Behavioral Targeting
Legal Developments in Europe and the Netherlands

Frederik Zuiderveen Borgesius

Ph.D researcher, focusing on behavioral targeting and privacy law
Institute for Information Law, University of Amsterdam
F.J.ZuiderveenBorgesius [at] uva.nl

Position Paper for the W3C Do Not Track Workshop, November 2012

Introduction

This paper discusses legal developments in Europe and the Netherlands. Recent decisions show that European data protection law, or privacy law, applies to behavioral targeting in most cases. Dutch law explicitly presumes that data protection law applies to behavioral targeting. This means that companies have to comply with data protection law's fair information principles. For example, companies must refrain from secret or excessive data collection. Perhaps the principles could provide inspiration for future W3C projects. Could technology design foster fair information processing?

I would like to speak at the workshop on such issues, and look forward to discussing them with the workshop participants.

Legal developments in Europe

In Europe, the right to privacy and the right data protection are fundamental rights.[1] Like most privacy laws in the world, European data protection law is triggered when a company processes "personal data". Many behavioral targeting companies process pseudonymous profiles (individual but nameless profiles). Do these companies process "personal data"? Yes, say European data protection authorities. This is compatible with case law of the highest court of the European Union.

[1] Article 7 and 8 of the Charter of Fundamental Rights of the European Union, and article 8 of the European Convention of Human Rights.

The European Data Protection Directive defines personal data as: “any information relating to an identified or identifiable natural person ('data subject').” A person is identifiable when he or she can be directly or indirectly identified. To determine whether a person is identifiable, it’s not decisive whether it’s the company holding the data, or another party that can identify a person.[2]

The Court of Justice of the European Union, the highest authority on the interpretation of European Law, has not ruled on behavioral targeting yet. But there is relevant case law. The discussion about behavioral targeting is similar to the debate about IP addresses. In November 2011, the Court ruled that the IP addresses in that case are personal data.[3] The Court thus reaffirms that information without a name can constitute personal data.[4]

European national Data Protection Authorities, cooperating in the Article 29 Working Party, say that data that can distinguish a person within a group are personal data.[5] The Working party adds that pseudonymous profiles, 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 known”.[6] Although not legally binding, the Working Party’s opinions are influential, since it usually takes decisions by consensus.

Many, although not all,[7] commentators agree that data protection law applies to behavioral targeting.[8] The Privacy Commissioner of Canada[9] and the American Federal Trade Commission reach similar conclusions.[10] The proposal for a new European Data Protection Regulation also applies to pseudonymous profiles and “online identifiers” in most cases.[11] Taking all this into account, it seems safe to assume that data protection law generally applies to behavioral targeting.

Legal developments in the Netherlands

In June 2012, the new Dutch Telecommunications Act entered into effect.[12] The Dutch Act essentially copies the ‘cookie clause’ of the European e-Privacy Directive,[13] and only allows the use of tracking technologies after prior informed consent of the user. (A translation of the

[2] Article 2(a) and recital 26 of the Data Protection Directive 95/46/EC.
[3] CJEU, 24 November 2011, Case C70/10 (Scarlet/Sabam), par. 51.
[4] See for example CJEU, 9 November 2010, Joined cases C-92/09 and C-93/09 (Volker und Markus Schecke and Eifert), par 52; CJEU, 24 November 2011, Joined cases C-486 and C-469-10 (Asociación Nacional de Establecimientos Financieros de Crédit), par. 42.
[5] Article 29 Working Party, Opinion 4/2007 on the concept of personal data (WP 136). 20 June 2007, p. 12-20.
[6] Article 29 Working Party, Opinion 2/2010 on online behavioral advertising (WP 171). 22 June 2010, p. 9.
[7] See e.g.: G-J. Zwenne, Over IP-adressen en persoonsgegevens, en het verschil tussen individualiseren en identificeren (About IP addresses and personal data, and the difference between individuating and identifying), Tijdschrift voor Internetrecht, February 2011, p. 4-9.
[8] See e.g.: P. Traung, ‘EU Law on Spyware, Web Bugs, Cookies, etc., Revisited: Article 5 of the Directive on Privacy and Electronic Communications’, Business Law Review 2010-31, p. 216–228.
[9] Office of the Privacy Commissioner of Canada, Privacy and Online Behavioural Advertising (Guidelines), December 2011, www.priv.gc.ca/information/guide/2011/gl_ba_1112_e.pdf, p. 2.
[10] The FTC says that privacy rules should apply when a company can reasonably link information to a consumer or a device (FTC, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers (March 2012), www.ftc.gov/os/2012/03/120326privacyreport.pdf, p. 22).
[11] The Regulation’s definition of personal data includes “online identifiers” in the list of examples that may be used to identify a person (article 4(1)). But see also recital 24 (Proposal for a regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data, COM(2012) 11 final).
[12] The official Dutch text can be found at: http://wetten.overheid.nl/BWBR0009950.
[13] Directive 2002/58/EC, as amended by Directive 2009/136/EC.

provision is in the appendix). Companies may not infer consent from inactivity of the user. Silence is not consent. The Dutch provision is technology-neutral: it applies to cookies and other tracking technologies such as device fingerprinting.[14] Without their consent, Dutch internet users may not be tracked. This also applies to users that haven't set a Do Not Track preference in their browser.

