

The way the cookie crumbles: online tracking meets behavioural economics

Ignacio N. Cofone*

ABSTRACT

Limitations on online tracking are object of a regulatory debate that has shifted to the use of default rules to enhance privacy. The European Union implemented this idea with the Cookies Directive. The Directive aims to change the default system for tracking and move to an opt-in system in which data subjects must agree to it beforehand. This article evaluates the Directive's implementation across Member States and studies the cases of the Netherlands and the UK. It then draws from the behavioural economics literature on default rules to evaluate these regulations and to consider whether it is possible to implement the policy in a way that avoids some of the problems they faced.

KEYWORDS: online tracking, online privacy, cookie law, data protection, default rules, consumer choice

INTRODUCTION

Advertisers, and in particular online behavioural advertisers, receive considerable benefits from tracking devices such as cookies. Unlike mass advertising techniques, such as billboards, the Internet is able to personalize content. Having more information about data subjects' interests, companies can increase the relevance of advertisements, targeting the particular interests of the person to whom an advertisement is shown. This increment in relevance allows for more sales and higher rents for advertising spots, increasing revenue for both sellers and websites. The click-through rate of advertisements (fraction of visitors that click on them), commonly used as a measure of their success, has been shown to increase by approximately 670 per cent with online behavioural advertisement compared to traditional advertisement.¹

* Resident Fellow, Yale Law School, Information Society Project; E-mail: ignacio.cofone@yale.edu. A previous version of this paper was presented at the 7th Privacy Law Scholars Conference (Washington DC). I am grateful to Michael Faure, Klaus Heine, Tobias Hlobil, Joasia Luzak, Aleecia McDonald, Stephan Michel, Sjoera Nas, Sharon Oded, Alessio Paccos, Robert Sloan, Jim Tierney, Ann-Sophie Vandenberghe, Louis Visscher and two anonymous referees for their comments and suggestions. I gratefully acknowledge financial support from Erasmus University Trustfunds. All errors remain my own.

1 Jun Yan and others, 'How Much Can Behavioral Targeting Help Online Advertising?', *Proceedings of the Eighteenth International Conference on World Wide Web* (ACM 2009).

The most common devices for this function are HTTP cookies. Cookies are small files that websites store in their visitors' devices. They allow these websites to identify the device when it visits the website again, remembering some information about the interaction.² There are two main types of cookies. Session cookies disappear when the browser is closed, while persistent or permanent cookies remain in storage.³ Data subjects who know how, can delete (permanent) cookies by using options in their browsers or removing them directly from the operating systems in their devices.

Cookies can also present benefits for data subjects. They make navigation faster, obviate the need to enter information such as language preference or username and password repeatedly, and allow for useful features such as a 'shopping cart'.⁴ They sometimes also increase the relevance of what is shown to a data subject, disregarding useless information and potentially saving her time⁵—such as in Google searches and in advertisements that the data subject might genuinely be interested in.

The main disadvantage of tracking devices is that they can make pieces of information public that people prefer to keep private, raising privacy concerns. This is especially so regarding sensitive information, which typically consists of information that could be a basis for discrimination, such as ethnicity, political opinions, sexual orientation or religious beliefs.

This article draws on the experience of the European Union (EU) and the behavioural economics literature on default rules to shed light on how we can improve existing regulations on online tracking devices, including cookies. It argues that one country effectively prohibited tracking without a previous and explicit manifestation of consent, and it faced difficulties in implementing this requirement because data subjects were framed by websites into opting into the tracking system.

This framework will lead to some suggestions regarding policy. What the literature calls an active choice system is a strong candidate to achieve the goals of default-based policies in this case. Additionally, price theory seems to indicate that regulations could have undesirable unintended consequences unless they treat different kinds of cookies in a different way, in particular session cookies and permanent cookies. Finally, a way of tackling what the default rules framework indicates as a central weakness of the policy's current implementations is targeting web browsers. They have fewer incentives to frame data subjects than do websites, as the policy's enforcing agents, even if they are not data controllers.

The next section reviews the online tracking policy debate and its suggested solutions. Section 'Implementations' explains the regulations made under the framework of the EU directives, with particular attention to the Netherlands and the UK.

2 Weihong Peng and Jenniffer Cigna, 'HTTP Cookies. A Promising Technology' (2000) 24 *Online Information Review* 150; Windows Development Center, 'HTTP Cookies' <[https://msdn.microsoft.com/en-us/library/windows/desktop/aa384321\(v=vs.85\).aspx](https://msdn.microsoft.com/en-us/library/windows/desktop/aa384321(v=vs.85).aspx)> accessed 9 July 2016.

3 EU Cookie Law Help, 'What's the Difference Between a Session Cookie and a Persistent Cookie?' <<http://eucookielaw.org.uk/session-cookies-and-persistent-cookies>> accessed 9 July 2016. Persistent cookies have some special types, such as third-party cookies, which automatically send the information they contain to other parties.

4 Peng and Cigna (n 2).

5 *ibid.*

Section 'Regulatory Default Rules' evaluates them from a behavioural economics perspective. The next section provides policy suggestions, and the final section concludes.

POLICY DEBATE

Preliminary considerations

The central polemic that online tracking devices generate is that they are installed on data subjects' devices without their explicit consent, which often means that they are installed without their consent at all.⁶ Additionally, it has become a common practice to utilize third-party cookies, which are considered especially problematic because they allow data subjects' data to be directly aggregated by a different website or advertising company than the one the data subject interacts with, often without her awareness.

Unlike social networks, where data subjects share their information and often know who has it in storage, in the case of tracking devices it is possible that in the absence of regulation data subjects ignore who collects their personal information, and who stores it. While social networks are familiar to the data subjects whose information they retain, that is not the case for data brokers, which are not consumer-facing.

These features can, on top of the societal costs produced by the potential individual harm derived from privacy breaches, lead data subjects to consider the Internet as an unsafe environment. This can make them equate all advertising with spam or attempt to block all advertising out of a concern for privacy, which is an undesirable result for all agents in the interaction. This leads to the question of whether regulation should allow websites and advertisers to continue tracking data subjects without their knowledge or consent.⁷

The EU directives

The regulatory efforts regarding tracking devices such as cookies after the Data Protection Directive⁸ started in Europe with the e-Privacy Directive,⁹ and the Cookies Directive (sometimes called Electronic Communications Framework Directive),¹⁰ and country-level regulations made on their basis.

The Data Protection Directive gave users a right to refuse tracking. In a behavioural economics framework, this can be seen as implicitly adopting an opt-out system, where data subjects are considered to have consented to the installation of

6 Joasia Luzak, 'Much Ado about Cookies: The European Debate on the New Provisions of the ePrivacy Directive Regarding Cookies' (2013) 21 ERPL 221.

7 Lauren Willis, 'Why Not Privacy By Default?' (2014) 29 Berkeley Tech LJ 61.

8 Directive 1995/46/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.

9 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

10 Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws.

cookies unless they indicate otherwise, but have to be offered the choice to opt-out.¹¹ The system had the problem that data subjects lacked an easy way to exercise the refusal.

For the e-Privacy Directive, there was a debate on whether there should be a change to an opt-in system requiring data subjects' prior explicit consent to install tracking devices. The opt-out system was however maintained due to the concern that the change would hinder electronic commerce.¹² As a result, Article 5(3) of the e-Privacy Directive reinforced the right to refuse tracking,¹³ leaving data collectors with two main obligations: to provide information about the purposes of information collection and to give data subjects the right to refuse it (opt-out).¹⁴

The Cookies Directive changed Article 5(3) of the e-Privacy Directive. The new article requires that data subjects give their consent when technologies that collect information are installed. The article indicates that consent has to be given previously, since although the word 'previous consent' is not used, it refers to consent that 'has [been] given'.¹⁵

These regulations were complemented with the Working Document 02/2013 ('providing guidance on obtaining consent for cookies'), which requires that data subjects are offered a meaningful choice and that websites obtain their consent before installing any cookies. According to the Article 29 Working Party, the EU moved with the new Article 5(3) into an opt-in system.¹⁶ Still, the article's wording does not rule-out the possibility of implicit consent, only requiring it to be prior. In the use of the terms by its interpretative authority, it seems that for an opt-in system to be in force, only previous consent is necessary, making it possible to have an opt-in system with either implicit or explicit consent.

