights from behavioural economics

5.1 Introduction

Insights from behavioural economics highlight more problems with informed consent. Behavioural economics uses findings from for example psychology to predict human behaviour. Research shows that people structurally act differently than rational choice theory predicts.

If many people make decisions that don't conform to rational choice theory, but do so in different ways, on average their decisions might still conform to rational choice theory. Random deviations from rational choice theory would not influence the theory's predictive power in the aggregate.[191] But people tend to make decisions that are systematically different from what rational choice theory predicts. Sunstein summarises: "[p]eople are not always 'rational' in the sense that economists suppose. But it does not follow that people's behaviour is unpredictable, systematically irrational, random, rule-free or elusive to scientists. On the contrary, the qualifications can be described, used, and sometimes even modeled."[192]

"What Can Behavioural Economics Teach Us about Privacy?", ask Acquisti & Grossklags in an influential paper from 2007.[193] Privacy scholars start to take behavioural economics insights into account. Important research on how people make privacy choices is done by scholars such as Acquisti, Cranor and McDonald, who all work or worked at the Carnegie Mellon University in Pittsburgh. Large parts of the following sections could be seen as a literature review of the Pittsburgh school.

The section is structured as follows. Section 5.2 introduces bounded rationality, heuristics, and biases. Section 5.3 to 5.4 discuss myopia, the status quo bias, and some more biases that are likely to influence privacy choices. Section 5.6 discusses the privacy paradox: sometimes people that say they care deeply about privacy, disclose personal data in exchange for minimal benefits. Section 5.7 concludes.

5.2 Bounded rationality, heuristics and biases

A first way in which people act differently from what might be expected from rational choice theory, is their bounded rationality. Simon explains: "[t]he term 'bounded rationality' is used to designate rational choice that takes into account the cognitive limits of the decision maker – limitations of both knowledge and computational

[191] Posner RA, 'Rational Choice, Behavioral Economics, and the Law' (1998) 50(5) Stanford Law Review 1551.
[192] Sunstein CR, 'Introduction' in Sunstein CR (ed), *Behavioral law and economics* (Cambridge University Press 2000), 1.
[193] Acquisti A and Grossklags J, 'What Can Behavioral Economics Teach Us About Privacy?' in Acquisti, A. and others (eds), *Digital Privacy: Theory, Technologies and Practices* (Auerbach Publications, Taylor and Francis Group 2007).

capacity."[194] The human mind has limited capabilities for decisions when many factors have to be taken into account. People tend to be bad at calculating risks, and at statistics in general.

Because of their bounded rationality, people often rely on rules of thumb, or heuristics. Kahneman defines a heuristic as "a simple procedure that helps find adequate, though often imperfect, answers to difficult questions."[195] Usually such mental shortcuts work fine. "Do as the others do" is often a useful heuristic for instance. When you are in a department store and everybody starts to flee for the exit, leaving the building too might be a good idea. But sometimes, heuristics might lead to decisions that people later regret. "Humans predictably err."[196] Such systematic deviations, or common mistakes, are called biases.

Acquisti & Brandimarte note that even fully informed people often have difficulties making privacy choices in their own interests.

> As a matter of fact, the information available to individuals when making decisions regarding privacy is often incomplete (…). Moreover, due to bounded rationality, the individual cannot obtain and retain all information necessary to make a perfectly rational decision. Even if she could access all that information, and even if she had unlimited capability of information storage and processing, her choices would nonetheless be influenced by several psychological biases and heuristics (…) All these factors influence the individual's privacy decision-making processes in such a way that even if she was willing, in theory, to protect her privacy, in practice she may not do so.[197]

Biases influence privacy choices. Somebody that wants to make a rational choice to consent to behavioural targeting, would have to take many things into account. Making "rational" choices about complex matters such as privacy is difficult, and biases can lead to systematic deviations from what rational choice theory predicts.

People often rely on heuristics when making choices regarding privacy. An example of a heuristic is assuming that a website with a "privacy seal" has good privacy practices, without doing research on the requirements for obtaining a seal.[198] Below

---

[194] Simon HA, 'Bounded Rationality (reprint from Simon, Herbert A., Bounded Rationality, in J Eatwell, M. Milgate and P. Newman (eds.), The New Palgrave: A dictionary of economics, London: Macmillan 1987, Volume 1, p. 266-268)' in Simon, HA (ed), *Models of bounded rationality, Vol. 3: Empirically grounded economic reason* (MIT Press 1997).

[195] Kahneman D, *Thinking, Fast and Slow* (Allen Lane/Pinguin 2011), 98.

[196] Sunstein CR and Thaler RH, *Nudge: Improving Decisions about Health, Wealth, and Happiness* (Yale University Press 2008), 7.

[197] Acquisti A and Brandimarte L, 'The Economics of Privacy' in Peitz M and Waldfogel J (eds), *The Oxford handbook of the digital economy* (Oxford University Press 2012), 564.

[198] Moores T, 'Do Consumers Understand the Role of Privacy Seals in E-Commerce?' (2005) 48(3) Communications of the ACM 86.

some well-known biases that are relevant for consent to behavioural targeting are discussed.

5.3 Myopia

Myopia, or present bias, is likely to influence people's decisions regarding consent to behavioural targeting. Myopia literally means limited sight or short sightedness. In behavioural economics, myopia refers to the effect that people tend to focus more on the present than on the future. People often choose for immediate gratification, thereby not paying attention to future costs.[199] "I can finish these footnotes on Monday". People that are planning to lose weight might choose for immediate pleasure and eat a piece of cake. Myopia also helps to explain why many people don't save enough for their retirement.[200]

Myopia suggests that many people might choose immediate access to a service, also if this means they have to consent to behavioural targeting, contrary to earlier plans. Say somebody reads about behavioural targeting, and decides not to accept any more tracking cookies. That night, she wants to visit the website of a newspaper, and wants to watch a TV show online. Both websites deny entrance to visitors that don't accept the tracking cookies of third parties.[201] Contrary to her earlier plans, she clicks 'yes' on both websites. In sum, myopia can help to explain the privacy paradox: people that say they care about their privacy often disclose personal data in exchange for small short term benefits.

Related biases concern overconfidence and optimism. People tend to underestimate the risk of accidents and diseases, and overestimate the chances of a long and healthy life or winning the lottery. Most drivers think they drive better than the average driver. Most newlywed couples think there's an almost 100% chance that they will stay together, even when they know that roughly one in two marriages ends in divorce.[202] Research suggests that people are too optimistic when they estimate the risks of privacy harms. For instance, people tend to underestimate the risks of identity fraud and of re-identification of anonymised data.[203] In conclusion, myopia suggests

---

[199] Luth HA, *Behavioural Economics in Consumer Policy: The Economic Analysis of Standard Terms in Consumer Contracts Revisited* (Ph.D thesis University of Rotterdam) (Academic version 2010), 53.

