‘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.

* * *

Short summary in Dutch

Betere privacybescherming op het gebied van behavioural targeting

Behavioural targeting is een vorm van marketing waarbij mensen op internet worden gevolgd, en er op basis van afgeleide interesses gerichte advertenties worden getoond aan mensen. Deze praktijk wordt door veel mensen ervaren als een aantasting van privacy. Behavioural targeting is al deels gereguleerd in Europese wetgeving. In dit verband zijn de belangrijkste Europese regels om online privacy te beschermen het toestemmingsvereiste in de e-Privacyrichtlijn voor tracking cookies en vergelijkbare volgtechnieken, en de regels in de algemene Richtlijn Bescherming Persoonsgegevens. In Nederland zijn deze regels geïmplementeerd in artikel 11.7a van de Telecommunicatiewet, respectievelijk in de Wet bescherming persoonsgegevens.

Door bedrijven te verplichten geïnformeerde toestemming te vragen voor behavioural targeting, probeert de wetgever mensen in staat te stellen keuzes te maken in hun eigen belang. Het idee is dat mensen zo zelf kunnen beslissen of, en in welke gevallen, zij een deel van hun privacy opgeven. Kortom, via geïnformeerde toestemming streeft de wetgever naar *empowerment* van het individu.

Inzichten uit *behavioural economics* (gedragseconomie) trekken de effectiviteit van deze *empowerment*-aanpak in twijfel. In de praktijk klikken veel mensen OK op elk verzoek dat zij tegenkomen op het internet. De wetgever zou zich daarom meer moeten richten op *protection*, het beschermen van mensen. In dit proefschrift wordt gepleit voor een gecombineerde aanpak van *empowerment* en *protection*.

In hoofdstuk 1 wordt de onderzoeksvraag toegelicht: welke maatregelen zou de EU wetgever kunnen nemen om de privacy van internetgebruikers beter te beschermen als het gaat om behavioural targeting, zonder daarbij onnodige lasten en regels op te leggen?

In hoofdstuk 2 wordt uitgelegd hoe behavioural targeting werkt. Deze studie onderscheidt vijf fasen in het proces van behavioural targeting. In fase 1 verzamelen bedrijven informatie over wat mensen doen op internet. Dit gebeurt vaak door middel van tracking cookies. Een cookie is een klein tekstbestand dat op de computer van een internetgebruiker geplaatst kan worden. Met behulp van tracking cookies kan een bedrijf iemands surfgedrag in kaart brengen. In fase 2 slaan bedrijven de informatie op. De informatie over een persoon is gekoppeld aan unieke identificatiecode, die in onder meer in een cookie kan worden opgenomen. In fase 3 worden de gegevens geanalyseerd. In fase 4 stellen bedrijven de gegevens ter beschikking aan adverteerders of aan andere bedrijven. In fase 5 tonen bedrijven gerichte, op vermeende individuele interesses gebaseerde, advertenties aan specifieke personen.

In hoofdstuk 3 worden de privacyproblemen geanalyseerd die het gevolg zijn van behavioural targeting. Privacy is moeilijk te definiëren. In deze studie worden drie perspectieven op privacy onderscheiden: privacy als beperkte toegang, privacy als zeggenschap of controle over persoonlijke informatie, en privacy als de vrijheid van onredelijke beperkingen op identiteitsvorming. Vanuit elk van de drie privacy-

perspectieven is behavioural targeting problematisch. Drie van de belangrijkste privacyproblemen veroorzaakt door behavioural targeting zijn (i) *chilling effects*, (ii) een gebrek aan controle over persoonlijke informatie, en (iii) het risico op discriminatie en manipulatie. Een *chilling effect* kan optreden als gevolg van grootschalige gegevensverzameling: mensen passen hun gedrag aan als zij weten dat hun activiteiten worden gevolgd. Het tweede privacyprobleem is dat mensen niet weten welke informatie over hen wordt verzameld, hoe deze informatie gebruikt wordt, en met wie deze wordt gedeeld. Hierdoor verliezen zij zeggenschap over de hen betreffende gegevens. Ten derde maakt behavioural targeting discriminatie mogelijk. Sommigen vrezen daarnaast dat behavioural targeting kan worden gebruikt om mensen te manipuleren. Gepersonaliseerde reclame zou zo effectief kunnen worden dat adverteerders een oneerlijk voordeel verkrijgen ten opzichte van consumenten.

In hoofdstuk 4 wordt een overzicht gegeven van het Europese juridische kader voor de verwerking van persoonsgegevens. Deze regels hebben als hoofddoel te bevorderen dat de verwerking van persoonsgegevens eerlijk en transparant gebeurt. Het hoofdstuk laat zien dat er een spanning bestaat in het gegevensbeschermingsrecht tussen *empowerment* en *protection* van mensen. Deze spanning is een terugkerend thema in dit onderzoek.

In hoofdstuk 5 wordt besproken of behavioural targeting binnen de werkingssfeer van het gegevensbeschermingsrecht valt. Veel bedrijven die aan behavioural targeting doen, zeggen dat het gegevensbeschermingsrecht niet van toepassing is op hun praktijken, omdat ze alleen “anonieme” gegevens verwerken. Europese gegevensbeschermingsautoriteiten (zoals het Nederlandse College Bescherming Persoonsgegevens), samenwerkend in de Artikel 29 Werkgroep, zeggen echter dat behavioural targeting doorgaans de verwerking van persoonsgegevens met zich meebrengt, ook als een bedrijf geen naam kan koppelen aan de gegevens over een individu. Als een bedrijf gegevens gebruikt om iemand te individualiseren of iemand te onderscheiden binnen een groep, dan zijn die gegevens persoonsgegevens volgens de Werkgroep. In deze studie wordt dit standpunt onderschreven.