The debate on tracking devices as a subject of regulatory concern emerges in the framework of data protection. The Charter of Fundamental Rights of the European Union recognizes in its Article 8 the protection of personal data as a fundamental right, highlighting the importance of consent,¹⁷ and the Digital Agenda for Europe 2020 places privacy and data protection in the Internet as a high-priority topic.¹⁸

11 Luzak (n 6).

12 Sylvia Mercado Kierkegaard, 'How the Cookies (almost) Crumbled: Privacy & Lobbyism' (2005) 21 CLS Rev 310.

13 Frederic Debussere, 'The EU e-Privacy Directive: A Monstrous Attempt to Starve the Cookie Monster?' (2005) 13 IJLIT 70.

14 The directive is meant to be technology-neutral and does not only concern cookies but also the tracking of data subjects by any other means. This said, the directive refers to 'the storing of information, or the gaining of access to information already stored', which limits its scope as it excludes tracking technologies that do not store information in a device nor retrieve information that is stored, such as some cases of fingerprinting or IP addresses. Peter Eckersley, 'How Unique Is Your Web Browser?', *Privacy Enhancing Technologies Symposium* (Springer Lecture Notes in Computer Science 2010).

15 Art 13 of the directive on unsolicited communications also requires prior but not explicit consent.

16 Working Party on the Protection of Individuals with regards to the Processing of Personal Data, 'Opinion 2/2010 on Online Behavioral Advertising' (Brussels, 22 June 2010) 13; Working Party on the Protection of Individuals with regards to the Processing of Personal Data, 'Opinion 15/2011 on the Definition of Consent' (Brussels, 13 July 2011) 9, 30.

17 Art 8.2 (on protection of personal data).

18 European Commission, 'Digital Agenda for Europe. A Europe 2020 Initiative' <<http://ec.europa.eu/digital-agenda/>>. pillar III, action 35, at <<http://ec.europa.eu/digital-agenda/en/pillar-iii-trust-security/action-35-guidance-implementation-telecoms-rules-privacy>>.

Article 29 Working Party has stated that control over personal information is central for data protection, where control is commonly instrumented by consent.¹⁹ Consent is additionally mentioned as determinant of lawfulness in the Data Protection Directive,²⁰ to which the e-Privacy Directive and the Cookies Directive refer.²¹ Additionally, Article 5(1), which determines the rationale of Article 5(3), focuses on requiring consent to intercept communications. In this context, the aim of these regulations seems to be to ensure data subjects' informed consent as a requirement for online tracking.

IMPLEMENTATIONS

Differing implementations

The e-Privacy Directive is a minimum harmonization directive,²² so Member States can establish different levels of protection. Most Member States modified their legislations to adjust to an opt-in system after the Directive was passed, either requiring implicit or explicit consent. Some of them, however, have chosen to stay within an opt-out system, in a different interpretation of the amended e-Privacy Directive than that of the Article 29 Working Party or, more likely, in breach of the Directive, rendering them non-compliant.

Among them, the Netherlands seems to have chosen the most demanding system (opt-in with explicit consent).²³ It can be useful to evaluate its regulation further and to compare it with an example of the most widespread system (opt-in with implicit consent).

The British regulation was chosen for this comparison. Both the Netherlands and the UK have adopted Article 5(3) of the Directive following the wording of the e-Privacy Directive almost literally in their legislations, and have undergone significant regulatory efforts to implement it. Like the Netherlands, the UK regulated the issue in a complete and detailed way that helps avoid ambiguities. In addition, the British regulation is arguably the most complete of those that allow implicit consent. It has been often taken by other Member States as a reference and it is cited directly by some, like the French regulation.

The Dutch regulation

In the Netherlands, the right to refuse cookies exists since 2004 (two years after the e-Privacy Directive), having been established by the ministerial decree Decision on

19 'Opinion 15/2011 on the Definition of Consent' (n 16). A29WP, 'Opinion 2/2013 on Providing Guidance on Obtaining Consent for Cookies' (2013).

20 Directive 1995/46/EC, recital 30. The Data Protection Directive establishes that companies need a legitimizing basis to collect personal data, of which the most common is consent. See Directive 1995/46/EC, Arts 2(h) and 6(a). See also Working Party on the Protection of Individuals with regards to the Processing of Personal Data, 'Opinion 03/2013 on Purpose Limitation' (Brussels, 2 October 2013) 1.

21 While the directive mentions the importance of explicit consent (recital 33), it does not discard the possibility to manifest it implicitly, defining it as 'any freely given specific and informed indication of his wishes by which the data subject signifies his agreement'. Directive 1995/46/EC, Art 2(h).

22 This means that EU Member States must respect the established level of protection as a minimum, while they can choose a higher level of protection.

23 See Appendix.

Universal Services and End-user Interests (*Besluit Universele Dienstverlening en Eindgebruikersbelangen*). The Directive's implementation came in place with the modification of Article 11.7a of the Dutch telecommunications law (*Telecommunicatiewet*) on 5 June 2012, which works in the framework of the Dutch Data Protection Act.²⁴ The new article, in line with the modification of Article 5(3) of the e-Privacy Directive, states that websites cannot install cookies in data subjects' devices without prior and specific consent (terms used by the Directive).

It is noticeable that the article, like the directive on which it is based (Cookies Directive), does not require consent to be explicit.²⁵ It was the National Regulatory Authority in charge of supervising the implementation of the Dutch telecommunications law (OPTA) who added this requirement in its guidelines.²⁶ The authority considered that the Dutch Data Protection Act—which states in its Article 23a that explicit consent is required for the collection of personal data—is applicable to tracking technologies in telecommunications and, in particular, to cookies. The obvious objection to this interpretation is that not all cookies collect this type of information, but the Dutch authority applied a reverse burden of proof according to which all cookies are considered to carry personal data unless proved otherwise by the data collector.²⁷ This was a controversial measure since, although it is usual for regulatory authorities to specify the application of a national law, it is unusual for them to add a new and significant requirement of this sort.

To comply with the regulation, websites do not install cookies in the visitor's device upon entering, and display a banner asking whether the visitor allows for the installation of cookies. When a website has asked a visitor her consent, this can be stored in a cookie in the visitor's device avoiding the need to ask again the next time the website is used—although the visitor can 'opt-out' again by deleting the cookie that stored her consent. So, if the visitor clicks on 'yes', she will not be asked again. However, if she clicks on 'no' she will be re-asked every time she visits the website since, as installing cookies is forbidden, the negative answer remains unrecorded.

If the visitor refuses the installation of cookies, the website is allowed under the Dutch Regulation—same as in the e-Privacy Directive²⁸—to block access.²⁹ This disposition became known as the 'cookie wall'.

In sum, the Dutch regulation not only adopts the wording of the Directive almost literally, but goes a step further in the implementation of an opt-in system by requiring explicit consent unless the website proves no personal data is being collected.

Disappointments and modification

When the Netherlands incorporated the opt-in system with explicit consent for cookies, there were several complaints about the regulation. From the industry's side,

24 *Telecommunicatiewet*, Arts 8 and 33.

25 Joasia Luzak, 'Privacy Notice for Dummies? Towards European Guidelines on How to Give "Clear and Comprehensive Information" on the Cookies' Use in Order to Protect the Internet Users' Right to Online Privacy' (2014) 37 JCP 91.