[200] Sunstein CR and Thaler RH, *Nudge: Improving Decisions about Health, Wealth, and Happiness* (Yale University Press 2008), chapter 6.

[201] Early 2013 this was the case in the Netherlands. The Public Broadcaster and one of the larger newspapers (Volkskrant) both installed a cookie wall (<www.publiekeomroep.nl> and <www.volkskrant.nl> accessed 15 February 2013).

[202] Sunstein CR and Thaler RH, *Nudge: Improving Decisions about Health, Wealth, and Happiness* (Yale University Press 2008), 31-33. In Europe some countries have lower divorce rates (Eurostat. 'Marriage and Divorce Statistics' (October 2012) <http://epp.eurostat.ec.europa.eu/statistics_explained/index.php/Marriage_and_divorce_statistics> accessed on 11 April 2013).

[203] Acquisti A and Grossklags J, 'Privacy and rationality in individual decision making' (2005) 3(1) IEEE Security & Privacy 26.

that it's difficult for people to make choices regarding consent to behavioural targeting according to their plans.

5.4 Status quo bias

The status quo bias, or inertia, refers to the power of the default.[204] Most people don't change the default option. This isn't in line with rational choice theory, which predicts that people choose according to their preferences, regardless of the default option (assuming there are no transaction costs).

A famous example of the status quo bias concerns the percentage of people that allow their organs to be used for transplantation if they die. European countries that use an opt-out system (people donate their organs unless they express that they don't want to) have many donors, while countries that use an opt-in system have few donors.[205]

When it comes to privacy choices, people tend to stick with the default, even when transaction costs are negligible. As Sunstein puts it, "true, we might opt out of a website policy that authorizes a lot of tracking (perhaps with a simple click) – but because of the power of inertia, many of us are not likely to do so."[206] The effect of the status quo bias is stronger when switching entails more transaction costs. Many people don't tweak the settings of their browser or their social network site accounts.[207]

Insights in the status quo bias are useful to understand discussions about opt-in versus opt-out systems. Companies often prefer to collect personal data, unless people object. Privacy advocates tend to prefer opt-in systems, where somebody has to take affirmative action to say "yes".

The status quo bias suggests that if people are presumed to consent to behavioural targeting unless they object (an opt-out system), a majority of people might "consent". If consent is interpreted as requiring an indication of will, most people might stick with the default: no tracking.

---

[204] Samuelson W and Zeckhauser R, 'Status Quo Bias in Decision Making' (1988) 1(1) Journal of Risk and Uncertainty 7.
[205] Johnson EJ and Goldstein D, 'Do Defaults Save Lives?' (2003) 302(5649) Science 1338.
[206] Sunstein CR, 'The Storrs Lectures: Behavioral Economics and Paternalism (forthcoming Yale Law Journal)' (2012) <http://ssrn.com/abstract=2182619> accessed on 5 April 2013, 55.
[207] On the settings of social media accounts: Acquisti A and Gross R, 'Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook' (2006) 4258 6th International Workshop, PET 2006, Cambridge, UK, June 28-30, 2006 (Lecture Notes in Computer Science) 36.

5.5 Other biases

This section discusses some other biases that are likely to influence choices about behavioural targeting. For instance, heuristics make people susceptible for framing: the way information is presented can influence decisions.[208] Many people see a link to a privacy policy as a quality seal. A 2008 survey found that most Californians thought that the mere fact that a website has a privacy policy, means that their privacy is protected by law.[209] 41% of Europeans don't read privacy policies, because they think it's enough to check whether a website has one.[210] Turow at al. argue that the phrase "privacy policy" is misleading.[211] At least one company speaks of a "data use policy", which seems a more apt name.[212]

People are more likely to consent if a pop-up looks more like an end user license agreement (EULA). Böhme and Köpsell varied the design of consent dialog boxes and tested the effect by analysing the clicks of more than 80.000 people. They conclude that people tend to click "agree" to a consent request if it looks like a EULA.

> [U]biquitous EULAs have trained even privacy-concerned users to click on "accept" whenever they face an interception that reminds them of a EULA. This behaviour thwarts the very intention of informed consent. So we are facing the dilemma that the long-term effect of well-meant measures goes in the opposite direction: rather than attention and choice, users exhibit ignorance.[213]

Research by Good et al. suggests that privacy policies with vague language give people the impression that a service is more privacy-friendly than privacy policies

---

[208] For example, Kahneman found that even among doctors, "[t]he statement that 'the odds of survival one month after surgery are 90%' is more reassuring than the equivalent statement that 'mortality within one month of surgery is 10%.'" Kahneman D, *Thinking, Fast and Slow* (Allen Lane/Pinguin 2011), 88.

[209] Hoofnagle, C and King J, 'What Californians Understand about Privacy Online (UC Berkeley)' (3 September 2008) <http://ssrn.com/abstract=1262130> accessed on 5 April 2013; Turow, J, 'Americans & Online Privacy: The System is Broken (Annenberg Public Policy Center of the University of Pennsylvania)' (June 2003) <www.annenbergpublicpolicycenter.org/Downloads/Information_And_Society/20030701_America_and_Online_Privacy/20030701_online_privacy_report.pdf> accessed on 5 April 2013; Turow J, Feldman L, and Meltzer K, 'Open to Exploitation: America's Shoppers Online and Offline (Annenberg Public Policy Center of the University of Pennsylvania)' (1 June 2005) <www.annenbergpublicpolicycenter.org/NewsDetails.aspx?myId=31> accessed on 5 April 2013.

[210] European Commission, 'Special Eurobarometer 359: Attitudes on Data Protection and Electronic Identity in the European Union' (2011) <http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf> accessed on 18 November 2012, 118-120.

[211] Turow J and others, 'The Federal Trade Commission and Consumer Privacy in the Coming Decade' (2007) 3(3) I/S: A Journal of Law & Policy for the Information Society 723.

[212] Facebook. 'Data Use Policy' (11 December 2012) <www.facebook.com/about/privacy> accessed on 10 April 2013.

[213] Böhme R and Köpsell S, 'Trained to Accept? A Field Experiment on Consent Dialogs' (2010) Proceedings of the SIGCHI Conference on Human Factors in Computing Systems 2403, 2406.

that give more details.[214] A study by Moore on privacy seals suggests that "any official-looking graphic" can lead people to believe that a website is trustworthy.[215]

Acquisti et al. discuss a "control paradox". People share more information if they *feel* they have more control over how they share personal information. The researchers conclude that control over personal information is a normative definition of privacy: control should ensure privacy. But in practice, "'more' control can sometimes lead to 'less' privacy in the sense of higher objective risks associated with the disclosure of personal information."[216]

In sum, a variety of biases influences privacy choices. If the lawmaker aims to ensure that people enjoy a certain level of privacy, focusing on informed consent may have unintended effects.

