J Consum Policy (2014) 37:547–559
DOI 10.1007/s10603-014-9263-3

ORIGINAL PAPER

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

J. A. Luzak

Received: 31 October 2013 / Accepted: 28 April 2014 /
Published online: 10 May 2014

Abstract The reviewed ePrivacy Directive aims at ensuring internet users' online privacy by requiring users to give informed consent to the gathering, storing, and processing of their data by internet service providers, e.g., through the cookies' use. However, it is hardly possible to talk about an "informed" consent if internet users are not aware of cookies or do not understand when and how they work. Currently, European rules require internet service providers to provide internet users with a "clear and comprehensive" information on the cookies' use without further specifying what kind of disclosure would be seen as compliant therewith. This paper assesses the need for harmonized European guidelines on transparent and readable disclosure on the cookies' use and suggests the way forward based on comparative legal research and findings from consumer behaviour research.

Keywords Online privacy · Cookies' use · Informed consent · Disclosure's transparency · Disclosure's readability

"Cookies" are small text files that are set on an internet user's computer when one browses the internet. Due to these cookies, the websites that internet users visit as well as other data on internet users may be tracked and stored (Charters 2002, p. 245; Miyazaki 2008, pp. 20–21). The basic objection to such practices as the cookies' use by website operators and other professional parties (the "marketers") is that internet users are often unaware of the cookies' use and have no control over them, which may lead to the infringement of users' online privacy (Charters 2002, pp. 248–250; Helberger et al. 2013, pp. 14–15, 161; Luzak 2013, pp. 225–227; Michelfelder 2001, p. 135; Pollach 2005, p.225). Studies show that even if ca. 90 % of experienced internet users claim to know cookies, only ca. 15 % can correctly answer any specific questions about them (Miyazaki 2008, p. 21). Internet users not only do not know what cookies are but usually are also not informed or not clearly informed that cookies are set

J. A. Luzak (✉)
Centre for the Study of European Contract Law, University of Amsterdam, Amsterdam, The Netherlands
e-mail: j.a.luzak@uva.nl

on their computers or for what purposes the information gathered through the cookies' use is processed (Charters 2002, p. 245; Kierkegaard 2005, p. 317; Pollach 2005, p. 222). Behavioural research suggests that knowledge about data risk and about regulations on personal data protection could help motivate internet users to better guard their personal information online (Park et al. 2012, pp. 1024–1025). This paper argues for the European guidelines' introduction that would specify the design, content, and form of privacy notices through which internet users would be better informed about the cookies' use. After all, it is hard to imagine that the cookies' use would decline, taking into account their usefulness in data collection accumulated for targeted online advertising, which is nowadays seen as one of the most effective ways to gain consumers' attention (Jennings 2012, pp. 193–194).[1] Following the old adage "if you can't beat them join them," the increased transparency about the cookies' use should enable better internet users' choices as far as data protection is concerned.

In order to ensure the protection of the right to online privacy, the new Article 5(3) ePrivacy Directive[2] states that internet users should receive "clear and comprehensive information" about the fact that their data may be accessed, stored, and processed online (Papakonstantinou and De Hert 2011, p. 29). Pursuant to this provision, users should be fully and in advance informed of the cookies' existence and use which may give them some control over the cookies' application and, therefore, a possibility to protect their online privacy. However, the European legislator leaves it unsaid what the yardstick should be for determining whether a given privacy notice is sufficiently clear and comprehensive, leaving it pursuant to Article 15a to the Member States to assess the marketers' compliance with this rule (Luzak 2013, pp. 229–231). If the privacy notice was standardized, then internet users would know what to expect when they visited a website, regardless of in which Member State the party who operated it was located. The same information appearing on various websites could facilitate internet users' education about cookies.[3] In turn, internet users who were more familiar with and more knowledgeable about cookies should on one hand feel more secure about concluding online transactions, since they would know the risks associated therewith, and on the other hand could better protect themselves from online risks. Surveys showed that almost 70 % of internet users refused to provide their personal data to the marketers due to a lack of information on the website on how these data would further be used (Hoffman et al. 1999, p. 82; Park et al. 2012, pp. 1024–1025).

Therefore, this paper's normative aim is to argue for a development of guidelines for future regulation and standardization of European privacy notices. The next chapter summarizes consumer behaviour research findings, establishing what sort of information and its method of conveying could be perceived as clear and comprehensive by internet users. These standards could then serve as a model when European guidelines are drafted. Additionally, the second chapter explores the link between an increased exposure to the same information and the

[1] The link between consumer behaviour research and internet users' behaviour that is made in this paper is based on the assumption that internet users are indeed often consumers and as such are likely to suffer from information asymmetry, as well as various behavioural biases.