But the Dutch Act goes further. It also contains a legal presumption regarding tracking technologies for behavioral targeting. The use of such technologies is presumed to entail the processing of personal data. The legal presumption shifts the burden of proof. It's up to behavioral targeting companies to prove that they don't process personal data. The provision basically codifies the view of the European data protection authorities. The Dutch legislator added the legal presumption to emphasize that default browser settings could never be interpreted as consent for tracking cookies or similar technologies.[15]

The Dutch Telecommunications Authority OPTA oversees compliance with the provision. OPTA says that the provision also applies to foreign website publishers and behavioral targeting companies. OPTA can issue fines of up to 450.000 euro.[16]

If a company processes "personal data", the Dutch Data Protection Authority also enters the picture. Because of the legal presumption, the Data Protection Authority doesn't have to prove that a company employing tracking technologies processes personal data. The Data Protection Authority can't impose fines, but it can impose large preventive penalties if a company doesn't comply with its administrative orders.[17]

The legal presumption enters into effect on 1 January 2013.[18] The Dutch Senate said that this delay could enable the online marketing industry to come up with a user-friendly system to obtain consent, for instance by developing a meaningful Do Not Track standard.[19]

Fair Information Processing

If a company processes personal data, it has to comply with all the data protection principles. Most importantly, data processing has to be transparent. Secret data collection is not allowed.[20] But there's more. For example, the data minimization principle prohibits the collection or storage of excessive amounts of data.[21] The security principle requires companies to ensure a reasonable level of security of data they process.[22] The law grants people whose data are being processed several rights. For instance, everyone has the right of

[14] Eerste Kamer, vergaderjaar 2011–2012, 32 549, G, 17 February 2012, p. 4-6 (answers of Minister of Economic Affairs, Agriculture and Innovation to the Senate).
[15] Explanatory memorandum to the amendment by Van Bemmel and Van Dam to the Bill to amend the Telecommunications Act (Dutch Parliament 2010-2011, 32549, nr. 39.
[16] OPTA, 'Veelgestelde vragen over de nieuwe cookieregels. Update' (Frequently asked questions about the new cookie rules. Update'), 2 August 2012 www.opta.nl/nl/actueel/alle-publicaties/publicatie/?id=3636, p. 3, p. 9.
[17] The website of the Data Protection Authority is at www.dutchdpa.nl.
[18] Article VII, 1(c) of the Besluit implementatie herziene telecommunicatierichtlijnen (decision implementation telecommunications directives), https://zoek.officielebekendmakingen.nl/stb-2012-236.html.
[19] Handelingen Eerste Kamer van de Staten Generaal, Vergaderjaar 2011-2012, Vergaderingnummer 28, Telecommunicatiewet en Wegenverkeerswet 1994, 32549, https://zoek.officielebekendmakingen.nl/h-ek-20112012-28-9.pdf.
[20] Article 10 and 11 of the Data protection Directive.
[21] Article 6(c) and 6(e) of the Data Protection Directive.
[22] Article 16 and 17 of the Data protection Directive.

access to data that have been collected concerning him or her, and the right to have data rectified. People can always withdraw their consent.[23]
At the core of the European data protection regime are the fair information principles. These forty-year old principles are well established.[24] The principles are contained in international instruments such as the OECD Data Processing Guidelines,[25] and the Data Protection Convention (ratified by 44 countries).[26] Although the national implementation varies, the principles express a worldwide consensus on how to ensure fair information processing.

Conclusion

In sum, European data protection law most probably applies to behavioral targeting. Dutch law is more explicit and presumes this is the case. Therefore companies must comply with data protection law's fair information principles.

Perhaps the fair information principles could provide inspiration for future W3C projects. Could the W3C help to put the principles in practice? For instance, maybe technology could help to make data processing transparent. Or technology might enable people's right to access data concerning them. As the Mission of the W3C puts it: "technology design can foster trust and confidence."[27]

* * *

[23] Article 12, 24 and 15 of the Data protection Directive; article 8 of the EU Charter of Fundamental Rights.
[24] See for an early example: US Department of Health Education and Welfare (HEW), Records, computers and the rights of citizens: report of the Secretary's Advisors Committee on Automated Personal Data Systems, Washington: US Government Printing Office 1973.
[25] See www.oecd.org/internet/interneteconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.
[26] See www.coe.int/dataprotection.
[27] W3C, Web of trust, http://www.w3.org/Consortium/mission#principles.

APPENDIX

Article 11.7a of the Dutch Telecommunications Act (unofficial translation by the author)

1. Without prejudice to the Data Protection Act, anyone who wishes to access information that has been stored in a user's terminal equipment, or wishes to store information in a user's terminal equipment via an electronic communications network, must:

a. provide the user with clear and complete information, in accordance with the Data Protection Act, at least about the purposes for which he wishes to access the information concerned and/or for which he wishes to store information, and

b. have obtained the user's consent for this activity.

Any activity as referred to in the preamble, with a view to collecting, analyzing or combining information about the user's or subscriber's use of various services of the information society, for commercial, charitable or idealistic purposes, is presumed to be the processing of personal data, as defined in article 1(b) of the Data Protection Act.

2. The requirements of paragraph 1 a and b shall also apply in the event that (other than by means of an electronic communications network) anyone causes information to be stored, or information stored in the terminal equipment to be accessed, by means of an electronic communications network.

3. The provisions of the first and second paragraph shall not apply if they relate to technical storage of, or access to, information, with the sole purpose of:

a. carrying out the communication over an electronic communications network, or

b. providing a service of the information society requested by the user, and the storage of, or access to, information is strictly necessary.

4. Regarding the requirements set out in paragraph 1(a) and (b), further rules can be given by governmental decree in agreement with Our Minister of Justice and Security. The Data Protection Authority shall be consulted about the draft of such a governmental decree.

* * *