26 OPTA, 'Veelgestelde Vragen over de Cookieregels' (2013).

27 *ibid.*

28 Directive 2002/58/EC, recital 25.

29 OPTA (n 26) 4.

it was stated that the regulation is ‘a very hard-to-explain deviation from the European directive, which doesn’t help anybody and makes it more complicated for both us and for the consumer’.³⁰ Before the law was passed, stakeholders formally complained that the cookie law is not only excessive for the directive’s aim but also goes beyond protecting personal information.³¹ The law was deemed especially problematic because Dutch public media companies are required to reach a certain percentage of the population, which they partly do via their websites, and the impossibility to install any type of cookies prevents them from monitoring how many people view their content.

Similarly, consumers seemed dissatisfied. Consumer associations have complained about what became known as the ‘cookie wall’ claiming that it has been mainly an annoyance for Internet users, and requested privacy protection to be matched by user-friendliness.³²

Sectors of the public opinion seemed dissatisfied with the regulation as well. Some have stated that the law was a failure due to its impracticality.³³ Others stated that the law misses the point entirely, since what is relevant for privacy is anonymity.³⁴ It was reported that consumers found the regulation annoying and unhelpful, and that it led them to mindlessly click to allow cookies every time they attempt to enter a website, being useless for its purpose.³⁵

Dutch academics have called the regulation a ‘policy fiasco of impressive dimensions’.³⁶ It has also been stated that the regulation’s main effect is making services more difficult to be offered³⁷ and that it hinders e-commerce both within and outside the Netherlands.³⁸

In addition, compliance has been low. A large amount of websites have breached the law and installed prohibited cookies in their visitors’ computers,³⁹ including the websites of most political parties that voted in favour of it⁴⁰ and of the government itself.⁴¹

When faced with these results, a large fraction of political parties who originally voted in favour of the law objected to its continuation. On 21 November 2012, D66 filed a proposal to change the regime because they considered the current regime too strict and unclear, and proposed to change it for an informed consent

30 Matt Steinglass, ‘Dutch Cookie Law May Lead to Online Exodus’ *TechHub* (21 June 2011).

31 Jan Driessen and others, ‘Verzoek Tot Inhoudelijke Behandeling Wijziging van de Telecommunicatiewet’ (Amsterdam; 3 July 2011).

32 Stephan Loerke, ‘The Dutch Find a Lighter Touch on Internet Privacy Laws’ *AdAge* (3 July 2013).

33 Arnoud Groot, ‘“Naïeve” Cookiewet Loopt Achter de Feiten Aan’ *Emerce* (4 November 2010); ‘Mislukte Cookiewet Is Een Wijze Les’ *NetKwesties* (11 April 2013).

34 Freek Vos, ‘Waar Maakt Iedereen Zich Zo Druk over? Leve de Cookies!’ *Volkscrant* (17 October 2012).

35 ‘Wetgever Maakt Surfen Onmogelijk’ *Financieel Dagblad* (11 June 2010).

36 Natali Helberger, ‘Freedom of Expression and the Dutch Cookie-Wall’ (2013) 1.

37 Bart van der Sloot, ‘Je Geld of Je Gegevens: De Keuze Tussen Privacybescherming En Gratis Internetdiensten’ (2011) 86 *Nederlands Juristenblad* 1493.

38 Gerrit-Jan Zwenne and Maxime Verhagen, ‘Dutch Cookie Law to Affect Businesses Outside Holland’ (2011) 13 *ECL & P* 1.

39 Arnoud Engelfriet, ‘Websites Negeren Massaal de Cookiewet’ *cookierecht* (13 July 2012).

40 Robert van Hittersum, ‘Dutch Political Parties Violate Their Own Cookie Law’ *FleishmanHillard* (7 June 2012).

41 ‘Opta Overtreedt Eigen Cookie-Regels’ *NU* (26 October 2012).

approach.⁴² Later on, both VVD and PvdA stated that the regulation was unworkable, and called it a 'cookie hostage' (*cookiegijzeling*) that must be put to an end.⁴³

These circumstances led to the Dutch Minister of Economic Affairs publishing a letter on 20 May 2013 containing a revision of the regulation.⁴⁴ The revision incorporates two changes: (i) it allows websites to let users show consent by clicking in any part of the website if it is clearly shown to them that doing so signifies consent and (ii) it allows analytics (cookies that do not track individual behaviour) without requiring consent.⁴⁵

This means, in practice, that the Dutch regulation is moving to a system of implicit consent. The Netherlands will join the majority of EU Member States in their implementation of the e-Privacy Directive. Until it finally does, the current regulation applies.

Implicit consent in the British regulation

As mentioned above, a useful case of implementation to compare with the Netherlands is that of the UK.

The UK implemented its regulation on cookies by an amendment in the Regulation 6 of the Privacy and Electronic Communications Regulations (PECR) on 26 May 2011. The amended regulation follows the language of the directive and requires in subsection 2(b) that the data subject 'has given his or her consent', while the previous disposition only required that the data subject is given an opportunity to refuse (opt-out).

However, with the amendment of section 2 of Regulation 6 PECR to match the language of the amended e-Privacy Directive, section 3 was also amended redefining consent. The amended section 3 states that data subjects can signify consent when they make changes in the Internet browser or some other program, hence allowing for implicit consent.

The Information Commissioner's Office (ICO) issued detailed guidelines in May 2012 on how websites should gather data subject's consent about cookies.

Regarding the timing of consent, the guidelines state that 'it is difficult to see that a good argument could be made that agreement to an action could be obtained after the activity the agreement is needed for has already occurred. This is not the generally accepted way in which consent works in other areas, and is not what users will expect'.⁴⁶ However, they only require consent to be prior 'whenever possible'.⁴⁷

42 'Voorstel Voor Ruimere Cookiewet' *NU* (21 November 2012); 'Kamp (EZ) Gaat Cookievoorstel D66 Bestuderen' *Emerce* (22 November 2012).

43 'Kamer Wil Einde Pop-Ups Door Cookiewet' *NU* (13 February 2013); 'Meerderheid Tweede Kamer Wil Einde Aan Cookie-Popups' *Tweakers* (13 February 2013).

44 Henk Kamp, 'Kamerbrief over Analytische Cookies En Artikel 11.7a van de Telecommunicatiewet' (Amsterdam; 20 December 2012).

45 'Cookiewet Versoepeld: Verplichte Melding Voor Minder Cookies' *Volkskrant* (20 December 2012).

46 Information Commissioner's Office, 'Guidance on the Rules on Use of Cookies and Similar Technologies' (London; 1 May 2012) 1, 5.

47 *ibid* 5.

The ICO guidelines, in line with Regulation 6 PECR, do not require explicit consent, and allow interpreting that implicit consent was given when visitors take actions that indicate so, such as visiting a website when cookies were not blocked. The British ICO has stated in this respect that ‘implied consent has always been a reasonable proposition in the context of data protection law and privacy regulation and it remains so in the context of storage of information or access to information using cookies and similar devices. While explicit consent might allow for regulatory certainty and might be the most appropriate way to comply in some circumstances this does not mean that implied consent cannot be compliant’.⁴⁸

However, for cookies that imply gathering of sensitive data, explicit consent could be required. According to the ICO guidelines, ‘website operators need to remember that where their activities result in the collection of sensitive personal data such as information about an identifiable individual’s health then data protection law might require them to obtain explicit consent’.⁴⁹

This presents an important similarity with the Dutch opt-in system. However, two differences produce important divergences in their application. First, the Dutch regulation requires explicit consent for all personal information, while the British would (potentially) require it for sensitive personal information only. Secondly, the Dutch and the British regulation have an opposite burden of proof. While the Netherlands requires that websites prove that the information carried is not personal information to avoid the requirement of explicit consent, the UK requires that the data subject (or a third party) proves that the information carried is personal and sensitive for explicit consent to be required. Despite having the same black letter law, the UK is much more lenient than the Netherlands in its regulatory application of the directive.

