The Cookiewars

Leenes, Ronald

Published in:
The Privacy & Identity Lab

Publication date:
2015

3 The cookiewars

From regulatory failure to user empowerment?

Ronald Leenes

3.1 Introduction

The European regulator has relatively early on seen the potential privacy harms of cookies as means to facilitate the marking and tracking of individuals as they browse the internet. Article 5(3) of the ePrivacy Directive 2002/58/EC[1] regulates the use of cookies (and other mechanisms). The Directive (or rather its implementation in national law the member states) has, so far, not been very successful in limiting the amount of tracking of individuals for, amongst others, the purposes of personalised, or behavioural advertising. It has been strongly opposed by the relevant industries, has seen a very low level of compliance, and where compliance exists this has been very slow in the making. Furthermore, ironically, the regulatory benefactors, individuals, have also opposed the regulation [14].

The battle to stop the unconsented tracking of individuals by ad-networks and others seems particularly lost now that the regulatees have successfully changed the meaning of the Directive[2]. What was intended to be an inform and consent requirement for the placement and use of cookies (thus providing the individual with a choice not to be tracked), has been turned into to an inform mechanism that cookies will be used (and hence individuals will be traced, no matter what they want). Individuals in many cases have no other choice but to accept the cookies (and hence acknowledge their use rather than consent with their use). The industry has thus succeeded in completely subverting and undermining the regulation's aim. The 'cookie law' can thus be seen as an example of regulatory failure in the domain of privacy and data protection.

[1] 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) L 201/37

[2] At least they seem to get away with their interpretation

However, the cavalry might be around the corner. Ad blockers, which not only block advertisements but also the mechanisms that deliver tracking-cookies from being installed on the user's equipment, are gaining rapid traction. Although they have been around for some years, their use until recently was confined to techies and nerds. This is rapidly changing. On PC's the ad-blocker barge is led, ironically, by Google Chrome [18]. Not only is Chrome increasingly the browser of choice of netizens, its users also install ad blockers. Until recently, ad blockers did not exist on one of the most important mobile platforms, iOS. Although Android has many more users, iOS users spend more time browsing the internet (and spend more money online) than Android users [6][8], making iOS an important platform for advertisers and advertisment funded content. iOS lacked ad blocking support in its native browser, Safari and web-kit. This has changed with the launch of iOS 9 in mid September 2015. Suddenly ad blockers are clearly on everyones agenda, either as a threat or a blessing. The adoption rate of both iOS 9 and Safari ad blockers is stunning and might represent a significant factor to change the ad and tracing game altogether.

This contribution explores the ongoing cookie-wars by discussing the apparent failure in regulating behaviour of entities in the advertising and adtech industries: from law to the market and code. The contribution proceeds as follows. Section 2 will briefly discuss the regulation at stake, art 5(3) ePrivacy Directive and its implementation in Dutch law. Dutch law is exemplary because it provided the most strict interpretation of the requirements for using cookies and hence, arguably, has spurred most opposition from those addressed by the law. Sections three and four will describe the first stages of the war against curbing the unlimited tracking and tracing of individuals, which can be characterized as a move from ignoring the regulation to actively undermining it and trying to change the law, to a clear separation of minds amongst the regulatees: the willing versus the unwilling. In section five I will discuss the latest phase in the battle, the one where users try to take control, and provides some concluding remarks.

3.2 The cookie regulation

Cookies are necessary devices to make the internet work. They provide for local storage of website preferences, allow maintaining the state of a connection (for instance for shopping carts) and they allow servers to recognize returning visitors. The latter characteristic makes them ideally suited for the marking and tracking of individuals across websites. Third parties (ad-brokers, social media, etc) typically embed small content (as small as a single transparent pixel) on

first party websites (the one visited by the user), which allows them to also place and read back cookies in the user's browser [21] [4]. Because these third parties do this on hundreds of thousands of websites, they can obtain detailed insight in the sites visited by individuals. The profiles based on this behavioural data can be used for providing targeted ads [2], but also for making decisions about individuals with respect to pricing of goods and services, eligibility of services, etc. Given that anonymity is very hard to achieve [17][10], and the efforts taken by the industry to combine data sources (which may contain identifying data), this not only affects the individual while browsing the net, but potentially also offline.

The European Commission has acknowledged the potential harm of cookies in the 2002 e-Privacy Directive[3]. Recital 24 of the ePrivacy Directive makes the blessings and potential threats of cookies and friends clear:

> "(24) Terminal equipment of users of electronic communications networks and any information stored on such equipment are part of the private sphere of the users requiring protection under the European Convention for the Protection of Human Rights and Fundamental Freedoms. So-called spyware, web bugs, hidden identifiers and other similar devices can enter the user's terminal without their knowledge in order to gain access to information, to store hidden information or to trace the activities of the user and may seriously intrude upon the privacy of these users. The use of such devices should be allowed only for legitimate purposes, with the knowledge of the users concerned."

Recital 25 specifies in more detail how cookies and similar mechanisms should be treated to limit their threat to the privacy of users.