5.6 Privacy paradox

Insights from behavioural economics can partly explain the privacy paradox: people say in surveys they care about privacy, but often disclose personal data in exchange for minimal benefits, and few people use technical tools to protect their privacy online.

Some conclude that people only care about privacy when they don't have to deal with other interests. "Consumers may tell survey takers they fear for their privacy, but their behaviour belies it. People don't read privacy policies, for example."[217] The idea is that people care more about a 1-euro discount than about their privacy when they're not giving survey answers. This is probably true for some people. But as a general conclusion it might be too simple to say that people don't care. Another interpretation is that people have difficulties acting according to their own stated preferences. Furthermore, research suggests that many people find technical privacy protection tools too complicated.[218]

In general, stated preferences (what people say in surveys) might be less reliable that expressed preferences (how people act). But regarding privacy decisions, it's doubtful whether expressed privacy preferences can be used to estimate how much people value their privacy (in monetary terms). It's easy to manipulate the value people

[214] Good N and others, 'User Choices and Regret: Understanding Users' Decision Process about Consensually Acquired Spyware' (2006) 2(2) A Journal of Law & Policy for the Information Society 283, 323.
[215] Moores T, 'Do Consumers Understand the Role of Privacy Seals in E-Commerce?' (2005) 48(3) Communications of the ACM 86, 89-90.
[216] Brandimarte L, Acquisti A and Loewenstein G, 'Misplaced confidences: Privacy and the control paradox' (2012) Social Psychological and Personality Science, 1, 6.
[217] Goldman E, 'The Privacy Hoax (Forbes)' (14 October 2002) <www.forbes.com/forbes/2002/1014/042.html> accessed on 5 April 2013.
[218] Leon P and others, 'Why Johnny Can't Opt Out: A Usability Evaluation of Tools to Limit Online Behavioral Advertising' (2012) Proceedings of the 2012 ACM Annual Conference on Human Factors in Computing Systems 589.

attach to their personal data.[219] For instance, in a study by Cranor & McDonald, most participants would not pay 1 dollar a month to keep a website from doing behavioural targeting. At first glance, this might suggest that few think that protecting their information is worth more than 1 dollar a month.

But, 69% would *not* accept a 1-dollar discount in exchange for having their data collected for behaviourally targeted advertising. This would suggest that most people think their personal data is worth more than 1 dollar a month. In short, people's willingness to pay for privacy seems to be different than their willingness to accept (a discount) to forego privacy. When one assumes that people make "rational" choices to maximise their own utility, in this case their privacy, the results are surprising.[220]

In follow-up interviews and a survey, Cranor & McDonald "found people generally unwilling to pay for privacy, not because they do not value it, but because they believe it is wrong to pay."[221] 69% of the respondents agreed with the statement "Privacy is a right and it is wrong to be asked to pay to keep companies from invading my privacy".[222] 61% agreed it would be "extortion" when a company would ask them to pay for not collecting data. The researchers "suggest that one reason people will not pay for privacy is because they feel they should not have to: that privacy should be theirs by right."[223] The price people attach to personal data doesn't appear to be a good indicator of how much people value their privacy. In sum, relying on survey data to establish how much people value their privacy has its problems. But for privacy choices, people's behaviour doesn't seem to be a good indicator of how much people privacy either. In conclusion, the privacy paradox can be partly explained by insights from behavioural economics.

5.7 Conclusion

This section discussed behavioural economics insights in the context of behavioural targeting. Bounded rationality influences people's decisions regarding privacy.

It's important to realise that biases are studied and used in marketing and advertising.[224] Free trial periods of newspapers can lead to subscriptions for years, because – in line with the status quo bias – people forget to cancel. "Buy this pack of shampoo, and get 2 euro back", relies on transaction costs and the status quo bias.

---

[219] Acquisti A, John L and Loewenstein G, 'What is privacy worth?' (2009) Workshop on Information Systems Economics.

[220] McDonald AM and Cranor LF, 'Beliefs and Behaviors: Internet Users' Understanding of Behavioral Advertising' (Telecommunications Policy Research Conference) (2 October 2010) <http://ssrn.com/abstract=1989092> accessed on 5 April 2013, 25.

[221] Idem, 28.

[222] Idem, 26.

[223] Idem, 26.

[224] Howells G, 'The Potential and Limits of Consumer Empowerment by Information' (2005) 32(3) Journal of Law and Society 349, 361-362; Bar-Gill O, Seduction by Contract: Law, Economics, and Psychology in Consumer Markets (Oxford University Press 2012).

Many people don't get around to sending in the coupon. (As an aside, sending in the coupon would disclose one's name and bank account number to the company.) The success of "Buy now, pay later" schemes can be partly explained by myopia and optimism bias.[225]

Myopia suggests that if people can only use a service if they "consent" to behavioural targeting, they might ignore the costs of possible future privacy infringements. The status quo bias influences decisions: it's likely that most people won't opt out of tracking. More biases are likely to affect privacy choices. For instance, the framing of a question steers choices. Hence, informed consent as a legal tool to protect people's privacy may have unintended effects.

An important caveat. We mustn't draw too broad conclusions about the effect of biases.[226] Privacy choices are context-dependent. Furthermore, one bias might influence a decision in one direction, while another bias might influence the same decision in another direction. Acquisti & Grossklags observe: "[t]he role of these effects on privacy decision making is likely to be significant, although by no means clear, since many competing hypotheses can be formulated."[227] Still, they argue it would be naïve to ignore knowledge about biases when setting policy that relies, in part, on the decisions of people whose privacy the law aims to protect.[228]

In sum, many behavioural biases are likely to influence people's choices about behavioural targeting. The following conclusion is only a slight exaggeration. People don't read privacy policies; if they read, they wouldn't understand; if they understood, they wouldn't act.[229]

---

[225] Sunstein CR and Thaler RH, *Nudge: Improving Decisions about Health, Wealth, and Happiness* (Yale University Press 2008), 35.

[226] Luth HA, *Behavioural Economics in Consumer Policy: The Economic Analysis of Standard Terms in Consumer Contracts Revisited* (Ph.D thesis University of Rotterdam) (Academic version 2010), 281.

[227] Acquisti A and Grossklags J, 'What Can Behavioral Economics Teach Us About Privacy?' in Acquisti A and others (eds), *Digital Privacy: Theory, Technologies and Practices* (Auerbach Publications, Taylor and Francis Group 2007), 371.

[228] Idem, 374. In the context of European consumer law Gomez reaches a similar conclusion (Gomez F, 'The Empirical Missing Links in the Draft Common Frame of Reference' in Micklitz HW and Cafaggi F (eds), *European Private Law After the Common Frame of Reference* (Edward Elgar Publishing 2010, 110).