The differences mentioned add to the fact that, in practice, the UK has been even more lenient in the implementation of the e-Privacy Directive than what its regulation leads one to expect. An open letter issued by the Department of Culture, Media and Sport on 2011 has stated that focusing on providing data subjects with information and choices regarding tracking is reasonable and sufficient to comply with the regulation. Furthermore, the letter has stated that consent is not time-bound, and does not necessarily have to be given in a previous manner in cases in which it is impractical to do so.⁵⁰

In the UK the requirement of explicit and prior consent has been deemed too burdensome when applied to all cookies, since many websites install cookies at the moment that data subjects open them.⁵¹ The policy’s focus shifted with the open letter to ensuring best efforts in minimizing the time between the installation of the first cookies and the obtaining of consent.⁵² This is a very wide interpretation of the ICO’s guidelines—which, according to the letter, were consulted before its

48 *ibid.*

49 *ibid.* 6.

50 Department for Culture Media and Sport, ‘Open Letter on the UK Implementation of Art 5(3) of the e-Privacy Directive on Cookies’ (2011).

51 Information Commissioner’s Office (n 46).

52 Department for Culture Media and Sport (n 50).

writing—which request the installation of cookies to be delayed until consent is given every time this is possible.

The British regulation, in sum, also almost literally copies the wording of the Directive, but attenuates it strongly by allowing for implicit consent when no personal data is carried—with an opposite burden of proof than the Dutch regulation—and sometimes even for subsequent consent. It seems to stay, therefore, as close to an opt-out system as it is possible without breaching the Directive.

There is a possible criticism to the British regulation and all other Member States that have an opt-in system with implicit consent—which is standard in data protection law. If a data subject who visits a website without blocking cookies is considered to be manifesting implicit consent, and hence opting in, is it doubtful to what extent this is really an opt-in system. In practice, the data subject's behaviour needed to install cookies under an opt-in system with implicit consent and under an opt-out system with a duty of notification are the same: obtaining information and accessing the website nonetheless. This blurs the distinction between opt-in and opt-out.

REGULATORY DEFAULT RULES

Sticking to the default

Based on behavioural economics findings, many advocate for choice mechanisms that nudge people into making better choices without reducing their range of options or coercing them into choosing one in particular.⁵³

One way to nudge people is changing the default option.⁵⁴ Default-based policies often rely on the *status quo* bias, which indicates that, when offered a choice containing a default option, people tend to remain in that default.⁵⁵ This effect, which is relevant for nudging in choice design, is found even when the costs of switching away from the default choice are close to zero—such as ticking a box on a form.⁵⁶

53 Cass Sunstein and Richard Thaler, 'Libertarian Paternalism Is Not an Oxymoron' (2003) 70 U Chi L Rev 1159; Richard Thaler and Cass Sunstein, 'Libertarian Paternalism' (2003) 93 Am Econ Rev 175.

54 Moving from an opt-out system to an opt-in system, or vice versa, is a way of changing the default.

55 William Samuelson and Richard Zeckhauser, 'Status Quo Bias in Decision Making' (1988) 1 J Risk Uncertainty 7; Daniel Kahneman, Jack Knetsch and Richard Thaler, 'Anomalies: The Endowment Effect, Loss Aversion, and Status Quo Bias' (1991) 5 J Econ Perspect 193.

56 Cass Sunstein, 'Impersonal Default Rules vs. Active Choices vs. Personalized Default Rules: A Triptych' (2013) <<https://dash.harvard.edu/handle/1/9876090>>; Eric Johnson and Daniel Goldstein, 'Defaults and Donation Decisions' (2004) 78 Transplantation 1713. The tendency to stick to the default has been found in several domains. Adherence to savings plans increases up to 50% when employees are enrolled automatically. Number of organ donors increases up to 400% in countries where being a donor is the default choice. The effect is also present in insurance, food choices and marketing, where number of consumers who agree to receive marketing e-mails increases up to 50% depending on the default. See Brigitte Madrian and Dennis Shea, 'The Power of Suggestion: Inertia in 401(k) Participation and Savings Behavior' (2001) 116 Q J Econ 1149; Eric Johnson and Daniel Goldstein, 'Medicine: Do Defaults Save Lives?' (2003) 302 Science 1338; Johnson and Goldstein, 'Defaults and Donation Decisions'; David Cohen and Jack Knetsch, 'Judicial Choice and the Disparities Between Measures of Economic Values' (1992) 30 Osgoode Hall LJ 737; Colin Camerer, 'Prospect Theory in the Wild: Evidence from the Field' in Daniel Kahneman and Amos Tversky (eds), *Choices, Values and Frames* (CUP 2000); Eric Johnson, Steven Bellman and Gerald Lohse, 'Defaults, Framing and Privacy: Why Opting In-Opting Out' (2002) 13 Marketing Lett 5. JD Downs, Julie, George Loewenstein, and Jessica Wisdom, 'Strategies for Promoting Healthier Food Choices' (2009) 99(2) Am Econ Rev 159.

In contracts, most rules are defaults, ultimately leaving the decision to the parties,⁵⁷ but in regulation defaults are less orthodox. Rules designed to nudge may be either ‘policy defaults’ or ‘penalty defaults’. Policy defaults aim to increase the number of people choosing the default option, relying on inertia.⁵⁸ Penalty defaults aim to encourage a private party to provide information to other parties in order to reduce rent-seeking (obtaining gains by generating uncompensated losses to others) under information asymmetries.⁵⁹ Penalty defaults rely on the incentives of a more informed agent to initiate a negotiation that persuades the other agent to switch away from the default.

In most cases, the default option is the one that parties would have chosen if contracting was costless.⁶⁰ However, ‘nudging defaults’ (policy and penalty) stand in contrast to rules that the parties to the interaction would want. The appeal of policy defaults comes from a paternalistic aim to shape people’s preferences.⁶¹ The appeal of penalty defaults stems from that, under a veil of ignorance, potential parties would have wanted the default as well.⁶²

Penalty defaults are intended for those information asymmetry contexts in which the more informed party withholds information from her counterpart and engages in rent-seeking. Rent-seeking occurs when information withholding reduces the surplus to be divided between parties, but a party still withholds it to obtain a larger portion of the surplus. This is possible when the share-of-the-pie-effect is larger than the size-of-the-pie effect: when the amount of the surplus taken from others is larger than the proportion by which the total surplus is reduced.⁶³ In those cases, a rule that encourages the party to reveal the information is desirable—since it increases the size of the surplus to be divided. Penalty defaults can counteract incentives to strategically withhold information similarly to presumptions in procedural law, making the rule attractive under a veil of ignorance.⁶⁴

This said, default rules (both policy and penalty) have disadvantages. From an information perspective, precisely because of the *status quo* bias, they cannot reveal true preferences as well as make active choices, in which there is no default and people must choose between neutrally presented options.⁶⁵ When people stick to a default, it is difficult to know if they did so because they genuinely prefer that option or because of inertia.

From an incentives perspective, penalty defaults face the additional disadvantage that default rules can create an endowment effect.⁶⁶ A default rule necessarily establishes a *status quo* from which parties can negotiate away, but establishing it can

57 Ian Ayres and Robert Gertner, ‘Filling Gaps in Incomplete Contracts: An Economic Theory of Default Rules’ (1989) 99 *Yale LJ* 87.

58 Craig McKenzie, Michael Liersch and Stacey Finkelstein, ‘Recommendations Implicit in Policy Defaults’ (2006) 17 *Psychol Sci* 414.

59 Ayres and Gertner (n 57); Jason Johnston, ‘Strategic Bargaining and the Economic Theory of Contract Default Rules’ (1990) 100 *Yale LJ* 615; Ian Ayres and Robert Gertner, ‘Strategic Contractual Inefficiency and the Optimal Choice of Legal Rules’ (1992) 101 *Yale LJ* 729.