> "(25) However, such devices, for instance so-called 'cookies', can be a legitimate and useful tool, for example, in analysing the effectiveness of website design and advertising, and in verifying the identity of users engaged in on-line transactions. Where such devices, for instance cookies, are intended for a legitimate purpose, [...], their use should be allowed on condition that users are provided with clear and precise information in accordance with Directive 95/46/EC about the purposes of cookies or similar devices so as to ensure that users are made aware of information being placed on

[3] See [11] for a detailed analysis of the cookie regulation, see [14] for a detailed analysis of why the regulation fails.

> the terminal equipment they are using. Users should have the opportunity to refuse to have a cookie or similar device stored on their terminal equipment. [...] The methods for giving information, offering a right to refuse or requesting consent should be made as user-friendly as possible. Access to specific website content may still be made conditional on the well-informed acceptance of a cookie or similar device, if it is used for a legitimate purpose."

The actual regulation of cookies et al. takes place in article 5(3) of the ePrivacy Directive. While the article was amended in 2009 by the Citizens' Rights Directive[4] the recitals cited above are still valid.

One of the prominent changes in article 5(3) ePrivacy Directive is that the right to refuse cookies as mentioned in recital 25, has been replaced by a stronger consent requirement:

> '3. Member States shall ensure that the *storing of information*, or the *gaining of access to information* already stored, in the terminal equipment of a subscriber or user is allowed on condition that the subscriber or user concerned *has given his or her consent, having been provided with clear and comprehensive information* in accordance with Directive 95/46/EC, inter alia about the purposes of the processing. [...]' (emphasis added)

The use of cookies thus has to comply with two cumulative conditions. On the one hand, the user[5] has to be provided with clear and comprehensive information in accordance with the Data Protection Directive, in particular with art. 10. The user should be informed about the identity of the entity that wishes to use cookies in their terminal equipment, the purposes of the processing and any information relating to the recipients or categories of recipients of the data, whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply, and the existence of their right of access, the right to rectify the data concerning him and the right to refuse the storing of or the access to their information. The second condition for using cookies is that the user give their consent to the use of cookies by the service provider.

[4] European Parliament and the Council of the European Union, Directive 2009/136/EC 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 (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws ("Citizens' Rights Directive") [2009] OJ L337/11 (18.12.2009).

[5] The Directive talks about subscriber or user, but for the purposes of this paper, I will simplify matters a bit and only talk about (website) users.

This consent has to be a freely given, specific and informed indication of the wishes of the user or the subscriber. Freely given consent means that the user should have a real choice whether to accept the cookies.

In theory here lies an opportunity for users to determine whether or not they want to be marked and tracked by first and third parties. This may be theory though, because recital 25 of the 2002 ePrivacy Directive specified that the access to specific website content may be made conditional on the acceptance of a cookie after the user is provided with clear and comprehensive information, if the cookie is used for a legitimate purpose[6]. This, as the Art. 29 Working Party rightly remarks [1], contradicts the notion of choice, meaning that users have a right to refuse the use of cookies by a provider on their equipment. Making access to a website (or parts thereof) conditional on the acceptance of cookies in many cases does not constitute free choice. Unsurprisingly the scope of consent is one of the topics of debate surrounding the cookie regulation. Can users refuse service providers to use cookies and still have access to the entire site? We will return to this question in the next section.

Another controversy regards the way in which consent should be obtained. Thirteen member states have claimed that the 2009 amendment to the ePrivacy Directive should be interpreted in light of the 2002 recitals: "As indicated in recital 66[7], amended article 5(3) is not intended to alter the existing requirements that such consent be exercised as a right to refuse the use of cookies or similar technologies for legitimate purposes."[8] A consequence of this disagreement about the meaning of consent is that there are national differences in the consent requirements. The Netherlands does not belong to 'the thirteen' and has opted for a strict interpretation of the consent requirement. In line with this interpretation, cookie preferences set in the browser preferences are not

[6]It is not too difficult to define legitimate uses of cookies, serving advertisements would be one.

[7]of Directive 2009/136/EC amending Directive 2002/22/EC

[8]Council of the European Union, 'Addendum to "I/A" note: Adoption of the proposal for a Directive of the European Parliament and of the Council amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of electronic communications networks and services, and 2002/20/EC on the authorisation of electronic communications networks and services (LA + S) (third reading) – Statements, 15864/09 ADD 1 REV 1', Brussels, 18.11.2009, as corrected by Council of the European Union, 'Corrigendum to the Addendum to "I/A" note: Adoption of the proposal for a Directive of the European Parliament and of the Council amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of electronic communications networks and services, and 2002/20/EC on the authorisation of electronic communications networks and services (LA + S) (third reading) – Statements, 15864/09 ADD 1 REV 1 COR 1', Brussels, 19.11.2009.

adequate to signal consent (or refusal); users have to give explicit consent[9] and must be given the opportunity to retract their consent.

The art. 29 WP has inventoried the various mechanisms that industry had developed since the 2009 amendment of the ePrivacy Directive to comply with the regulation in 2013 and has provided guidance on the way consent for cookies can be obtained properly [3]. The four elements that jointly need to fulfilled are:

1. The user's decision must be based on appropriate information about the types of purposes of cookies that are used by the website, as well as indication about the installation of third party cookies or about third party access to data that are collected via cookies on the specific website. Information about the expiration of the cookies, typical values and any other technical information should also be offered to the users.