[229] Ben-Shahar and Schneider arrive at a similar conclusion on the regulatory technique of mandated disclosure of information in general: people "often do not read disclosed information, do not understand it when they read it, and do not use it even if they understand it." Ben-Shahar O and Schneider C, 'The Failure of Mandated Disclosure' (2011) 159 University of Pennsylvania Law Review 647, 665.

6. Policy implications

6.1 Introduction

This section explores possible regulatory answers to the problems with informed consent that were discussed above. What are the policy implications of insights from behavioural economics in the context of consent to behavioural targeting? This paper distinguishes two regulatory techniques: *empowering* the individual, and *protecting* the individual.

The first technique, empowerment, primarily aims to enable people to make choices in their own interests. For instance, the law can aim to make informed consent more meaningful. The lawmaker could also arrange education for internet users. The second technique, protection, primarily aims to safeguard people's privacy interests. Prohibitions of certain practices fall in this category. Such measures don't rely on helping people making decisions in their own best interests, but limit people's choices.

Third, there's a middle ground between empowering and protecting people, or between informed consent and prohibitions. The lawmaker could steer people towards making certain decisions, without actually limiting their options. The law could set default rules, and use transaction costs strategically to make it harder to opt out of the default.

The section is structured as follows. Section 6.2 discusses rules that aim to empower people. Section 6.3 discusses rules that aim to protect people. Lastly, sticky defaults are mentioned as a middle ground.

6.2 Empowerment of the individual

A first regulatory answer to the practical problems with informed consent is aiming to empower people. For instance, the law can aim to make data processing more transparent, or to make informed consent more meaningful. This empowerment approach broadly fits with the existing data protection approach. This section discusses empowerment rules in reaction to information asymmetry, to transaction costs, and to insights from behavioural economics.

Information asymmetry is a problem in the context of consent to behavioural targeting. For some problems data protection law already suggests an answer, but for others it doesn't. First, many people don't know their online behaviour is being monitored for behavioural targeting. At first glance, the answer seems reasonably straightforward. The law requires companies to obtain consent for the use of tracking

technologies, and requires companies to be transparent about their data processing practices.

Second, people have scant idea about what companies do with their personal data. Again the answer seems reasonably straightforward. Data protection law requires companies to be open about their data processing practices, and about the processing purposes. Moreover, data must be "collected for specified, explicit and legitimate purposes and *not further processed in a way incompatible with those purposes*".[230] From the start, companies must explain clearly what they do with personal data.

In sum, for two categories of information asymmetries data protection law has an answer. But this doesn't suggest that solutions are easy. For internet users and for poorly funded Data Protection Authorities it's hard to make companies comply with the law, especially when companies are based outside the European Union. Moreover, whether transparency requirements could actually achieve informing people is questionable.

For two categories of information asymmetry, data protection law doesn't have an answer. First, people don't know the consequences of future uses of personal data.[231] Perhaps the law could help. Companies could be required to disclose certain information. For instance, companies could be required to disclose the number of data breaches that have occurred the year before.[232] In other contexts, the law also requires information about risks, such as on cigarette warnings. Again the question is whether such warnings would help.

Another category of information asymmetry is that people don't know what their data are worth. Therefore, it's hard to make an informed decision whether to disclose personal data in exchange for the use of a "free" service. Data protection law doesn't seem to have an answer here. But maybe data protection law's transparency principle could provide inspiration. It has been suggested that companies should be required to tell an internet user how much profit they make with her personal data.[233]

Perhaps education could help. People lack understanding of behavioural targeting, and of online privacy risks in general. It's not suggested that people all become ethicists, lawyers and computer scientists. But some basic knowledge of privacy and security risks would be useful. As Cranor & McDonald put it, "consumers cannot protect themselves from risks they do not understand."[234] But perhaps we shouldn't hope for too much. Learning takes time. For instance, people appear to have scant

[230] Article 6(1)(b) of the Data Protection Directive, emphasis added.
[231] [Education about privacy risks seems to be the appropriate answer.]
[232] Thanks to Professor Bar-Gill for this suggestion.
[233] Traung P, 'The Proposed New EU General Data Protection Regulation: Further Opportunities' (2012)(2) Computer Law Review international 33, 42.
[234] McDonald AM. and Cranor LF, 'Beliefs and Behaviors: Internet Users' Understanding of Behavioral Advertising' (Telecommunications Policy Research Conference) (2 October 2010) <http://ssrn.com/abstract=1989092> accessed on 5 April 2013, 27.

idea about behavioural targeting, although it happens since the mid 1990s.[235] While it's questionable whether education could keep up with the pace of technology, some knowledge is probably better than none at all.

In sum, at least two approaches are needed to mitigate the information asymmetry problem. First, education is needed. Second, data protection law should be enforced more rigorously. For instance, enforcing the transparency principle may help to mitigate the information asymmetry problem. But people may receive too many requests for consent, and may receive more information than they can handle. This brings us to transaction costs.

Transaction costs are one of the causes of information asymmetry. Reading privacy policies would take time, and they're often long, hard to understand, and vague. Some companies change their privacy policies without notice. Keeping track of whether a company lives up to the promises is costly as well.

Data protection law has some answers. Obtaining "consent" by silently changing a privacy policy isn't possible under data protection law.[236] Data subjects thus shouldn't have to keep checking a privacy policy. Furthermore, privacy policies that refer the reader to other privacy policies don't comply with data protection law's transparency principle. And in theory, Data Protection Authorities should help to ensure that companies don't act contrary to their promises. Hence, enforcing the law should mitigate the transaction costs.

Part of the reason that people don't read privacy policies or consent boxes is that it would take too much time. It must be possible to write shorter privacy policies, using less legalese. The Working Party calls for privacy policies with "simple, unambiguous and direct language,"[237] and suggests the use of layered privacy policies. A company should explain in a few sentences what it wants to do with personal data. People should be given the chance to click through to more detailed information. This would be an improvement. Standardised short notices may also help.[238] But such ideas have had little effect in practice.

Moreover, describing complicated data processing practices accurately leads to a long text. If the text is too concise, it doesn't provide enough information. In some ways,

---

[235] Cookies have been used to track people's online behaviour since at least 1996 (Carmichael M, 'Interactive; The Net Gets Nosy; Are Cookies Really Monsters?; What's Inside Those Netscape Tracking Sweets' (18 November 1996) <http://adage.com/article/news/interactive-net-nosy-cookies-monsters-inside-netscape-tracking-sweets/75640/> accessed on 10 April 2013.) See about the early history of cookies: Kristol DM, 'HTTP Cookies: Standards, Privacy, and Politics' (2001) 1(2) ACM Transactions on Internet Technology (TOIT) 151.

[236] See section 2.3.

[237] Article 29 Working Party, 'Opinion 10/2004 on More Harmonised Information Provisions' (WP 100), 25 November 2004, 5.