60 FH Frank Easterbrook and Daniel Fischel, ‘The Corporate Contract’ (1989) 89 *Colum L Rev* 1416.

61 Sunstein and Thaler (n 53).

62 Ayres and Gertner (n 57) 106.

63 *ibid.*

64 *ibid* 107.

65 John W. Payne, James R. Bettman and Eric J. Johnson, *The Adaptive Decision Maker* (CUP 1993).

66 Russell Korobkin, ‘The Status Quo Bias and Contract Default Rules’ (1998) 83 *Cornell L Rev* 608. These are intended for policy defaults, but not for penalty defaults.

make the person who benefited from it require a higher compensation to forfeit it than the one she would have offered to acquire it.⁶⁷ Independently of the default rule chosen, it will generate situations in which the default remains without it being the most beneficial outcome for the parties. This dilutes the difference between mandatory and default rules.⁶⁸ Hence, if one's objective is not to shape preferences, one should consider setting either a default that is preferred by the majority or an active choice system that requires people to select their preferred option.⁶⁹

Moreover, libertarian paternalism's policy design methods—including policy and penalty default rules—have been criticized on two fronts. Some have said that its practices lead to manipulation and are subject to slippery slopes that can lead to conclusions incompatible with liberal democracies.⁷⁰ Others criticized it for assuming a too comprehensive view of people's bounded rationality—it is often difficult to know people's best interest.⁷¹

One's judgment as to which type of default rule is established by the amended e-Privacy Directive depends on what one considers the aim of the Directive to be. If the Directive's aim is to reduce the overall amount of tracking devices being installed, then the default is a policy default. If it aims to ensure informed consent, as I consider here, then the default is a penalty default. The idea that a do-not-track (DNT) default in cookies works as a penalty default has been suggested before.⁷² Some consider that, by changing the default option into the most burdensome for websites, the choice mechanism forces them to educate data subjects to make them switch away from the default.⁷³ This leads one to expect that changing the default for cookies from an opt-out to an opt-in will leave data subjects better informed of the functions, advantages and disadvantages of cookies.

When default rules fail

In some cases, default rules do not give the expected outcome. One scenario in which default rules are likely to fail is when their application is given to an agent who (i) has an interest on whether the other agents make a choice switch and (ii) can shape the way the default rule is presented.⁷⁴ Choice architecture can be powerful when regulators design the choice mechanism but, when companies design it, they

67 Russell Korobkin, 'The Endowment Effect and Legal Analysis' (2003) 97 *NWU L Rev* 1227; Cass Sunstein, 'Switching the Default Rule' (2002) 77 *NYU L Rev* 106.

68 *ibid.*

69 Korobkin (n 67).

70 Martin Wilkinson, 'Nudging and Manipulation' (2013) 61 *Polit Stud* 341; Mario Rizzo and Douglas Glen Whitman, 'Little Brother Is Watching You: New Paternalism on the Slippery Slopes' (2009) 51 *Arizona L Rev* 685; Douglas Glen Whitman and Mario Rizzo, 'Paternalist Slopes' (2007) 2 *NYU J L & Liberty* 411.

71 Mario Rizzo and Douglas Glen Whitman, 'The Knowledge Problem of the New Paternalism' (2009) 4 *BYU L Rev* 905; Martin Lodge and Kai Wegrich, 'Rational Tools of Government in a World of Bounded Rationality' (2014) 75 *London School of Economics Centre for Analysis of Risk and Regulation Discussion Paper 1*. <<http://www.lse.ac.uk/accounting/CARR/pdf/DPs/DP75-Lodge-Wegrich.pdf>> accessed 1 October 2016

72 Jay Kesan and Rajiv Shah, 'Setting Software Defaults: Perspectives from Law, Computer Science and Behavioral Economics' (2006) 82 *Notre Dame L Rev* 583.

73 *ibid.*

74 Willis (n 7); Lauren Willis, 'When Nudges Fail: Slippery Defaults' (2013) 80 *U Chi L Rev* 1155.

can often circumvent regulatory intentions.⁷⁵ This is especially true for penalty defaults, which seek to reduce the profit of the party engaging in rent-seeking.

A penalty default that failed to meet its objective due to this mistake was the regulation for overdraft charges in the United States. A regulation required banks to obtain prior and explicit consent from their consumers (hence opting in) to provide them with overdraft coverage. The regulation's drafters stated explicitly that they intended it as a default rule to protect consumers. However, most consumers opted-in, and the policy was considered a failure.⁷⁶

Why was that so? When faced with the regulation, banks sent a letter to their consumers asking them if they wanted to keep their account unchanged and maintain the benefit of being able to withdraw money on overdraft, or to change the *status* of their account, by checking either yes or no in a form. The forms gave the options 'yes: keep my account working the same with *shareplus* ATM and debit card overdraft coverage/no: change my account to remove *shareplus* ATM and debit card overdraft coverage'.⁷⁷ Advertising, additionally, said: 'Don't lose your ATM and debit card overdraft protection'.⁷⁸

Without violating the regulation, banks could manipulate the opt-in system into an active choice. An active choice or forced choice system is one without a clear default, in which agents (in this case bank clients) must choose one alternative.⁷⁹ Moreover, the choice was not neutral. Banks were able to change the perception of the *status quo* and prime consumers into opting into the system by favouring one alternative in the active choice and highlighting the losses in the other.⁸⁰ The regulation failed because it did not take into account that it targeted agents (banks) who were behaviourally informed (they were aware of the effects of default rules and active choices) and had interests against it.⁸¹

For a change in the default choice to yield its expected result, people must be treated similarly regardless of their choice.⁸² When companies introduce additional incentives to switch, most of the benefits of the default system are lost. Regulation can limit differential treatments, but those limits are difficult to establish and even more difficult to police.⁸³ The bank overdraft regulation should have been more specific in the choice mechanism design. Design techniques are never neutral and they can easily frame consumers.⁸⁴ This makes the choice design as important as the choice itself.⁸⁵ Still, it is possible that banks would have found another way to reframe the choice.⁸⁶

75 *ibid.*

76 Willis (n 7).

77 Willis (n 74).

78 Willis (n 7).

79 Gabriel Carroll and others, 'Optimal Defaults and Active Decisions' (2009) 124 QJ Econ 1639.

80 Punam Keller and others, 'Enhanced Active Choice: A New Method to Motivate Behavior Change' (2011) 21 J Consum Psychol 376.

81 Cass Sunstein, 'Acceptance Speech for the Title of Honorary Doctor at Erasmus University Rotterdam' (Rotterdam, 8 November 2013).

82 Willis (n 7).

83 *ibid.*

84 Ari Waldman, 'Designing Privacy Policies' (2016) Working Paper, on file with author.

85 *ibid.*

86 In that case, the more specific choice design would have carried high-monitoring costs.

Finally, one could ask how would have the overdraft regulation worked if implicit consent had been allowed to opt-in the system,⁸⁷ and whether this would have avoided its problems. It then becomes noticeable that it is difficult to imagine a choice design in which banks could have implemented this format in a way that it is not substantially the same for their clients as the previous opt-out regime.

Similarities with online tracking regulations

A central problem of the interaction at hand is asymmetric information. Websites know more than data subjects about the cookies installed in their devices and data subjects do not know enough about them to provide informed consent, which was identified as the regulation's aim.

This, however, is not the sole problem. If it were, data subjects could educate themselves in a less costly way than regulation and websites could have some incentives to care about their users' privacy since that would bring them revenue from privacy-informed data subjects. More importantly, a change from an opt-out to an opt-in default system should not matter for well-informed and rational data subjects in a scenario where the cost of switching is low.⁸⁸

This indicates that the informational asymmetry is part of a multifaceted problem. Data subjects not only are uninformed about the specifics of cookies, but they also do not inform themselves.⁸⁹ Additionally, as argued above, changing the choice system is relevant because data subjects tend to stick to the default rule. This leads to an approach in which regulation aims to protect data subjects that do not engage in the necessary actions to protect themselves.