2. The consent has to be obtained before any cookies are set or read.

3. The consent should be expressed as an active indication of the user's wishes and there should be no doubt with regard to the intention of the user. A broad range of tools is proposed as adequate for this, such as splash screens, banners, modal dialog boxes or the active configuration of browser settings.

4. The user should be able to exercise a real choice, on the entry page of the website, between "the option to accept some or all cookies or to decline all or some cookies and to retain the possibility to change the cookie settings in the future" [3, p. 5].

How did these guidelines work out in practice?

3.3 The first war

Unsurprisingly the information and consent requirements have raised opposition from the industry. Lobby organisations, such as the IAB (Interactive Advertising Bureau Europe), UNICE (Union of Industrial and Employers' Confederations of Europe), FEDMA (Federation of European Direct and Interactive

[9] There are two exceptions to the consent requirement. Cookies can be used without the user's consent if either they are used (a) for the technical storage of the access to information for the sole purpose of carrying out the transmission of a communication over an electronic communications network and (b) for the provision of an information society service that is explicitly requested by the subscriber or the user, when the storing of or the access to information is strictly necessary for the provider (art. 5(3) ePrivacy Directive, last sentence)

Marketing) have raised concerns that prior and explicit consent of the user would create unnecessary barriers to the internet and have a devastating effect on electronic commerce [16]. The regulation has also been critiqued as being incomprehensible and difficult for providers to comply with[10]. This may well be the case for smaller service providers, such as individual bloggers that incorporate advertisements on their site, but is more difficult to maintain for the big players that have ample in-house legal staff. Maybe the latter just lack incentives to comply. In this light, the distinction in types of regulatees introduced by Kagan and Scholtz [9] comes to mind. First there are the amoral calculators, who base decisions on cost-benefit analyses. Secondly there are political citizens who choose not to comply out of civil disobedience. And thirdly there are the organizationally incompetent who are not able to comply because they lack the information and/or means to do so. The big internet players (ad-brokers, ad-platforms, social media, search engines, etc) belong to category one or two, the small bloggers may belong to category three.

The uptake of the regulation has been slow to put it mildly[11]. Industry has resisted implementation of the required measures, the regulator has hardly enforced the regulation, and the general population could not care less[12].

In a survey of the top 100 Dutch websites we conducted in Spring 2014 [14], we found four prevalent types of implementations of the cookie requirements at the time:

1. Explicit agreement to all cookies used on the site;
   Many websites put up a relatively unobtrusive overlay (usually a 'banner') that basically states that "by entering this site you agree to the use of cookies by this site", which is usually supplemented with a link pointing to additional information about the cookies to be set by the website. To get rid of the intruding overlay, the user actively needs to close it. The websites implementing this approach considered that the active closing of the banner by the user constitutes consent. These banner practices are

[10] DDMA reactie consultatie aanpassing artikel 11.7a Tw (Input to the consultation wrt the modifcation of art 11.7a Tw by the Dutch Dialogue Marketing Association) http://www.Internetconsultatie.nl/cookiebepaling/reactie/4fe0665e-5be2-40a6-a3c6-690f109674fa

[11] http://www.consumentenbond.nl/test/elektronica-communicatie/veilig-online/privacy-op-internet/extra/cookiewet-heeft-weinig-opgeleverd (last accessed 09 November 2014).

[12] Searching Google on "stupid eu cookie law" delivers some 680.000 hits (Nov 2014). Some of the international concerns can be found http://techcrunch.com/2011/03/09/stupid-eu-cookie-law-will-hand-the-advantage-to-the-us-kill-our-startups-stone-dead/ and http://www.wired.co.uk/news/archive/2012-05/24/eu-cookie-law-moaning (last accessed 09 November 2014).

prevalent mechanisms used by website operators throughout the EU [3].

The banner affects the user experience only slightly because it is placed at the top or bottom of the screen and the user can navigate the content out of the way. The banner/overlay clearly communicates to the user that by performing a certain action, such as clicking a button with a text 'accept cookies' or similar, the user accepts cookies to be placed by the site[13]. If the user presses the button, cookies will be set and read. Our study (and others) revealed that many sites actually placed cookies irrespective of pressing the button because the service providers consider the use of the site to imply implicit consent to the use of cookies.

Although the banners and the click-through that leads to more information may be considered adequate with respect to the information obligation, they are insufficient to comply with the Dutch consent requirement (and go against the Art. 29 guidelines as outlined above). Simply clicking on a banner that provides information or having a banner visible on a webpage is no way to express that one consents to the use of cookies, and it also does not provide a clear option to the user to withdraw their consent later in time.