[2] 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 ("ePrivacy Directive") [2002] OJ L201/37. Article 5(3) was changed by 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 (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws ("Citizens' Rights Directive") [2009] OJ L337/11.

[3] See further on this in Chapter 2.

internet users' learning process, which link needs to be further studied if the recommendation for privacy notices' standardization is to be given. The following two chapters show that a lack of European guidelines leads to divergent interpretation and differing information requirements' implementation regarding the cookies' use in at least some Member States. This could contribute to a lack of clarity and confidence among internet users in concluding cross-border transactions and, therefore, to the internal market's suffering (IMCO August 2011, pp. 14, 16, 77, 102). This paper presents divergent implementation measures on an example of English and Dutch law, which both struggled with timely and efficient adoption of the new rules. While the implementation deadline was set for May 2011, the Netherlands introduced relevant changes to its Telecommunication Law[4] only in June 2012. The UK's parliament transcribed the new provisions in time but immediately thereafter the Information Commissioner's Office (the "ICO"), an authority entrusted with their enforcement, announced that they would delay enforcement for at least a year (McDougall 2011). The ICO issued then very specific guidelines[5] on how to formulate privacy notices, which allow for an interesting comparison when contrasted with more general Dutch guidelines issued by the Onafhankelijke Post en Telecommunicatie Autoriteit (the "OPTA") (ICO May 2012, pp. 1–30; OPTA 2012, pp. 1–5) as to their potential of standardizing cookies' disclosures in these Member States. These national guidelines are evaluated from the perspective of consumer behaviour research findings as defined in the second chapter. Moreover, I assess whether these two Member States have complied with the obligations set in Article 15a of ePrivacy Directive for competent national authorities to effectively monitor privacy infringements and to enforce ePrivacy Directive's objectives. In the final chapter, general findings from this paper are compiled in order to draft an example of what European guidelines at one point could look like.

Consumer Behaviour Findings

It has been argued in the legal literature that internet users' consent should only be seen as such when it was an "informed consent" (Helberger et al. 2013, pp. 157–158; Opinion 2/2010, p. 12; Opinion 15/2011, p. 9).[6] Internet users may only then be seen as having given informed consent, when they were fully informed, have understood the information given to them, and have explicitly agreed to their personal data's collection and processing by the marketers. Therefore, it is crucial to investigate what could be seen as "clear and comprehensive information" on cookies' use since it cannot be assumed that *any* information given in the privacy notice would fulfil this requirement. Upon the breach of this obligation, internet users would not be able to give informed consent to their personal data's use, which would mean that their online privacy could be infringed.[7]

Providing internet users with a "clear and comprehensive information" on the cookies' use, e.g., in a privacy notice, is one way in which the marketers could help internet users to decide whether to disclose personal information to a given marketer (Helberger et al. 2013, p. 54; Liao et al. 2011, p. 712; Milne and Culnan 2004, pp. 16, 24; Schwaig et al. 2013, p. 9; Wirtz et al. 2007, p. 341). However, studies showed that this will only hold true upon fulfilment of three

[4] Telecommunicatiewet, 19.10.1998 with changes, http://wetten.overheid.nl/BWBR0009950/geldigheidsdatum_29-06-2012.

[5] A few guidelines have been issued by the ICO, the most recent one (of May 2012) will be referred to here.

[6] See on informed consent: Sefton-Green 2005, pp. 171–173; Gozzo 2005, pp. 22–30.

[7] This paper focuses on the analysis of the requirements for an "informed" consent, leaving the methods of obtaining users' consent outside its scope.

conditions. Firstly, a privacy notice needs to attract internet users' attention so that they are inclined to read it. Secondly, it should truthfully reveal privacy rules that a given marketer observes. Lastly, a privacy notice should be understood by internet users, which means the information needs to be given in a coherent and legible way (Helberger et al. 2013, p. 14; Milne and Culnan 2004, p. 16).