A possible reason why the Dutch regulation did not meet its aim is that, despite stating so, it did not effectively force websites to implement an opt-in system.

Similarly to American bank customers deciding on overdraft coverage, data subjects were asked a polar question: whether they agreed with the website's use of cookies or not. This is different than facing an opt-in system; both bank customers and data subjects had to make a conscious choice.

In both cases, the most effective way to get customers to switch away from the default was not to inform them about the costs and benefits of each option. As a consequence, after websites incorporated the regulation what data subjects faced was not a DNT default but an active choice. This similarity illustrates what can happen when the choice architect has is interested in subverting the regulation.

Furthermore, data subjects under the cookie regulation were more pressured than bank customers while choosing. While the latter could still use other bank services normally after choosing 'no', data subjects were often either unable to access the website due to the 'cookie wall', or able to access it but subject to several

87 This would have been an opt-in policy more favourable to banks.

88 Since costs for opting in or out of the default are low, the number of informed and rational people opting into a tracking system under a DNT default should be the same as those not opting out under a track-me default. In such a case, adopting an opt-in system with explicit consent, an opt-in system with implicit consent, or an opt-out system, would be indifferent. What is more, since explicit consent implies higher transaction costs, it would be the worst alternative.

89 This could be due to a *status quo* bias caused by reference dependence or implied endorsement. McKenzie, Liersch and Finkelstein (n 58).

malfunctions because the negative choice also meant that session cookies, which are necessary for some features, were not installed.

The ‘cookie wall’ and the statement presenting cookies as necessary for the website’s functioning (which they sometimes are) framed data subjects’ choice. Data subjects’ choice was whether they desired to be tracked, but whether they still wanted to visit a website seconds after typing its URL. This effect was even stronger in websites that, together with the ‘cookie wall’, placed a banner that allowed only for the ‘yes’ option—data subjects who wanted to choose no had to leave the website since they had nowhere to manifest their choice.

As with other default choice systems, a DNT default works only if people under the DNT regime are treated the same as those in the track-me regime.⁹⁰ If websites are able to present data subjects with incentives to switch, most of the policy’s benefits are lost.⁹¹ It has been argued that the cookie wall was problematic because it puts pressure on choice.⁹² This can hamper the validity of consent by violating the free consent requirement established by the Article 29 Working Party—even without amounting to coercion.⁹³

Like the bank overdraft regulation, the Dutch and other European regulations asked agents who are behaviourally informed and have counteracting interests to them to be the choice architects of an opt-in default system. Are there regulatory alternatives?

POLICY SUGGESTIONS

Reconsidering the penalty default

Having evaluated the different ways Member States implemented the amended e-Privacy Directive’s previous consent requirement for tracking (opt-in system), the question arises as to whether making the choice an opt-in is conducive to the aim of the regulation and desirable in the context of the multifaceted information problem. It may be better to present it as an active choice with two options presented equally—as did the Dutch regulation, albeit unintentionally.

As mentioned above, default rules can be set as policy defaults or as penalty defaults, depending on the aim with which the default rule is set. In policy defaults, opt-in systems are preferable when one choice is in itself more valuable than the others, either by most of those facing the choice, or for society as a whole.⁹⁴ This is the case, for example, of organ donation: some jurisdictions change the default to increase the number of donors because donation is valuable in itself.

However, for tracking devices such as cookies it is arguable that it is desirable to reduce their use only inasmuch as they cost consumers more than they benefit them, and not to absolutely eliminate them from the Internet—even when ignoring companies’ benefits that should also be present in a social welfare function. Cookies are not inherently harmful, as they present both costs and benefits for the industry and

90 *ibid.*

91 Willis (n 7).

92 Luzak (n 6); Helberger (n 36).

93 ‘Opinion 15/2011 on the Definition of Consent’ (n 16).

94 McKenzie, Liersch and Finkelstein (n 58).

for data subjects. The ‘stickiness’ of an effective opt-in default policy, then, could actually leave us with fewer cookies than what is socially desirable. This can have harmful dynamic effects. If the entry in the website market (which is financed by advertising) is diminished by an opt-in system, this policy would lead to fewer websites in the future and a less interesting Internet for data subjects. This idea is in line with the classification of this policy under penalty defaults.

Penalty defaults can make a stronger case in favour of an opt-in system for cookies than policy defaults, as companies are clearly more informed than data subjects about the functioning of the cookies they install. As discussed above, penalty defaults are useful when (i) one party is more informed than the other, (ii) she engages in rent-seeking by withholding information and reducing total welfare, and (iii) contracting around the default rule can release the information. So the question to ask to determine whether a penalty default is useful is: does this rule increase the amount of available information by reducing what was previously withheld?

This question involves two facts. The first is whether there is rent-seeking behaviour exploiting the information asymmetry.⁹⁵ The second is whether the penalty default imposes a cost on the informed party sufficient to induce a negotiation and a disclosure that reduces the information asymmetry.⁹⁶

While there is asymmetric information between websites and data subjects regarding cookies’ functions, it is unclear whether it produces rent-seeking. Moreover, the default did not induce a negotiation between them. The information release produced by the regulation is that a website utilizes cookies. Data subjects from countries that applied the Directive most strictly were not more informed about cookies’ functions after clicking away banners. Individual negotiations to induce data subjects to opt into tracking would have been difficult due to the large number of data subjects involved, and it is difficult to anticipate whether information about the characteristics of cookies would induce them to opt in.

Given the difficulties in assessing the costs and benefits of cookies for each case, applying the principle of informed consent to an active choice system presents benefits over an opt-in policy—which regulates the way to present the choice. If a data subject knowingly agrees to cookies, there are good reasons to believe the exchange is valuable.

The presence of heterogeneous preferences is a substantial argument in favour of active choice designs instead of default rules.⁹⁷ And data subjects have heterogeneous preferences regarding tracking. People have different levels of disutility from tracking and each person has different levels of disutility depending on the information concerned. A neutral presentation of the choice might be more appropriate for the aim of informed consent.

Finally, this would cope with the criticisms of libertarian paternalism noted above, since an active choice system would be a non-paternalistic alternative to the default-based regulation.

95 Ayres and Gertner (n 57) 127.

96 *ibid* 128.

97 Sunstein (n 56).

Differentiating cookies

Cookies present different levels of privacy reduction. As a first distinction, session cookies and permanent cookies do not present the same risks for privacy breach. As mentioned above, session cookies disappear after the browser is closed, whereas permanent cookies remain in storage for a longer period of time, usually until deleted. If one assumes an equal risk of privacy breach per period of time, permanent cookies—which can last for years—present a much higher privacy risk than session cookies—which tend to last for a few hours. In addition, user profiles are normally constructed with permanent cookies, while most cookies that allow functions in websites (such as a shopping cart) are session cookies. Permanent cookies, hence, present a higher (expected) privacy reduction than session cookies. And session cookies are more useful for users.

Due to the incentive structure of website providers, regulations should treat permanent cookies and session cookies differently. In the same way as permanent cookies involve a higher privacy cost for data subjects than session cookies, they involve a larger payoff for websites and advertisers since, by lasting for a longer time, they make collecting information easier.

Establishing a DNT default for all cookies reduces the amount that websites are able to install in data subjects' devices (contingent on consent) by making every cookie marginally less likely to be installed. This reduces websites' ability to make user profiles and tailor advertisements based on those profiles. This, in turn, reduces the total payoff of cookie use for websites. If websites can install fewer cookies, and they can choose which cookies to install because all of them are treated equal, they will install those that are most profitable. This means that a regulation that treats all cookies equally reduces the payoff of cookie diversification. By setting incentives for websites to install only the most invasive cookies, it shifts the relative prices towards cookies that are more costly from a privacy perspective.