In hoofdstuk 6 staat het concept van geïnformeerde toestemming centraal. Sinds 2009 volgt uit de e-Privacyrichtlijn, kort gezegd, dat tracking cookies slechts geplaatst mogen worden als de betrokkene toestemming heeft verleend, na te zijn voorzien van duidelijke en volledige informatie. Bovendien staat de Richtlijn Bescherming Persoonsgegevens bedrijven slechts toe om persoonsgegevens te verwerken, als zij de verwerking op toestemming of op een andere wettelijke grondslag kunnen baseren.

In hoofdstuk 7 worden de praktische problemen bij het geven van geïnformeerde toestemming voor behavioural targeting geanalyseerd. Uit onderzoek uit op het gebied van de rechtseconomie (*law and economics*) en de gedragseconomie (*behavioural economics*), en uit empirisch onderzoek naar hoe mensen keuzes maken over privacy, blijkt dat er in de praktijk vrijwel onoplosbare problemen zijn met geïnformeerde toestemming. Vrijwel niemand leest privacyverklaringen of toestemmingsverzoeken. Veel mensen klikken OK op vrijwel elk verzoek dat zij tegenkomen op het internet. Eigenlijk kan ook niet van mensen verwacht worden dat zij elk verzoek zouden lezen. Onderzoek toont aan dat het mensen enkele weken per jaar zou kosten om elke privacyverklaring die zij tegenkomen op het internet te lezen. Bovendien: zelfs als iemand een toestemmingsverzoek zou lezen en begrijpen, dan nog is er een grote kans dat hij of zij toch op OK klikt bij een privacy-onvriendelijke verzoek. De wet staat website-houders in veel gevallen toe om mensen een *take-it-or-leave-it* keuze te bieden. Zo installeren veel websites tracking-muren of cookie-muren – barrières waar mensen alleen langs komen als zij op toestaan dat er via de website tracking cookies worden geplaatst.

Er is daarom voor de wetgever reden tot ingrijpen. Gezien de beperkte mogelijkheden van geïnformeerde toestemming als privacybeschermingsmaatregel, wordt in deze studie gepleit voor een gecombineerde aanpak van *empowerment* en *protection* van mensen.

Overigens is het is onduidelijk of, vanuit een economisch perspectief, de maatschappij als geheel beter of slechter wordt van behavioural targeting. Ook is omstreden of behavioural targeting nodig is om “gratis” websites te financieren. Advertenties die niet gebaseerd zijn op behavioural targeting zijn ook mogelijk, zoals contextuele reclame: advertenties voor auto’s op websites over auto’s.

Hoofdstuk 8 bespreekt mogelijke maatregelen om mensen beter in staat te stellen om voor hun eigen belangen op te komen (*empowerment*). Om de informatieasymmetrie in de context van behavioural targeting te verminderen, zou het transparantiebeginsel beter gehandhaafd moeten worden. De wetgever zou moeten afdwingen dat toestemmingsverzoeken simpel, kort, en gemakkelijk te begrijpen zijn. Privacyverklaringen en toestemmingsverzoeken kunnen veel duidelijker en begrijpelijker worden geformuleerd. De bestaande regels over toestemming moeten strenger gehandhaafd worden. "Wie zwijgt stemt toe" zou niet geaccepteerd mogen worden.

In hoofdstuk 9 worden maatregelen toegelicht om het individu te beschermen (*protection*). Als de wetgeving voor de bescherming van persoonsgegevens volledig nageleefd zou worden, dan zouden mensen redelijke bescherming genieten, ook als zij OK klikken op elk toestemmingsverzoek. Hoewel toestemming een belangrijke rol speelt in het gegevensbeschermingsrecht, geeft toestemming bedrijven geen vrijbrief om met persoonsgegevens te doen wat zij willen. Ook als iemand toestemming heeft gegeven, dient het bedrijf nog te voldoen aan de overige eisen uit het gegevensbeschermingsrecht. Het gaat immers om dwingend recht. Zo eist de wet dat bedrijven persoonsgegevens beveiligen, en verbiedt de wet het gebruik van persoonsgegevens voor doelen die onverenigbaar zijn met het verzameldoel. Verder mogen bedrijven geen disproportionele hoeveelheden gegevens verzamelen en verwerken – ook niet na toestemming van het individu. Met betere handhaving en explicitering van de huidige normen, kan de wetgever een deel van de omvangrijke privacy-problemen adresseren. Maar dit is waarschijnlijk niet voldoende. Als de samenleving beter af is als bepaalde behavioural targeting praktijken niet plaatsvinden, dan zou de wetgever een verbod van dergelijke praktijken moeten overwegen.

Zo zouden tracking-muren verboden moeten worden voor publieke omroepen en voor overheidswebsites. In Nederland ligt nu een wetsvoorstel voor met een vergelijkbare regel. De wetgever zou ook een stap verder kunnen gaan, door alle commerciële dataverzameling voor behavoural targeting en vergelijkbare doelen te verbieden op overheidswebsites.

Hoofdstuk 10 bevat de conclusie. Er bestaat geen wondermiddel voor privacybescherming als het gaat om behavioural targeting. Terwijl de huidige regelgeving veel nadruk legt op *empowerment,* zonder veel reflectie op de praktijk, zou een gecombineerde aanpak van *protection* en *empowerment* effectiever zijn. Om de privacy van mensen beter te beschermen, moet het gegevensbeschermingsrecht strikter worden gehandhaafd. Maar omdat geïnformeerde toestemming als privacybeschermingsmaatregel tekort schiet, moet de wetgever niet al te hoge verwachtingen hebben van empowerment. Er moet ook voldoende aandacht gegeven worden aan het beschermen van mensen.

* * *