Internet users need to be enticed to read privacy notices. Attractiveness of the privacy notice's display, e.g., giving it a prominent place on a website, may increase the internet users' chances of actually noticing and reading it (Harridge-March 2006, pp. 754–755; Milne and Culnan 2004, pp. 17, 19, 25; Wirtz et al. 2007, p. 341). Therefore, it stands to reason that the font in which a privacy notice is written should not be smaller than the other information's font that is conveyed on a website and that the text should be concise in order to be comprehensive (Milne and Culnan 2004, p. 23). For clarity's sake, it could be argued that a detailed privacy notice should be provided to internet users on a website's separate page, and that only a link that leads to it should be prominently displayed at the main website itself (Jones and Tahri 2010, p. 620). However, that link should be clearly visible to anyone visiting a website for the first time, since it may be unrealistic to expect internet users to search for any privacy notices that may have been placed on a website (Van Wel and Royakkers 2004, p. 134). The marketers should only not stop at just trying to draw the users' attention to a privacy notice but should also try to have them read it. Currently, research shows that internet users often do not read privacy notices since they are too long, too boring, hard to understand, and often the same (Milne and Culnan 2004, p. 23).[8] Across the European Union, 41 % of internet users admit to not reading privacy notices on websites (IMCO August 2011, pp. 80–81) and more specifically, e.g., 60 % of British primary and secondary school respondents confess to not reading privacy policies (Furnell and Phippen 2012, p. 15).[9] Since internet users are more likely to read privacy notices when they perceive them as understandable (Milne and Culnan 2004, p. 24), it should be ascertained that a privacy notice is comprehensive, brief, and written in a plain language.[10]

As far as the privacy notice's content is concerned, the most important information that the marketers should reveal to internet users is whether and how they use cookies and who will have access to the data collected through them (Harridge-March 2006, p. 752; Jones and Tahri 2010, p. 619; Michelfelder 2001, p. 132; Nowak and Phelps 1995, p. 57). The marketers should be truthful in their disclosure (Harridge-March 2006, p. 756). Research showed that if internet users do not trust a marketer to reveal correct information or to comply with the information he reveals, then they are less likely to spend time and effort on reading privacy notices (Dinev and Hart 2006, pp. 73–74; Milne and Culnan 2004, p. 18). Other studies pointed out that if consumers feel that a message is personally relevant to them, they would be more likely to read it (Milne and Culnan 2004, p.18). In this respect, entitling a privacy notice, e.g., "find out more about how our site works and how we put you in control" could be expected to be effective. Moreover, it could be beneficial to avoid labelling it as a "privacy policy," in order not to create a misleading impression with internet users that the sole existence thereof signifies protection of their data on a given website. In a study, 75 % of respondents when asked about the significance of a privacy notice's existence on the marketer's website believed that it would mean that the marketer would not share their information with others (Turow et al. 2008, p. 422). Since the information's comprehensiveness depends to

[8] One of the surveyed consumers asked: "How about the 'Privacy Notice for Dummies' version?"
[9] Similar data comes from the US research, see, e.g., Earp and Baumer 2003, pp. 81–83.
[10] The following paragraphs discuss how to make the content of privacy notices more understandable to internet users.

a large extent on the capabilities of the audience receiving it, then websites directed at a specific demographic, e.g., young internet users, should adjust their content pursuant to their average users' knowledge and expectations (Milne and Culnan 2004, p. 19; Nowak and Phelps 1995, p. 57). If the privacy notice's content changes, internet users should receive a clear notification thereof, since it cannot be expected that they would re-check the privacy notice every time they access the website (Van Wel and Royakkers 2004, p. 134).

Even if internet users read a privacy notice, they still may not understand what they have read and what are the potential threats to their privacy. With regards to clarity of the form in which the information is provided to internet users, the language used by the marketers is of crucial importance. Unfortunately, privacy notices are often written in a legal jargon that serves to protect the marketers against any potential lawsuits rather than to actually be informative to internet users (Pollach 2005, pp. 223, 228). American researchers found that in order to understand 80 % of the examined privacy notices more than a college degree was necessary (Pollach 2005, p. 223). Recent British survey tested privacy notices of various popular social websites, e.g., Facebook, Twitter, and LinkedIn, and evaluated their text as at least "difficult" if not "confusing," pursuant to the Flesch Reading Easel standards (Furnell and Phippen 2012, pp. 14–15). The British researchers estimated also that these privacy notices could not be understood by people with a reading age of under 16, while it is believed that about half the working adults in the UK have a reading age of 11 or lower, pursuant to the Flesch Kincaid Grade Level standards (Furnell and Phippen 2012, pp. 14–15). It is not only the legal jargon but also the complicated syntax's use, the lack of straightforward answers, and the modalities' use (e.g., "from time to time," "occasionally") that allow the marketers to downplay the frequency and the probability with which certain data handling practices take place (Pollach 2005, p. 228). This could be the result of either the marketers' intention to obscure unfair data handling practices or their lack of drafting skills. Regardless the reason, internet users upon reading such a privacy notice would not understand how their data would be used, which means they would not be able to protect their online privacy by giving or refusing to give an informed consent to such data gathering practices (Helberger et al. 2013, p. 15). Behavioural studies show that the more straightforward the information is given to consumers, the more they will trust in its message and be likely to read it (Harridge-March 2006, p. 756; Milne and Culnan 2004, p. 19; Schoenbachler and Gordon 2002, p. 14). A privacy notice which gives an impression to internet users that certain practices are used only from time to time reduces the disclosure's information value, and as such should not be classified as "clear and comprehensive" (Caudill and Murphy 2000, p. 13; Pollach 2005, pp. 228, 230; Van Wel and Royakkers 2004, p. 134). Therefore, it should be recommended to draft a privacy notice in categorical terms, without the use of adverbs of frequency or exceptions, which would make it impossible for internet users to precisely determine when and how their data are used. The legal jargon should be avoided as much as possible; preferably layman terms should be used (Caudill and Murphy 2000, p. 16; Wirtz et al. 2007, p. 341).