Even if one assumes websites care about their users' privacy and would thus install the least invasive cookie under a regulation that treats them all equally, in a context where the cost per installation of cookie (obtainment of consent) is fixed, websites must pay this cost only once for a permanent cookie, but several times if the same function is performed by several session cookies. Assuming that firms try to reduce costs, this will lead them to shift to permanent cookies whenever possible.⁹⁸ This increases the total privacy cost of cookies.

If less privacy-invasive cookies (such as analytics, or session cookies in general) can be more easily installed, while more invasive cookies require previous consent, websites will have incentives to diversify cookies. They will request consent for permanent cookies only when they are necessary for their goal. This leads to enhanced privacy for data subjects without harming websites.

The same effect is caused from data subject's side. Under a regulation that does not differentiate cookies, data subjects entering a website are notified that it uses

98 This argument applies both to websites under perfect competition and those with monopoly power, as cost minimization is independent of market power.

cookies or asked to agree to its use of cookies. It is costly for that data subject to know, however, if those cookies are session cookies or permanent cookies, categories to which she could react differently. Her perceived privacy risk, as well as her annoyance during browsing, will be determined solely by that notification or banner. In this situation, a website maximizing the number of visitors will ask the question as few times as possible, hence recurring to fewer and more invasive permanent cookies.

Under a regulation that requires authorization for permanent cookies but not for session cookies, websites would have incentives to use session cookies as much as possible and reduce the number of times data subjects receive the notice or banner for permanent cookies. This also makes the notice or banner more informative, since data subjects would know that it corresponds to permanent cookies. Additionally, this would make data subjects less prone to accept banners requesting consent for tracking (each acceptance is more costly on average than one to current banners that do not differentiate cookies) thus enhancing privacy.

The following subsection suggests a more effective mechanism to implement DNT. From this point of view, it has the additional benefit of allowing for session cookies while preventing permanent cookies from being installed.

Targeting web browsers

A way to address the problems faced by the Dutch regulation is a regulation that targets web browsers and not websites.⁹⁹ While this is technically possible, the legal change would face conceptual and political feasibility obstacles.

The conceptual obstacle is that EU data protection law has traditionally targeted data controllers and not technology creators. Browsers rarely fit under the first category since they seldom define the purpose of the processing.¹⁰⁰ This makes it difficult for individual EU Member States to place requirements on them. The political obstacle would be jurisdictional limits and a consequent lack of enforcement, which would depend on the ability to coordinate regulatory efforts. It was unfeasible for Dutch regulators to make demands to browsers, most of which are based in the USA. This is less so for the EU in general—it has held transnational entities accountable under data protection law before. But the jurisdictional limits are still present for EU law. And the USA, which is the jurisdiction that could implement this more easily, would probably be resistant to it given its sectorial approach to data protection. Still, it is possible that, if enacted by the right jurisdictions, browsers would respond to a regulation of this kind. After all, the current regulation must be also implemented with US websites to be effective. And browsers have responded well to DNT headers when asked to implement them—better than websites did.

Targeting browsers would present significant benefits. First, a browser's business model is harmed by a policy that reduces the use of cookies only inasmuch as the company who owns the browser also owns websites or other applications that profit from targeted advertising—which are now targeted. Unlike websites, browsers' lack

99 Ian Brown and Christopher Marsden, *Regulating Code* (CUP 2013).

100 A29WP, 'Opinion 1/2010 on the Concepts of "Controller" and "Processor"' (2010) 7.

direct incentives to twist the default policy, while they have the technical capability of blocking them.

In a similar way as a regulation can call websites to apply a DNT preference and avoid sending cookies as was successfully done with DNT headers, it can call browsers to apply it by blocking cookies sent by websites. Websites' intentions notwithstanding, browsers could operate as gatekeepers and choose whether to let cookies through. Websites would be unable to easily set up a cookie wall as they did in the Netherlands and the UK.

Secondly, browsers are easier to police than websites, so regulatory costs would be reduced. The internet has millions of websites but five browsers through which most traffic passes. Requesting them to block cookies can establish a DNT default at lower enforcement costs. Moreover, the measure would reduce compliance costs due to the reduced number of agents directing efforts to apply the regulation. Under the current Dutch regulation, all websites that operate in the Netherlands must design a banner for the opt-in mechanism—or active choice. This duplication of efforts consumes resources that could be better used elsewhere.

Browsers can also implement the policy in more convenient way for data subjects. They can ask whether to navigate with cookies in a more relevant context than that of websites—even when well intentioned. When websites ask whether a data subject agrees with cookies being installed, the data subject is asked every time she changes website, which was found by most to be bothersome and not user-friendly.¹⁰¹ This not only interrupts navigation and annoys data subjects but also makes it difficult for them to allow tracking in some occasions and not in others. If browsers posed this question, data subjects could be asked every time they open the browser. This would avoid interrupting navigation and would allow them to switch system by opening a new window. Requesting browsers to block cookies, thus, allows for a more user-friendly way of knowing whether a data subject wants to browse with or without them. This fits better with the Cookies Directive's aim of requesting consent as user-friendlily as possible within technical limitations.¹⁰²

All major browsers already contain a function under which data subjects can navigate the internet without permanent cookies being installed. This function prevents (with exceptions) cookies, local storage, history and caches to remain in the device after browsing. One can use them to navigate without leaving permanent traces in one's device, which facilitates tracking, while receiving the less inconvenient session cookies that allow for the use of many features—such as streaming or shopping carts.

This function currently offers an opt-out for permanent cookies that requires few clicks and avoids the need for privacy enhancing technologies. Article 29 Working Party stated that browser settings do not represent an opt-in because they accept cookies by default and data subjects often ignore how to change them.¹⁰³ This opt-out can easily be turned into an opt-in by requiring browsers to open in this mode

101 Helberger (n 36).

102 Directive 2009/136/EC, recital 66.

103 'Opinion 2/2010 on Online Behavioral Advertising' (n 16) 14.

by default. Or it can be turned to an active choice system by requiring them to neutrally present the choice when the browser is opened.

Most privacy-enhancing technologies—especially those that are more sophisticated—have usability problems,¹⁰⁴ and so did the cookie wall applied by websites. This function embedded in browsers is simpler to use. Establishing this function as a default would make it even simpler.¹⁰⁵ This would provide a simpler regulation with fewer incentives to undermine the policy.

CONCLUSION

This paper argues that the behavioural economics literature on default rules helps identify why online tracking regulations in Europe faced implementation difficulties. These regulations either arguably stayed in practice within an opt-out default system by allowing for implicit consent, or their policy was neutralized by websites, having an active choice system as a result. The one member state that adopted a DNT default requiring previous and explicit consent decided to attenuate it moving to implicit consent thereafter.

Both the Netherlands and the UK implemented the wording of the amended e-Privacy Directive in their regulations but gave it in practice very different meanings. While the Dutch regulation follows what seems like the intention of the e-Privacy Directive's amendment and becomes what could be the strictest legal system in the world regarding cookies, the British regulation approaches the issue more conservatively and regulates it as close to an opt-out system as the wording of the amendment allows. Noting the implementation problems that the Dutch regulation faced, it is easier to understand the British government's reluctance to move to an opt-in system and the Dutch decision to moderate its own regulation.

As argued here, this took place because penalty default rules were applied outside of their scope and their design was trusted to agents with incentives to undermine them. Reconsidering the opt-in system, relying on web browsers instead of websites for the choice design, and taking into consideration the differences in privacy costs between permanent and session cookies, would improve consumer choice.