[238] Verhelst EW, *Recht Doen aan Privacyverklaringen: een Juridische Analyse van Privacyverklaringen op Internet [A Legal Analysis of Privacy Policies on the Internet] (Ph.D thesis University of Tilburg)* (Academic version 2012), 222-225; Kelly PG and others, 'Standardizing Privacy Notices: An Online Study of the Nutrition Label Approach' (2010) Proceedings of the SIGCHI Conference on Human Factors in Computing Systems 1573.

mitigating transaction costs by making privacy policies easier to understand conflicts with the goal of mitigating the information asymmetry.[239] And reading privacy policies, even short ones, takes time. Many short notices together still add up to a lot of information.

Maybe logos or seals could communicate the data processing practices of companies more effectively than privacy policies. In practice, such schemes haven't worked well. Some providers gave seals to any company, without a prior check. One researcher found that websites with a seal from TRUSTe (a popular provider of privacy seals) were generally less trustworthy than companies without that seal.[240]

More research is needed on alternative ways of presenting information. Calo suggests that we shouldn't forget about informed consent and transparency just yet, before better ways of presenting information have been tried.[241] Researchers have looked into better ways of conveying information, for example with interactive systems.[242] This is an important research avenue. Cooperation between several disciplines would be needed, such as technology design, computer interface design, and psychology. But even if effective ways of communication could be developed, it might be difficult to make companies use them.[243] A company that wants to distract people from certain information has many ways to do so, for instance by giving more information than needed.[244]

Perhaps the law could facilitate intermediaries that help people using information. For instance, companies could be required to disclose their data processing practices to organisations that give ratings or seals. Regulators could audit intermediaries to ensure honesty.[245]

If an internet user wants to take her business to a more privacy-friendly service, transaction costs may be a problem again. For example, it's not easy to switch to

---

[239] Nissenbaum calls this tension between completeness and conciseness the 'transparency paradox'. Nissenbaum H, 'A Contextual Approach to Privacy Online' (2011) 140(4) Daedalus 32, 36. See also Bar-Gill O, *Seduction by Contract: Law, Economics, and Psychology in Consumer Markets* (Oxford University Press 2012), 37.

[240] Edelman B, 'Adverse Selection in Online "Trust" Certifications and Search Results' (2011) 10(1) Electronic Commerce Research and Applications 17.

[241] Calo MR, 'Against Notice Skepticism in Privacy (and Elsewhere)' (2012) 87(3) Notre Dame Law Review 1027.

[242] See e.g. Groom V and Calo MR, 'Reversing the Privacy Paradox: An Experimental Study' (Telecommunications Policy Research Conference) (25 September 2011) <http://ssrn.com/abstract=1993125> accessed 10 April 2013.

[243] A recent European consumer protection directive calls for information "in a clear and comprehensible manner". See article 6(1) of the Consumer Rights Directive (Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council (L 304/64, 22 November 2011, 0064-0088)).

[244] Ben-Shahar O and Schneider C, 'The Failure of Mandated Disclosure' (2011) 159 University of Pennsylvania Law Review 647, [ ].

[245] See generally: Bar-Gill O, *Seduction by Contract: Law, Economics, and Psychology in Consumer Markets* (Oxford University Press 2012), 41-42; Luth HA, *Behavioural Economics in Consumer Policy: The Economic Analysis of Standard Terms in Consumer Contracts Revisited* (Ph.D thesis University of Rotterdam) (Academic version 2010), 243-247.

another email provider or another social network site provider. The proposal for a new Data Protection Regulation attempts to mitigate this problem, by introducing a right to data portability.[246] A company would have to offer users the possibility to download their data in an easily transferable format, to make it easier to switch to another company.[247]

In sum, solving the problem of information asymmetry is hard, but it might be possible to improve the situation. Lower transaction costs would make it easier to inform oneself. With complete information, hypothetical "rational" people could make decisions in their best interests. But behavioural economics insights suggest that solving the information asymmetry problem may not be enough.

Now we turn to regulation that aims to help people to overcome their biases. Even fully informed people often make choices against their own best interests. Exaggerating a bit: everybody clicks "yes" to everything. What should the law's reaction be?

Regulation could aim to help people overcome their biases, by helping people to make choices according to their own stated interests. A first bias that is likely to influence choices regarding privacy is the status quo bias. Current European law has the beginning of an answer. The e-Privacy Directive requires consent for most tracking technologies. We saw in section 2.3 that an opt-out system rarely complies with the law's requirements for consent. The status quo bias suggests that the privacy-friendly interpretation of the law matches the formal legal interpretation of the law: consent should be opt-in consent.[248]

But the myopia bias suggests that an opt-in system might have limited effect to steer people towards privacy-friendly choices. If people are offered a short-term advantage in exchange for consenting to being tracked, many might agree, even if they were planning not to. One possible reaction could be prohibiting companies from making the use of a service dependent on accepting behavioural targeting.[249] Like this it would be harder for companies to push people towards consenting to unwanted tracking. But this approach would interfere with freedom of choice, and with many business models on the internet. Perhaps some services couldn't be offered for "free" anymore, if not enough people consent to tracking. This possible cost for consumers

---

[246] Article 18 of the European Commission proposal for a Data Protection Regulation. (European Commission, 'Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)' (COM(2012) 11 final) (25 January 2012)).

[247] See for a critique on the provision: Swire P and Lagos Y, 'Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique (forthcoming Maryland Law Review)' (2012) <http://ssrn.com/abstract=2159157> accessed on 5 April 2013.

[248] See Sunstein CR, *Simpler: The Future of Government* (Simon and Schuster 2013), 38.

[249] A document submitted by civil society organisations, academics and citizens to the members of the European Parliament says: "No more coupling of service usage to personal data use (no more 'take-it or leave-it' online)" ('The Brussels Privacy Declaration' (January 2011) <http://brusselsdeclaration.net/> accessed on 11 April 2013). I am one of the signatories.

shouldn't be ignored. A lighter measure might be requiring companies to offer a tracking-free version of their service, which has to be paid for with money.[250] This would probably be less effective, because myopia might lead most people to choose for the free version.[251]

Framing also influences privacy choices. "Click here for more relevant advertising", sounds different than "Click here for continuous surveillance". As long as information isn't misleading, data protection law probably doesn't have an answer to the framing effect. But perhaps standardised privacy policies could help. In sum, the law could try to reduce the effect of biases, but this is hard.

In conclusion, one approach to improve the protection of privacy in the context of behavioural targeting is regulation that aims to empower people. For instance, enforcing data protection law's transparency requirements more vigorously could help. Companies that ask consent should do so clearly, in easy to understand language. More research is needed on better ways of presenting information. Maybe organisations should be set up to give quality ratings to websites and services. The law could also try to help people to overcome their biases. These kinds of rules that aim to empower the data subject fit in the tradition of data protection law.