2. Implicit agreement to all cookies used on the site;
   This type represents a very obscure form of the information and consent requirements. Typically buttons on banners of this type merely state 'Ok' or 'Proceed', thus obfuscating the fact that pressing of the button is taken to mean approval of the placement of cookies. In some cases the banner even disappears after a certain time or when the end-user navigates to another page on the site. The 'Proceed' button reminds of the kind of notice and consent found in 'terms of service' that users are supposed to have read and games where one receives instructions for the game first and then has to press 'start' or 'proceed' to actually play the game. In both cases, the user, due to past experience, is likely to just press the button and get on with what they came for. In other words, pressing the button is not actually perceived by the user as signaling consent to cookies being used. Therefore such implementations are insufficient to obtain valid user consent.

3. 'Coerced' agreement to all cookies (cookiewall);
   This type of notice and consent is the most offensive implementation of the requirements. A cookie wall is a prominent overlay that blocks (or

[13] And others given that the banner usually only mentions 'cookies', not whose they are.

greys out) the underlying content and contains basic information about the use of cookies by the site followed by a prominent button that allows the user to signify their consent to the use of cookies. These overlays effectively act as a gatekeeper; unless the user accepts the cookies, access to the site is prevented. Early 2014, some of there overlays claimed that the site is legally required to obtain the user's consent for storing cookies sometimes even implying that it is (legally) obligatory to use cookies (without mentioning that it is actually the publisher's choice to do so)[14]. Many also claimed that the website cannot function without the user accepting all cookies, which is inaccurate. The operator is not required to obtain the user's consent for cookies that are necessary for the site to function (art 11.7a 3b Tw). Operators (willingly and knowingly?) seem to confuse technical necessity with commercial desirability. Also in other respects do website operators creatively comply with the regulation. They nudge [22] users into accepting all cookies, by presenting a green button for consent, and a red one for refusing cookies (or even just for obtaining just more information), thus suggesting that cookies are good for the user[15]. The sad bottom line of the cookie-walls is that although they at first glance appear to offer choice (press green to accept cookies, red to refuse), there actually is only one: accepting all cookies, pressing red means end of story for the user.

4. Detailed choice/consent of cookies. The final option is meaningful choice. There are many implementations within this category, but they all have in common that the user is presented a typology of cookies, such as necessary, improved functionality, social media, (behavioural) advertising, and for each type the option to accept or refuse the respective cookies. Depending on the user's choice, certain functionality may be lacking, such as a forum if the user does not accept social media cookies, or be replaced by other content, such as behavioural advertisements being replaced by other types of advertisements. This type of information/consent regarding the use of cookies matches the regulator's intention as expressed in recital 25 ePrivacy Directive and the Art 29 WP guidance cited above, best.

[14] One of the few sites that is totally open about their reliance on cookies is the subversive 'news-site' Geenstijl.nl. Their cookie-wall states: "[...] I understand that these cookies, scripts and webbeacons are placed by NewsMedia Websites and third parties, for functional and analytic reasons, to provide me with advertisements, *track my internet behaviour or just because they like tracking me*. I also consent to the fact that my personal data can be processed through these cookies, scripts and webbeacons for these purposes. [...]

[15] The publicly funded Vrije Universiteit Amsterdam (`http://www.vu.nl`) used this approach in early 2014. It has since been taken down

Real choice was fairly rare in Spring 2014 and so were cookie walls[16], most sites adopted types 1 and 2. However, the cookie walls were (and still are) the most interesting from my point of view. The regulator aimed at giving the user choice whether or not to accept cookies, maybe even in the hopes that the marking and tracking of users would thus be limited. Cookie walls subvert this 'notice and choice' model. Recital 25 of the ePrivacy Directive leaves room for closing off content if the user is unwilling to accept cookies but this was, according to the Article 29 Working Party [3], meant to concern 'specific website content', rather than the entire website.

Late 2012, a number of high profile websites, including those of the public broadcasting system (NPO, Netherlands Public Broadcasting), which incorporates tens of websites of individual NPO licensees, had put up cookie-walls. This led the parliamentary debate because a publicly funded organisation was basically demanding its visitors to be marked and tracked by a whole range of third parties, which seemed outrageous to many. The Dutch Data Protection Authority (CBP) investigated the NPO practice and issued a letter[17] and later a full report[18] on the NPO's cookie policy. Among other things, the DPA provides their assessment with respect to the legitimacy of cookie-walls. The DPA notes that the NPO users cannot get access to the NPO website – which is sustained by public money –, unless they consent to all types of cookies at once, including third party tracking cookies. The NPO has 'a factual situational monopoly', there is no other way for users to obtain information and programmes of the public broadcasters online. NPO users are obliged to consent to the use of cookies (if they want to visit the sites). They have no free choice[19], and consent can therefore not serve as a ground on which the processing of the collected user data can be justified and therefore there is no legitimate purpose pursued either. The NPO cookie-wall, in other words is illegal.

