

Improving Privacy Protection in the Area of Behavioural Targeting.
F.J. Zuiderveen Borgesius

‘Improving Privacy Protection in the area of Behavioural Targeting’

Frederik Zuiderveen Borgesius

Institute for Information Law (IViR), University of Amsterdam

F.J.ZuiderveenBorgesius@uva.nl

Short summary PhD thesis

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

Chapter 1 introduces the research question: how could European law improve privacy protection in the area of behavioural targeting, without being unduly prescriptive?

Chapter 2 explains what behavioural targeting is, by distinguishing five phases. During the first phase of behavioural targeting, firms track people's online behaviour. Second, firms store data about individuals. Third, firms analyse the data. Fourth, firms disclose data to other parties. In the fifth phase, data are used to target ads to specific individuals.

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

Chapter 4 gives an overview of the data protection principles. Data protection law is Europe's main legal tool to protect information privacy, and aims to ensure that personal data processing happens fairly and transparently. The chapter shows that there's a tension within data protection law between empowering and protecting the individual. This tension is a recurring theme in this study.

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

Chapter 6 discusses the role of informed consent in the regulation of behavioural targeting. Current law regarding behavioural targeting places a good deal of emphasis on informed consent. The e-Privacy Directive requires firms to obtain informed

consent for the use of most tracking technologies, such as cookies. Furthermore, in general data protection law, consent is one of the legal bases that a firm can rely on for personal data processing.

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

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

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

Chapter 10 summarises the main findings and answers the research question. There's no easy solution, but legal privacy protection can be improved in the area of

behavioural targeting. While current regulation emphasises empowerment, without much reflection on practical issues, this study argues for a combined approach of protecting and empowering people. To improve privacy protection, the data protection principles should be more strictly enforced. But the limited potential of informed consent as a privacy protection measure should be taken into account. Therefore, the lawmaker should give more attention to rules that protect, rather than empower, people.

* * *