A different approach is education for internet users. People can't make meaningful choices if they don't understand the question. There's a need for education about internet technology and privacy risks. This approach also aims to empower people. In sum, transparency probably can't be achieved, but it could be improved. The next section discusses rules that protect rather than empower people.

6.3 Protection of the individual

The law can also focus on protecting, rather than on empowering people. This section discusses such mandatory rules, or more specifically: prohibitions. Perhaps society is better off when certain behavioural targeting practices were prohibited. If aiming to empower the individual is not the right tactic to protect privacy, maybe prohibitions should be introduced in addition to the data protection regime. Some might say that the tracking of internet users isn't proportional to the purposes of marketers, and should therefore be prohibited. But less extreme measures can be envisaged. Different rules could apply to different circumstances.

The protection approach is likely to be more controversial than the empowerment approach. Current data protection law leaves the data subject some freedom of choice. The data subject's choices are limited, as most data protection rules can't be waived.

---

[250] Traung P, 'The Proposed New EU General Data Protection Regulation: Further Opportunities' (2012)(2) Computer Law Review international 33, 42.

[251] See on the attraction of "free" offers: Ariely D, *Predictably Irrational* (Harper 2008), chapter 3.

Relative to data protection law, prohibitions are more radical. But there are strong arguments in favour of bans.

First, it may be impossible to reduce the information asymmetry problem to manageable proportions. The more we use the internet, and the more companies we encounter that want to collect our data, the harder this problem will become. As we move into the era of the internet of things[252] and ubiquitous computing,[253] it may become even more difficult to make data processing transparent. Second, even if the information asymmetry problem could be solved – which is not a given – behavioural economics shows that people might make choices that don't conform to their own stated interests. Third, if informed consent doesn't work in the context of behavioural targeting, it's likely to affect millions of people.[254]

The main argument against prohibitions is probably that they unduly limit freedom of choice. When the sole goal of a prohibition is protecting people against themselves, it reeks of unwarranted paternalism. How much paternalism is acceptable depends, among other things, on one's political views.[255] But many prohibitions also protect society, or third parties. For instance, environmental law is best described as an answer to an externalities problem, rather than as a paternalistic intervention in people's freedom. Moreover, the current situation is that many people are being tracked and profiled without meaningful consent. This could be seen as a paternalistic intervention imposed by the marketing industry, without prior debate.[256]

Several scholars have hinted at the need for prohibitions in privacy law, because they lost faith in informed consent.[257] But it appears that few scholars have elaborated on

---

[252] The internet of things can be defined as "a dynamic global network infrastructure with self configuring capabilities based on standard and interoperable communication protocols where physical and virtual "things" have identities, physical attributes, and virtual personalities, use intelligent interfaces, and are seamlessly integrated into the information network" (Vermesan O and others, 'Internet of Things Strategic Research Roadmap' in Vermesan O and Friess P (eds), *Internet of Things* - Global Technological and Societal Trends (River 2011), 10).

[253] "[U]biquitous computing has as its goal the nonintrusive availability of computers throughout the physical environment, virtually, if not effectively, invisible for the user" (Weiser M, 'Ubiquitous Computing (Hot Topics)' (1993) 26(10) Computer (IEEE) 71, 71).

[254] Radin suggests that the amount of people affected should be taken into account when regulating standard contract terms (Radin MJ, Boilerplate. *The Fine Print, Vanishing Rights, and the Rule of Law* (Princeton University Press 2013, chapter 9).

[255] See about the distinction between soft and hard paternalism: Cserne P, *Freedom of Contract and Paternalism: Prospects and Limits of an Economic Approach (Ph.D thesis University of Hamburg)* (Academic version 2008), 19.

[256] Hoofnagle CJ and others, 'Behavioral Advertising: The Offer You Cannot Refuse' (2012) 6(2) Harvard Law & Policy Review 273.

[257] See e.g. Barocas S and Nissenbaum H, 'On Notice: the Trouble with Notice and Consent (Proceedings of the Engaging Data Forum: The First International Forum on the Application and Management of Personal Electronic Information)' (October 2009) <www.nyu.edu/pages/projects/nissenbaum/papers/ED_SII_On_Notice.pdf> accessed on 5 April 2013; Solove DJ, Privacy Self-Management and the Consent Paradox (forthcoming Harvard Law Review 2013) <http://ssrn.com/abstract=2171018> accessed 13 April 2013; Tene O and Polonetsky J, To Track or "Do Not Track": Advancing Transparency and Individual Control in Online Behavioral Advertising (2012) 13(1) Minnesota Journal of Law, Science, and Technology 281. See generally about mandatory rules regarding privacy: Allen A, *Unpopular Privacy: What Must We Hide?* (Oxford University Press 2011).

what should be prohibited.[258] Some examples of possible prohibitions are given below. In principle, prohibitions could target different phases of behavioural targeting. As noted, behavioural targeting entails (i) the tracking of people's online behaviour, (ii) to compile profiles of people, (iii) for targeted advertising.[259]

First we look at the phase of data collection and tracking. Maybe data protection law's categories of "sensitive data", such as data regarding health, religion, and political opinions, could provide inspiration. The Data Protection Directive allows the processing of such data after "explicit" consent, unless a member state decides that such data may not be processed on the basis of consent.[260] A prohibition along the following lines could be considered. "Personal data regarding people's health may not be processed for behavioural targeting." Or a prohibition could be considered for the tracking of children for behavioural targeting. At present, European data protection law doesn't have specific rules for children.[261]

Data collection for behavioural targeting could be banned in certain contexts.[262] Should we be able to read the news without a fear of surveillance?[263] Does, or should, the right to receive information in the European Convention of Human Rights imply a right to access information without being tracked?[264] Should online newspapers be banned from engaging in behavioural targeting?

A counter argument is that some news services might rely on income from behavioural targeting. On the other hand, advertising would still be possible if behavioural targeting were banned. Many radio stations are funded by advertising that doesn't involve profiling individual listeners. Furthermore, in the long run behavioural targeting may be a bad thing for online news providers. Without behavioural targeting, advertisers that want to reach New York Times readers have to advertise on the New York Times website.[265] With behavioural targeting, advertisers can target people that received a cookie on the New York Times website. This implies that advertisers can reach New York Times readers without buying advertising on the

---

[258] De Hert and Gutwirth discuss factors to take into account when deciding whether prohibitions are needed. De Hert P and Gutwirth S, 'Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power' in Claes, E, Duff A and Gutwirth S (eds), *Privacy and the criminal law* (Intersentia 2006).
[259] See section 2.1.
[260] Article 8 of the Data Protection Directive.
[261] The proposal for a Data Protection Regulation has specific rules regarding children; see e.g. article 6, 8, 11, 17 and 33 (European Commission, 'Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012) 11 final)').
[262] Nissenbaum H, 'A Contextual Approach to Privacy Online' (2011) 140(4) Daedalus 32.
[263] See about media law and behavioural targeting: Helberger N, 'Freedom of expression and the Dutch cookie-wall', conference paper MIT 8 Public Media Private Media Conference, Boston, 3-5 May 2013, <www.ivir.nl/publications/helberger/Paper_Freedom_of_expression.pdf> accessed on 20 July 2013.
[264] Bernal discusses "a right to roam the internet without data being gathered about you" (Bernal PA, *Do Deficiencies in Data Privacy Threaten Our Autonomy and if so, Can Informational Privacy Rights Meet this Threat?* (Ph.D thesis London School of Economics and Political Science) (Academic version 2011), 134).
[265] The New York Times is merely mentioned as an example.