The DPA's letter and report highlight that coercing users in accepting cookies in order not to be excluded from services is highly problematical, especially in cases of a factual situational monopolies, such as publicly funded

[16] See [14] for details of our sample

[17] Dutch Data Protection Authority, Letter of 31.01.2014 responding to the parliamentary questions on the NPO cookie policy, available at `http://www.cbpweb.nl/downloads_med/med_20130205-cookies-npo.pdf`

[18] Dutch Data Protection Authority, Report on final findings of the investigation of the Dutch DPA on the processing of personal data via cookies by the Dutch Public Broadcaster (NPO), June 2014, available at `http://www.cbpweb.nl/downloads_rapporten/rap_2013_npo-cookies-publieke-omroep.pdf`

[19] A relevant European Court of Justice case in this respect is Schecke (ECJ, 9 November 2010, C-92/09 (Volker und Markus Schecke GbR v. Land Hesse), where the AG argues that a person can not be required to forgo a fundamental right (data protection) as a condition for funding.

universities and public broadcasters. That such monopolies may not misuse their position to undermine autonomy of their users may seem reasonable, but what about cases where users do have a choice to go to other service providers and these providers can argue they have legitimate purposes for using tracking cookies? The DPA letter does not provide much guidance here and as we will see later on, industry has decided they are free to employ cookie-walls.

The NPO has taken down their cookie-wall shortly after the DPA's report, but others have not. In fact, in 2015 others have since enacted cookie-walls. Large websites that depend on advertising revenues have increasingly opted for making their content available only to those users that unconditionally accept all cookies, and that are hence being tracked all over the internet. Their bet seems to be that users prefer content over privacy (or rather, not being tracked)[20].

The fact that websites build cookie-walls, and increasingly seem to do so, shows that they are unwilling to provide internet users with a real choice not to be tracked. This stands in contrast with the goals outlined in recitals 24 and 25 of the ePrivacy Directive.

The cookie debate is full of rethoric [14] and arguments provided by the parties involved need to be taken with caution. The industry has claimed that the rules are unclear and that hence legal uncertainty exists that cannot easily be resolved by individual service providers, leading to user-unfriendly implementations[21].

Another argument hinges on the economic effects[22] resulting from obliging European providers to inform users about cookie policies and obtain their consent versus providers from elsewhere who are considered to be exempt from this obligation[23]. An English entrepreneur phrases this concern concisely in a

[20] One of the few studies regarding the opinion of Dutch users with respect to cookies was conducted by the Dutch Consumer Union (Consumentenbond) in April 2014 among 1000 Dutch Internet users, see `http://www.consumentenbond.nl/test/elektronica-communicatie/veilig-online/privacy-op-internet/extra/cookiewet-heeft-weinig-opgeleverd`.
Half of the respondents always clicks 'OK' on cookie-consent requests, while 25% makes their choice dependent on the website asking for consent. The survey also reveals that a large proportion of the respondents, 71%, wants to be able to block tracking cookies and only a small minority, 11%, is willing to accept tracking cookies from every site. More telling is that of the 50% that accepts cookies, a third would want to block all tracking cookies. Interestingly, 50% periodically deletes (all?) cookies. These results mean that even the people who want to block tracking cookies have discovered that resistance is futile and that there is hardly any other option than to simply play along.

[21] see footnote 10

[22] For instance, in the UK, compliance with the EU's 'cookie law' would cost the UK economy as much as 10 billion pound if implemented correctly according to customer data platform QuBit as quoted in a Wired UK report `http://www.wired.co.uk/news/archive/2012-04/24/eu-cookie-law-compliance-`£10bn in April 2012 (last accessed 11 November 2015).

[23] A report by the Information Technology and Innovation Foundation (ITIF) (available at `http:`

TechCrunch article: "It clearly makes UK companies less competitive because sites we build will need to be plastered with warnings – and our competitors will not. It is a well known fact that at each stage of a signup process you lose customers – if you have to have a big warning sign just for a cookie that will remember you for purely convenience so that it keeps you logged in. The user won't read that detail – they will just think your a privacy nightmare and won't sign up."[24]

3.4 Truce?

The fierce opposition against the strict cookie Dutch regulation by industry has resulted in yet another amendment to the regulation. In 2013, the Minister of Economic Affairs on 20 May 2013 published a Draft Bill for the amendment of Article 11.7a of the Dutch Telecommunications Act (hereafter Bill)[25] and opened a public consultation on the topic. The new amendment regulates that public sector websites[26] can not put up cookie walls, limits the consent requirement for analytic cookies and cookies necessary for providing the requested service, provided these do not (or only to a limited extent) affect the individual's privacy, and determines that processes used for profiling and individual decision making are to be considered processing of personal data as determined in the Data Protection Act (Wet bescherming persoonsgegevens).

Alongside the parliamentary debates on the 2014 amendment, the Dutch DPA published a report on the investigation it carried out with regard to the processing of personal data by the advertising agency YD for behavioural targeting, based on inter alia the use of cookies. The DPA found that offering the users the possibility to opt-out from the installation of tracking cookies and from receiving personalised advertisements did not meet the requirements of

---

//www2.itif.org/2014-economic-costs-eu-cookie.pdf,) estimates the compliance costs at 2.3 billion dollars for the entire EU. The validity of such numbers can be doubted, but there certainly are costs associated with amending websites to comply with the regulation.

[24] See, for instance, http://techcrunch.com/2011/03/09/stupid-eu-cookie-law-will-hand-the-advantage-to-the-us-kill-our-startups-stone-dead/ (last accessed 11 November 2015).