Consumer behaviour studies point also to valid reasons why the information given to internet users on the cookies' use should be harmonized across Europe. Firstly, it is likely that if internet users are exposed to the same information, presented in the same format, time, and over again, they would learn to recognize it easier and start paying more attention to it, as well as know better what they should expect from it.[11] This could facilitate internet users' education

[11] This strategy tends to be successful in making consumers pay attention to advertisements (Pechmann and Stewart 1988, pp. 285–330; D'Souza and Rao 1995, pp. 32–42; Yaveroglu and Donthu 2008, pp. 31–43). Research shows also robustness of the repetition priming effect, proving that the repetition of identical signs results in faster and more accurate responses, e.g., with regards to traffic signs (Castro et al. 2007, p. 39–40). On the other hand, some researchers claimed that repeat exposure to the same information could desensitize consumers (Magat et al. 1988, pp. 201–232).

process about cookies and make them feel more confident as to their use online. Secondly, previous studies on information processing by consumers showed that especially when consumers were confronted with a large number of information at once and they needed to analyse it in a short time, they were inclined to make trade-offs. These trade-offs result in a choice as to which information consumers will follow more closely and which they will not spend much of their energy and time on (Morris et al. 1989, pp. 64–80). Again, when the marketers wanted consumers to focus on a specific information statement and, therefore, increased their exposure thereto, this caused consumers to indeed be more likely to start paying attention to this information (Friedmann 1988, pp. 507–515). Additionally, researchers found a positive correlation between knowledge about and understanding of data collection risks and of existing regulatory protection, and the level of protective measures that internet users were willing to undertake (Park et al. 2012, pp. 1024–1025). When internet users had a better grasp on the data collection's existence and its process, they were more likely to protect themselves from such actions. The fact that nowadays there seems to exist a privacy paradox, where internet users describe their fear of and unwillingness to share their personal data but then proceed to give it away anyway, might then be explained by the lack of understanding of the data collection's process and risks (Turow et al. 2008, pp. 412, 420–422).

Let us now look whether cookies' disclosures in the UK and in the Netherlands correspond to the rules mentioned in this chapter as a result of the implementation and enforcement of the new ePrivacy Directive rules. There may be no need for the European guidelines if internet users are exposed to the same information with regards to the cookies' use.

English Guidelines

The UK implemented the new provisions of the ePrivacy Directive on the 25th of May 2011 through the ePrivacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011, but refrained from the active enforcement thereof for another year (ICO May 2012, p. 2; McDougall 2011). Prior to the implementation, a report was commissioned by the Department for Culture, Media, and Sport to assess the new rules' potential impact on cookies (DCMS April 2011, pp. 1–91). The report showed that most British internet users have limited understanding of cookies and the way they work (Furnell and Phippen 2012, pp. 12–18; ICO May 2012, p. 3). This might have been the reason why the British authorities decided to focus their implementation efforts on increasing knowledge about and of cookies among internet users (Evans 2012). Broader consumer education was seen as a key to making internet users more comfortable online and giving them some more control over their online privacy (Bond 2012, p. 215; ICO May 2012, p. 3). While the ICO did not consider it one of its responsibilities to determine the precise wording of the information that should be given to internet users, it provided the marketers with certain suggestions and examples as to how to comply with the new rules (ICO May 2012, p. 8). These examples do not constitute an exhaustive list of proper methods of conveying information about the cookies' use to internet users, and therefore, they do not guarantee legal certainty. The marketers may still choose another method and/ or form to inform internet users about the cookies' use, and they could still be seen as complying with the European rules. On the other hand, by keeping this list open, the ICO makes sure that if other technological developments come along that enable conveyance of such information in a clearer, user-friendly way, the marketers could use them.