The explanation and policy suggestions offered can be useful not only for the Netherlands and the UK but for any country considering incorporating a DNT default. This suggestion presents a further step towards moving away from a post-breach regime based on policing data controllers and to building privacy by design, where privacy is embedded as functionally as possible within the technologies that we use.¹⁰⁶ Within Europe, it can help design an implementation that ensures informed consent and achieves the Directive's aims in line with the goal of 'smart

104 Pedro Giovanni Leon and others, 'Why Johnny Can't Opt out: A Usability Evaluation of Tools to Limit Online Behavioral Advertising', *Proceedings of the Association for Computing Machinery Special Interest Group on Computer-Human Interaction Conference* (Association for Computing Machinery Press 2012).

105 If this were not a problem, regulators could design forms for data subjects to complete when they enter into a website, specifying the types of cookies they prefer to allow, for how long they prefer to allow them, for the use of whom, etc. But this would be of little use.

106 This has been defined as 'the philosophy and approach of embedding privacy into the design specifications of various technologies'. Ann Cavoukian, 'Privacy by Design' (2009) 1 <<https://www.ipc.on.ca/wp-content/uploads/Resources/pbd-primer.pdf>> accessed 1 October 2016. See also Peter Hustinx, 'Privacy by Design: Delivering the Promises' (2010) 3 IDIS 253.

regulations'.¹⁰⁷ The technology and the behavioural insights to implement effective limits on online tracking are already available; it is the law that needs to catch up.

APPENDIX I

To evaluate how EU Member States incorporated the directive, data was gathered from their legislations and regulations (when available) to determine whether they modified their regulatory framework after the directive changed. The applicable norms were searched for, together with their dates of modification, and countries were classified either under an opt-in or an opt-out system for online tracking. The countries falling under the first category were further classified either as opt-in with implicit consent allowed or opt-in with a requirement of explicit consent.¹⁰⁸

Table A1 schematizes how the directive was implemented across Member States.

107 Commission Decision establishing the REFIT Platform (19 May 2015) <http://ec.europa.eu/smart-regulation/better_regulation/documents/c_2015_3261_en.pdf>; Interinstitutional Agreement of Better Law-Making (13 April 2016) <http://ec.europa.eu/smart-regulation/better_regulation/documents/ia_blm_final_en.pdf>

108 Implicit consent is the consideration that a person has agreed on an action without explicitly manifesting such agreement; she has implicitly manifested it with her actions or her inaction upon particular circumstances. Elizabeth Fuller, 'Implied Consent Statutes: What Is Refusal?' (1986) 9 *Am J Trial Advoc* 423. Although there are parallels between opt-in versus opt-out and implicit versus explicit consent, they are not equivalent. While the first classification refers to the timing of consent, the second refers to the form in which consent must be given.

Table A1: Summary of incorporation of the directive by EU country and their classification by system

Country	Norm	Date of amendment	System	Consent	Authority	Regulation
Austria	Telecommunications Act (section 96.3)	22 November 2011	Opt-in	Implicit	Österreichische Datenschutzbehörde	No
Belgium	Electronic Communications Act	28 June 2012	Opt-in	Implicit	Commission de la protection de la vie privée/Belgian Telecom Regulator (IBPT)	Yes
Bulgaria	Electronic Messages Act	29 December 2011	Opt-out	-	Commission for Personal Data Protection	No
Croatia	Electronic Communications Act (Zakon o elektoničkim komunikacijama)	15 July 2011	Opt-in	Implicit	Croatian Personal Data Protection Agency	No
Cyprus	Regulation of Electronic Communication and Postal Services Law	18 May 2012	Opt-in	Implicit	Commissioner for Personal Data Protection	No
Czech Republic	Act No. 101/2000 Coll.	1 January 2012	Opt-out	-	Office for Personal Data Protection	No
Denmark	Act on Electronic Communications Networks and Services (Act No. 169)	14 December 2011	Opt-in	Implicit	Datatilsynet	Yes

(Continued)

Table A1: (continued)

Country	Norm	Date of amendment	System	Consent	Authority	Regulation
Estonia	Electronic Communications Act	Not amended	Opt-out	-	Estonian Data Protection Inspectorate	N/A
Finland	Personal Data Act (Henkilötietolaki 1999/523)	25 May 2011	Opt-in	Implicit	Office of the Data Protection (Data Protection Board)	No
France	Article 32 II of the Act of 6 January 1978	27 August 2011	Opt-in	Implicit	Commission Nationale de l'Informatique et des Libertés	Yes
Germany	Telecommunications Act	Not amended	Opt-in	Implicit	Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit	N/A
Greece	Law 3471/2006 amended by Law 4070/2012	10 April 2012	Opt-in	Implicit	Hellenic Data Protection Authority	
Hungary	Act CVII of 2011 on Communications	3 August 2011	Opt-out	-	Data Protection Commissioner of Hungary	No
Ireland	Electronic Communications Networks and Services	1 July 2011	Opt-out	-	Data Protection Commissioner	No
Italy	Article 122 of the Data Protection Code	28 May 2012	Opt-in	Implicit	Garante per la protezione dei dati personali	Yes
Latvia	Law on Information Society Services	8 June 2011	Opt-in	Implicit	Data State Inspectorate	No

(Continued)

Table A1: (continued)

Country	Norm	Date of amendment	System	Consent	Authority	Regulation
Lithuania	Law on Electronic Communications	1 August 2011	Opt-in	Implicit	State Data Protection Inspectorate	Yes
Luxembourg	2005 Act on the specific provisions for the protection of individuals in relation to the processing of personal data in the electronic communications sector	1 September 2011	Opt-in	Implicit	<i>Commission Nationale pour la Protection des Données (CNPDP)</i>	No
Malta	Legal Notice 239 of 2011	1 January 2013	Opt-in	Implicit	Office of the Data Protection Commissioner	No
The Netherlands	Telecommunications Act article 11.7a	5 June 2012	Opt-in	Explicit	College bescherming persoonsgegevens	Yes
Poland	Telecommunications Law	22 March 2013	Opt-in	Implicit	Bureau of the Inspector General for the Protection of Personal Data	No
Portugal	Law 46/2012 amending Law 41/2004	29 August 2012	Opt-in	Implicit	Comissão Nacional de Protecção de Dados	No
Romania	Ordinance 13/2012 amending Law 506/2004	26 April 2012	Opt-out	-	National Supervisory Authority for Personal Data Processing	No

(Continued)

Table A1: (continued)

Country	Norm	Date of amendment	System	Consent	Authority	Regulation
Slovakia	Act on Electronic Communications	1 October 2011	Opt-in	Implicit	Office for Personal Data Protection of the Slovak Republic	No
Slovenia	Electronic Communications Act (ZEKom-1)	15 January 2013	Opt-in	Implicit	Information Commissioner	Yes
Spain	Information Society and Electronic Commerce law (34/2002) amended by Royal Decree 13/2012	2 April 2012	Opt-in	Implicit	Agencia de Protección de Datos	Yes
Sweden	Electronic Communications Act (Sw. lagen om elektronisk kommunikation, 2003:389)	1 July 2011	Opt-in	Implicit	Datainspektionen	Yes
UK	Regulation 6 PECR	26 May 2011	Opt-in	Implicit	Office of the Information Commissioner Executive Department	Yes

The Cookies Directive's implementation in the EU has been the following: six member states stayed in an opt-out system (Bulgaria, Czech Republic, Estonia, Hungary, Ireland and Romania), twenty one incorporated an opt-in system but allow for implicit consent (Austria, Belgium, Croatia, Cyprus, Denmark, Finland, France, Germany, Greece, Italy, Latvia, Lithuania, Luxembourg, Malta, Poland, Portugal, Slovakia, Spain, Sweden, Slovenia and UK), and one incorporated an opt-in system requiring explicit consent (the Netherlands). Countries were considered to have an opt-in system if previous consent was required for tracking, and an opt-out system otherwise. Countries were classified under opt-in with explicit consent if they additionally required that such previous consent be explicit, and under opt-in with implicit consent if the requirement was absent or if they specified that consent could be manifested implicitly.