[25] Draft Bill for the purpose of Internet consultation, Amendment of the Dutch Telecommunications Act (Amendment article 11.7a), available at http://www.Internetconsultatie.nl/cookiebepaling/document/731. Unofficial English translation can be found at: http://www.iab.nl/wp-content/uploads/downloads/2013/06/Amendment-Telecommunications-Act.pdf.

[26] "[. . . een dienst van de informatiemaatschappij die wordt geleverd door of namens een krachtens publiekrecht ingestelde rechtspersoon. . . " art 11.7a para 5.

the Dutch law.[27] These developments resulted in companies modifying their cookie policies and a decrease in the number of cookie walls. Also the number of websites implementing differentiated opt-in mechanisms has grown since. The same development was noted in the UK[28] by Eleanor Treharne-Jones. She suggested that the shifting tide compared to the fierce industry opposition to cookie management in 2012 may be due to three alternatives: privacy is seen as a market differentiator and sophisticated cookie management is an instrument in this space, (global) businesses prepare themselves to get ahead of the compliance curve with the proposed EU Data Protection Regulation on the horizon, there may be a maturation of the market where businesses realise that they can comply and build trust without concerns over losing customers. Her conclusion is that changing the mind-set of industry may require regulatory patience to raise industry and consumer awareness and achieve a significant behaviour change instead of strict enforcement.

In 2015, the tide seems to be turning again. Next to the fact that the already noted increase in number of sites that offer meaningful inform and choice mechanisms seems to be continuing, two opposite movements also can be witnessed. On the one hand, the cookie-walls are back. With a bang. A number of prominent websites have opted for clear cookie-walls[29]. They make no secret about their stance in the tracking debate. Their business model is deeply rooted in revenu based on behavioural advertising and they make clear to the user that they will have to play along, else no site visits. The second development is that certain third party cookie users have (finally) taken their responsibility and implemented inform and consent mechanisms. Google, for instance, has changed their consent policies in July 2015. The company now requires publishers to ask site visitors from the European Union for permission to use their data [30]. According to the new policy, publishers have the option to display a prominent link to how Google uses data when using partner sites or apps. Google offers their (AdSense, DoubleClick Ad Exchange, etc) users support in implementing compliant mechanisms[31].

This does not mean that all is well. Many websites (still) implement a very

[27] Dutch Data Protection Authority, Report on final findings of the investigation of the Dutch DPA on the processing of personal data by YD for behavioural targeting, March 2014 with corrigendum of 29 April 2014, available at http://www.cbpweb.nl/downloads_rapporten/rap_2013_yd-cookies-privacy.pdf.

[28] https://iapp.org/news/a/two-years-onhas-the-eu-cookie-directives-time-finally-come

[29] examples are http://www.volkskrant.nl/, http://tmgonlinemedia.nl/, http://geenstijl.nl, http://tweakers.net

[30] See, for instance http://www.cookiereports.com/news/google-banner-is-not-sufficient-to-meet-eu-cookie-consent-requirements

[31] See http://cookiechoices.org

limited consent mechanism. What the banners typically do is provide detailed information about the cookies employed by the site[32], but without offering the user any real choice to reject the placement of (certain) cookies. This means that the 'consent and choice' model is effectively replaced by a 'inform and acknowledge' mechanism.

The discussion regarding the behaviour and opinions of marketers and consumers in the previous section and the status quo described in this section suggest that the effectiveness (and potentially efficiency) of the regulation might be questionable. Is this a case of regulatory failure?

Regulatory failure comes in different flavours[19, ch. 5]. One of them is output failure: regulators fail when they do not produce the outcomes stipulated in their mandate. In the case of the cookie regulation we can try to infer the aims of the regulation from Recitals 24 and 25 of the ePrivacy Directive and Recital 66 of the Citizens' Rights Directive. According to these recitals, the private sphere of citizens is intruded by devices (including cookies, spyware, webbugs) without their knowledge and these devices are used to gain access to information, store hidden information or trace the activities of the user. 'The use of such devices should be allowed only for legitimate purposes, with the knowledge of the users concerned' (Recital 24) and '..., their use should be allowed on condition that users are provided with clear and precise information ... so as to ensure that users are made aware of information being placed on the terminal equipment they are using. Users should have the opportunity to refuse to have a cookie or similar device stored on their terminal equipment.' (Recital 25). The primary aims therefore can be construed as making Internet users aware of cookie practices and providing them with an opportunity to refuse such practices. However, there may be implied aims as well. The recitals implicitly seem to point at proportionality and subsidiarity. If it is necessary to use cookies in a given practice then the website owner should be capable of explaining why and obtain consent. If the cookies are in fact unnecessary, then one can spare the effort of informing the user and obtaining their consent by simply not using cookies. The secondary aim of the cookie regulation can then be framed as an attempt to limit the amount and scope of webcookies. Leenes and Kosta [14] list seven reasons why the regulation fails to achieve this latter aim. The core reasons for failure are the following. Art. 5(3) focuses on the practice of placing information in the user's terminal equipment obtaining