New York Times website.[266] In sum, the long-term effects of legal limits on behavioural targeting for the economics of media are uncertain.

Prohibitions could also focus on the second phase of behavioural targeting: the storage and analysis of data. Current data protection law requires companies to delete data when the data are no longer "necessary" for the processing purpose.[267] A clearer rule could prohibit storing data for behavioural targeting longer than two days. This could help to ensure that profiles don't become too detailed. And there would be less data that can fall in the wrong hands. Evidently, regulating the retention period of data doesn't help if one thinks that the tracking itself is the main problem.

The law could also prohibit the sharing of personal data for behavioural targeting among companies. This could mitigate fears like being charged a higher health insurance rate because of web searches for diseases. A ban on data sharing could also help to make the data flows around behavioural targeting less opaque.

The law could also focus on the third phase of behavioural targeting: the use of data for targeted advertising. For instance, some people fear the effect of "filter bubbles": too much personalisation of advertising and other content might nudge people into a certain direction.[268] Should the use of behaviourally targeted and personalised messages be allowed in all circumstances? Is there reason for concern when political parties personalise behaviourally targeted messages?[269]

Should certain kinds of price discrimination be prohibited? Many people say they dislike the idea of personalised pricing, at least when it could lead to higher prices.[270] Should we prohibit online shops to adapt prices based on the profile of a website visitor? A counter argument is that personalised pricing might be a good thing, from an economic perspective.

Each of the ideas above is fraught with problems. Defining and agreeing on prohibitions would be hard. Prohibitions that aim to protect the greater good should be less controversial than those that protect people against themselves. But often a prohibition protects society and an individual at the same time. For instance, it could

---

[266] See about the changing power relations in the media landscape: Turow J, The Daily You. How the New Advertising Industry Is Defining Your Identity and Your Worth (Yale University Press 2012).

[267] Article 6(e) of the Data Protection Directive.

[268] Pariser E, *The Filter Bubble* (Penguin Viking 2011); Hildebrandt M and Gutwirth S (eds), *Profiling the European citizen: Cross-Disciplinary Perspectives* (Springer 2008). See for a critique on the fear for filter bubbles: Van Hoboken JVJ, *Search Engine Freedom: on the Implications of the Right to Freedom of Expression for the Legal Governance of Search Engines (Ph.D thesis University of Amsterdam)* (Information Law Series, Kluwer Law International 2013), chapter 10.

[269] See Barocas S, 'The Price of Precision: Voter Microtargeting and its Potential Harms to the Democratic Process' (2012) Proceedings of the First Edition Workshop on Politics, Elections and Data 31; Turow J and others, 'Americans Roundly Reject Tailored Political Advertising' (Annenberg School for Communication of the University of Pennsylvania) (July 2012) <www.asc.upenn.edu/news/Turow_Tailored_Political_Advertising.pdf> accessed 10 April 2013.

[270] Office of Fair Trading, 'Online Targeting of Advertising and Prices' (2010) <www.oft.gov.uk/shared_oft/business_leaflets/659703/OFT1231.pdf> accessed on 5 April 2013.

be argued that it's better for a democratic society if people can read online news without a fear of being tracked.

Another question is how prohibited practices should be defined. Would a prohibition of using any "health data" for behavioural targeting also cover daily visits to a website with gluten free recipes? If we would want to prohibit tracking on news services, how to define a news service? Would the ban apply to political blogs, and to online newspapers that only gossip about celebrities? Agreeing on prohibitions is hard, but that shouldn't be a reason to ignore the possibility.

An advantage of hard and fast rules is that they might be easier for companies than data protection law's open norms. "Delete everything after 2 days" might be easier to comply with than estimating when the data minimisation principle requires deletion. Clearly defined rules may also be easier to enforce.[271]

There are many precedents for prohibitions in law. In Europe for instance, there are minimum safety standards for products,[272] and some kinds of products are banned.[273] Minimum safety standards could be seen as bans of products that don't comply with the requirements. Many national consumer protection statutes contain a blacklist of contract terms that aren't enforceable.[274] Consumer law relies on a combination of empowerment rules (such as information disclosure on packaging) and prohibitions.

There might also be a middle ground between empowering and protecting people; between data protection law's informed consent approach and hard prohibitions. The law could use insights from behavioural economics. Thaler and Sunstein call this nudging: gently pushing people's behaviour in a certain direction, without actually limiting their freedom of choice.[275] For instance, the law could set a default of the most desired option, while leaving people free to change it.

---

[271] See on the lawmaker's choice between open and fuzzy norms on the one hand, and specific rules on the other hand: Baldwin R, Cave M and Lodge M, *Understanding Regulation: Theory, Strategy, and Practice* (2nd edition) (Oxford University Press 2011), chapter 11 and 14; Sunstein CR, 'Problems with Rules' (1995) 83(4) California Law Review 953.

[272] Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on General Product Safety (L 011, 15 January 2002, 0004-0017).

[273] For instance, novelty lighters are banned in the European Union (Commission Decision of 11 May 2006 requiring Member States to take measures to ensure that only lighters which are child-resistant are placed on the market and to prohibit the placing on the market of novelty lighters (notified under documents number C(2006) 1887 and number C(2006) 1887 COR) (L 198, 20 July 2006, 0041-0045) 2006/502/EC)

[274] Ebers M, 'Unfair Contract Terms Directive (93/13) ', in Schulte-Nölke H, Twigg-Flesner C and Ebers M (eds), *Consumer Law Compendium* <www.eu-consumer-law.org/study_en.cfm> accessed 10 April 2013, 344.

[275] They describe nudging as follows: "A nudge, as we will use the term, is any aspect of the choice architecture that alters people's behavior in a predictable way without forbidding any options or significantly changing their economic incentives. To count as a mere nudge, the intervention must be easy and cheap to avoid. Nudges are not mandates. Putting the fruit at eye level counts as a nudge. Banning junk food does not" (Sunstein CR and Thaler RH, *Nudge: Improving Decisions about Health, Wealth, and Happiness* (Yale University Press 2008), 6).

Nudges could be made stronger by using transaction costs strategically.[276] Say a majority of people disapproves of using any kind of health-related data for behavioural targeting. The law could prescribe an opt-in regime, and add transaction costs. For example, people can only opt in with a phone call. Transaction costs could come in different shades, to introduce different degrees of "stickiness" for the default. One mouse click might be enough to consent to relatively innocuous kinds of tracking, and four mouse clicks might be needed for more worrying practices. (As an aside: on the Youronlinechoices website of the Interactive Advertising Bureau, it takes three clicks and a waiting period of up to 30 seconds to opt out of receiving advertising that is behaviourally targeted.[277]) For some behavioural targeting practices, perhaps an opt-in should only be possible with a letter by registered mail.

Perhaps the law could build on the Do Not Track standard. Under European law, it's not allowed to track people that don't set a Do Not Track preference. In other words, in Europe Do Not Track implies an opt-in system for tracking. People could consent to a particular company tracking their online behaviour. The lawmaker could make the no-tracking default "stickier", by adding transaction costs to consenting to tracking.[278] Such a measure could be coupled with a prohibition of making a service dependent on consenting to behavioural targeting in certain circumstances.

In conclusion, two regulatory techniques were distinguished: empowering people and protecting people. Empowerment of the data subject implies, among other things, making informed consent more meaningful. Rules that aim at protection of the individual are also possible. Specific prohibitions could be introduced. Banning certain practices implies that the lawmaker must make difficult normative choices. Under the empowerment approach, such choices largely fall on the shoulders of individual internet users. Lastly, a middle ground between prohibitions and informed consent was discussed: sticky defaults. The next section summarises the findings of this paper and concludes.

---

[276] Thanks to Professor Bar-Gill for suggesting this line of thought, and for suggesting the phrase "using transaction costs strategically". If a nudge is made stronger by using transaction costs strategically, it might not count as a "nudge" anymore for Sunstein & Thaler, since it's not easy and cheap to avoid.

[277] First the visitor has to choose a country (click 1), then she must click on "your ad choices" (click 2). Next the visitor must wait until the website contacts the participating advertising networks. Then the visitor can opt out of receiving targeted advertising (click 3). See <www.youronlinechoices.com> accessed on 10 April 2013. See in more detail about the (non) user friendliness of opt-out systems: Leon P and others, 'Why Johnny Can't Opt Out: A Usability Evaluation of Tools to Limit Online Behavioral Advertising' (2012) Proceedings of the 2012 ACM Annual Conference on Human Factors in Computing Systems 589.

[278] Ayres I, 'Regulating Opt-Out: An Economic Theory of Altering Rules' (2011) 121(8) Yale Law Journal 2032.

7. Conclusion

European data protection law requires companies to obtain informed consent for the processing of personal data for behavioural targeting in most cases. There's a separate consent requirement for the use of tracking technologies. This paper discussed the following question. What are the policy implications of insights from behavioural economics in the context of consent to behavioural targeting?

People's choices regarding privacy can be analysed using economic theory. Consent to behavioural targeting could be seen as a trade-off: people often consent to a company processing their personal data in exchange for the use of a "free" service. However, information asymmetries hinder meaningful decisions.

Many people don't realise that their online behaviour is tracked. If somebody doesn't realise releasing personal data in exchange for the use of a "free" service, that "choice" can't be informed. But even if companies asked people consent for behavioural targeting, information asymmetry problems would remain. First, people often don't know what a company will do with their personal data. Second, if people knew, it would be hard to predict the consequences of future data usage. Third, people don't know the value of their personal data, so they don't know how much they "pay". In sum, making meaningful decisions about behavioural targeting is hard for people because of a lack of information.

Because of transaction costs, like the time it would take to inform oneself, the information asymmetry problem is hard to solve. Reading privacy policies would cost too much time, as they tend to be difficult to read and long. Some suggestions were made to mitigate the information asymmetry problems.

First, there's a need for education about behavioural targeting and online privacy in general. People can't really choose if they don't understand the question. Second, data protection law must be applied more vigorously. Companies that seek consent must do so in clear and straightforward language. Third, research is needed into better ways of presenting information to people. But even if all these measures were taken, considerable information asymmetries would probably remain. If people are asked to consent to data collection hundreds of times per day, even simple requests are overwhelming.

Moreover, insights from behavioural economics suggest that even fully informed people face problems making privacy choices in their own best interests. Many biases influence our decisions. For instance, people are myopic and tend to discount disadvantages in the future. If people can only use a service if they "consent" to behavioural targeting, they might ignore the costs of possible future privacy infringements, and choose for immediate gratification. Furthermore, people tend to stick with the default. Many other biases influence privacy decisions.

Data protection law has answers to only some of these problems. If consent would be implemented as requiring affirmative action of the data subject (an opt-in system), the status quo bias would nudge people towards privacy friendly choices. But myopia suggests that if the use of a service is made dependent on consenting to behavioural targeting, many people might consent, contrary to their own stated interests. The framing effect suggests that people can be pushed towards decisions that they might later regret. In sum, insights from behavioural economics cast doubt on the effectiveness of informed consent as a privacy protection measure. Many people click 'I agree' to any statement that is presented to them.

So what should the law do? A rather blunt reaction to myopia could be: prohibit companies from making the use of a service dependent on consenting to tracking. But sector-specific rules that prohibit certain behavioural targeting practices are also possible. However, prohibitions to protect people against themselves reek of unwarranted paternalism. On the other hand, it could be argued that some prohibitions would protect society as a whole. Some examples of possible prohibitions were mentioned. For instance, the tracking of children for behavioural targeting could be prohibited. Or it could be prohibited for online news services to engage in behavioural targeting. The examples show that it wouldn't be easy to agree on prohibitions.

Lastly, there might be a middle ground. Instead of introducing prohibitions, the lawmaker could use insights from behavioural economics. The law could set defaults, and make them stickier by adding transaction costs. For instance, the law could set formal requirements for consent, like a minimum of five mouse clicks, or a letter by registered mail. Such measures would leave freedom of choice intact, at least formally, but the status quo bias in combination with transaction costs would steer people towards privacy. When new rules are adopted, it can't be ruled out that some services that rely on income from behavioural targeting couldn't be offered for "free" anymore. This should be taken into account.

In sum, the lawmaker has a range of options. There will probably always be a large category of cases where relying on informed consent, in combination with data protection law's other safeguards, is the appropriate approach. For those cases, transparency and consent should be taken seriously. More effective ways of presenting information are needed. But this isn't enough. Merely relying on data protection law to protect people's privacy in the context of behavioural targeting doesn't seem sufficient. If we decide, after debate, that it's better for our society if certain practices don't happen, prohibitions may be the best answer.

* * *