[32] See http://www.cookiereports.com/ for a clear example. The banner reads "We use cookies to support your experience on our site. By continuing to use our site you agree to our use of cookies." Very detailed information about these cookies can be obtained by clicking on 'more information'. Here the user is told that 8 cookies are used for 'Marketing and anonymous cross site tracking'.

information about a citizen, not so much on what this is done for: marking and tracking. If the regulator seriously wants to limit marking, tracking, (behavioural) profiling etc, then it should regulate this more directly. A reason why this has not happened is that politics is divided over the question whether marking and tracking is an acceptable business model or not; the current regulation is a political compromise. A second reason why the regulation fails is that, despite it resulting from a Directive that aims to harmonize regulation across the EU, there are different national implementations, causing publishers to complain about legal uncertainty and undue compliance burden. The third major reason is that the general public does not care. At first they were uninformed about cookies. Once informed about their existence and purposes, they became annoyed by the implementation of the inform and consent mechanisms by publishers. The publishers (and adtech industry in the back) have effectively created a Stockholm syndrome among the general public. Website owners where thus able to create an unusual alliance with the targets (victims) of profiling against their protectors (the regulator). Publishers had no choice but to reject the regulation. They acted rationally. Many web sites depend on advertising revenue and targeted advertisements result in higher revenues than plain advertisements[33]. A final reason I want to mention here is that enforcement is lax. As witnessed in this contribution, the Dutch DPA has issued multiple reports, and so has the ACM (Authority for Consumers & Markets). Serious penalties have so far not been issued.

So, now what? Do we (netizens) throw our towels in the ring, or what?

3.5 Aiding the rebels

The regulator has/had another iron in the fire: Do Not Track. Both the US FTC (since 2010 [7]) and the European Commission (since 2011[12]) have called the industry to develop and adopt a Do Not Track Standard as a means of self-regulation. The World Wide Web Consortium (W3C) has taken the lead in getting the relevant players around the table in September 2011. After years of intense debates, one can seriously doubt whether this initiative will be successful. There is still no agreement about core concepts, several big (advertising groups) have abandoned the initiative and parties, such as Yahoo! have announced they will not honour the DNT signal, thus making it doubtful that the standard will be widely respected by the industry [4, section 8.5]. DNT does not

[33] According to a study sponsored by the Network Advertising Initiative. Howard Beales, The Value of Behavioral Targeting, available at `http://www.networkadvertising.org/pdfs/Beales_NAI_Study.pdf`

seem the way forward in giving netizens meaningful choice whether they want to be marked and tracked.

The new kid on the block is another form of regulation, techno-regulation [13]. Users can take control into their own hands, for instance through ad blockers. Ad blockers have been around for quite some time, buy until fairly recently were only used by tech-savy netizens. That seems to be changing rapidly. At first, ad blockers were primarily used to block advertisements. Increasingly they are also used by people whose main concern is the tracking of their online behaviour. As Doc Searls put it in an article in the Harvard Business Review [20] "Yet ad blockers have been around almost as long as online advertising — certainly as long as we've had browser add-ons and extensions. So why has ad blocking become so popular, so fast? In a word, tracking." In the article he illustrates the relation between tracking concerns and ad blockers by presenting the Google trends graphs for 'How to block ads' and 'retargeting' and both show a clear rise in time[34]. Ad-blockers allow users to specify sources they want their browser to block. Given the fact that many adtech and other entities engaged in profiling are well known, the adblockers can be provided with clear blacklists.

This new battle has just begun, but as a result of Push (Apple, though facilitating content-blockers in iOS 9 and Google(ironically) through their Chrome browser) and Pull (customers), blockers may get the boost required for mass adoption [5]. Pagefair [18] claims there are about 200 million adblock users around the world, with a global growth of 41% in the last 12 months. Growth rates are 48% in the US and 82% in the UK. These are serious numbers. And this may change the bargaining power of users versus content providers and the industry. The industry (and publishers) are openly worrying about the future. As with the first cookie war, there is much hyperbole in the debate.

> 'Every time you block an ad, what you're really blocking is food from entering a child's mouth,"[35].

Ad-blocking is being compared to piracy, stealing and violating an implicit contract between publishers and readers. If it were a real contract, then consent of the users/readers would be required, just as art 5(3) ePrivacy Directive tried to achieve. Now that consent is bypassed and all sorts of third parties introduced into the equation, without the reader being aware of, it is inappropriate to talk about piracy, stealing and contracts.

[34] Google trends shows a slowly decreasing interest in 'Do not track', while 'Ad blocker' gives a hockey-stick curve

[35] Wrote Tom's Guide editorial director Avram Piltch in May 2015 `http://www.tomsguide.com/us/ad-blocking-is-stealing,news-20962.html`

The ad industry and publishers who depend on ad revenues clearly play the moral card, but whether content blocking is morally wrong remains to be seen. [36]

> David Whittier, a former professor of cyberethics at Boston University, said the clearest defense of ad blocking comes from utilitarianism, which suggests that the most ethical action is the one that maximizes utility. "In this case, ad blocking is completely ethical because it by far benefits more people than it harms," he said. "Anyone who says that online advertising is annoying and distracting is absolutely right."[37]

In any case, the discussion about the sustainability of marking and tracking as the foundation of the prevalent business model on the internet is revived. Whether or not it will have any effect remains to be seen. For sure, the ad industry is not going put down their arms, close shop and go fishing. It will find other ways to do, or continue their, business, not necessarily with less tracking of user behaviour. As to the publishers

> ... if you're worried about publishers and advertisers surviving, remember that publishers got along fine before there was adtech, and for most companies advertising is just one form of overhead.[20]

For me as a regulation scholar, the new phase in the cookie debate is interesting because it shows the different modalities at play in regulating human behaviour: law, social norms, market, architecture (code)[15].

References

[1] ARTICLE 29 DATA PROTECTION WORKING PARTY. Opinion 8/2006 on the review of the regulatory framework for electronic communications and services, with focus on the eprivacy directive. Tech. rep., Article 29 Data Protection Working Party, 2006.

[2] ARTICLE 29 DATA PROTECTION WORKING PARTY. Opinion 2/2010 on online behavioural advertising, wp171. Tech. rep., Article 29 Data Protection Working Party, 2010.

[36] Interesting starting points for this discussion are http://blog.practicalethics.ox.ac.uk/2015/10/whats-the-moral-difference-between-ad-blocking-and-piracy/ and http://blog.practicalethics.ox.ac.uk/2015/10/why-its-ok-to-block-ads/

[37] http://digiday.com/publishers/kant-on-ad-blocking/

[3] ARTICLE 29 DATA PROTECTION WORKING PARTY. Working document 02/2013 providing guidance on obtaining consent for cookies (wp208). Tech. rep., Article 29 Data Protection Working Party, 2013.

[4] BORGESIUS, F. Z. *Improving Privacy Protection in the Area of Behavioural Targeting*. Kluwer Law International, 2015.

[5] DEDIU, H. How quickly will ads disappear from the internet?, 09 2015.

[6] EXPERIAN. Americans spend 58 minutes a day on their smartphones, 28 May 2013.

[7] FEDERAL TRADE COMMISSION. Protecting consumer privacy in an era of rapid change: A proposed framework for business and policymakers. Tech. rep., FTC, 2010.

[8] ILFELD, B., AND GOLDMAN, J. ios 9 content blockers: Impact analysis and mitigating strategies. Tech. rep., 10Up, 23 Sept 2015.

[9] KAGAN, R., AND SCHOLTZ, J. The criminology of the corporation and regulatory enforcement strategies. In *Enforcing Regulation* (1984), J. Hawkins and J. Thomas, Eds., Kluwer, p. 494.

[10] KOOT, M. R. *Measuring and Predicting Anonymity*. University of Amsterdam, 2012.

[11] KOSTA, E. Peeking into the cookie jar: The european approach towards the regulation of cookies. *International journal of law and information technology 21* (2013), 27.

[12] KROES, N. Reinforcing trust and confidence. (speech /11/461), Online Tracking Protection & Browsers Workshop Brussels, 22 June 2011.

[13] LEENES, R. Framing techno-regulation: An exploration of state and non-state regulation by technology. *Legisprudence 5*, 2 (2011), 143–169.

[14] LEENES, R., AND KOSTA, E. Taming the cookie monster with dutch law – a tale of regulatory failure. *Computer Law & Security Review 31* (2015), 317–335.

[15] LESSIG, L. *Code and other laws of Cyberspace*. Basic Books, 1999.

[16] MERCADO-KIERKEGAARD, S. How the cookies (almost) crumbled: Privacy and lobbyism. *Computer Law & Security Review 21*, 317 (2005).

[17] OHM, P. Broken promises of privacy: Responding to the surprising failure of anonymization. *UCLA Law Review 57* (2010), 1701–.

[18] PAGEFAIR, AND ADOBE. The cost of ad blocking. Tech. rep., 2015.

[19] ROBERT BALDWIN, MARTIN CAVE, AND MARTIN LODGE. *Understanding Regulation: Theory, Strategy, and Practice*. Oxford University Press, 2011.

[20] SEARLS, D. Ad blockers and the next chapter of the internet.

[21] TENE, O., AND POLONETKSY, J. To track or 'do not track': Advancing transparency and individual control in online behavioral advertising. *Minn. J. L. Sci. and Tech 13*, 281 (2012).

[22] THALER, R. H., AND SUNSTEIN, C. R. *Nudge: Improving Decisions about Health, Wealth, and Happiness*. Yale University Press, 2008.

Author biography

Ronald Leenes is full professor in regulation by technology at the Tilburg Institute for Law, Technology, and Society (TILT), Tilburg University, the Netherlands. His primary research interests are techno-regulation, conceptual issues with respect to privacy, data protection in practice, data analytics, robotics and human enhancement. Currently his work focuses on accountability and transparency in Big Data and the Cloud and on regulatory failure in technology regulation. He was responsible for TILT's research in several EU projects, such as PRIME, PRIMELIFE, ENDORSE, Robolaw and A4Cloud and has contributed extensively to NoE FIDIS. He was PI.lab Scientific Director in 2011-2012. Email: R.E.Leenes@tilburguniversity.edu