The ICO guidelines make it clear that the requirement of providing "clear and comprehensive" information does not only pertain to the content thereof but also to its form and design. As far as the design is concerned, before the information can be read and understood by

internet users, it has to first attract their attention and entice them to read it (ICO May 2012, p. 18). In this respect, the ICO notices that internet users are more likely to notice the information if it is a website's integral part and when it fits in the website's design (ICO May 2012, p. 8). The ICO does not consider as sufficient a current marketers' practice to refer to the privacy notices at the bottom of a website through a link placed there, unless this link is prominently visible. In order to increase the link's attractiveness, it should be formatted differently than the other text placed on the website, making it distinguishable as important information. The marketers could use a different font size or style to this aim. Links placed on the bottom of a website are considered easy to overlook, especially if they only become visible after an internet user would scroll through large amounts of text. Therefore, for compliance sake, it may be better to move a link to the top of the website or to its side. Such a link should point out very clearly to its function: educating internet users on cookies and their effect. A link titled "privacy notice" is unclear, contrary to "what cookies we use and how they influence you" or, what the ICO advises: "find out more about how our site works and how we put you in control." In addition, the rephrasing of the link's title in the above-mentioned way makes a link more personal to internet users. Comparing these suggestions with the consumer behaviour research findings as described in the previous paragraph, we may see that the ICO took them into account when drafting their guidelines. Other techniques that are being recommended for the marketers to use are: mouse over highlights (making the link stand out among other text) or clickable images (e.g., of a cookie, to attract attention). Additionally, headlines in the "news" sections of a website could point out to the change in the privacy notice and the internet users' need to find out more about cookies (ICO May 2012, p. 18). The ICO mentions, however, that setting the information about cookies in the website's privacy notice will not always be seen as compliant. Namely, when there is no prior relationship between an internet user and a website, i.e., the internet users is not registered at the website as a customer or a recurrent visitor and he just browses through it, then it may not be expected of the internet user that he will make an effort to read a privacy notice. In such a case, the information about cookies should be prominently displayed on a website itself and not just linked to it (ICO May 2012, p. 23).

When assessing whether the information provided by a marketer is "clear and comprehensive," the information's content needs to be considered. While deciding what kind of information should be conveyed to internet users, a marketer should take into account the expected knowledge of internet users visiting this marketer's website. If the marketer expects its audience to be technically savvy, he does not have to include in its information the very basic explanation as to what cookies are. Instead, he may focus on the information about how his website uses cookies (ICO May 2012, pp. 8, 17, 22). In this respect, the information would more likely be considered as "comprehensive," if the marketers in their privacy notices explained the function and working of different cookies they used instead of just listing them all (Bond 2012, p. 215; ICO May 2012, p. 17). For example, if a cookie is used for remembering in what language version an internet user wants to access a website, then the information should explain that and notify the internet user that the next time he visits he will not have to repeat his choice, since it will be remembered by the cookie (ICO May 2012, p. 21). Additionally, if the information is gathered or processed by third parties, then this fact should be pointed out specifically to internet users. The marketers should also convey additional information (or link to it) regarding who that third party is and how it may use the information (ICO May 2012, pp. 22–23). It is necessary to include in the information's scope, details on how internet users may withdraw their once-given consent to cookies' use and how they may remove cookies that have already been set on their computers. This part of the information should also explain the consequences that cookies' removal would have on the website's functionality (ICO May 2012, p. 25).

Finally, the information would only then be clear and comprehensive to internet users if upon reading it, they understand it (ICO May 2012, p. 17). The form in which the information is given is of crucial importance. For example, the marketers need to make sure that the language they use in drafting the information is suitable for their audience (ICO May 2012, p. 8). Highly technical language explaining how the website works would likely not be understood by most internet users. This is again in tune with the recommendations from the consumer behaviour research to simplify disclosures and introduce plain language in them. However, it is a bit disappointing that the ICO did not try to draft model disclosure texts for the marketers to follow in their privacy notices.

Alongside the ICO, also the International Chamber of Commerce (the "ICC") issued a cookie guide. Since the guidelines of the ICO are not exhaustive and the marketers may be flexible in their compliance therewith, it does not surprise that the industry decided to self-regulate in this area. Interestingly, the ICC guidelines reach somewhat further in their suggestions to the marketers as to how to draft proper privacy notices. This may suggest that the industry sees the need for the standardization and attempts to achieve it despite a lack of a mandatory requirement thereof on national or European level. While the ICO points out mostly certain methods of how to draw internet users' attention to the information on the cookies' use and how to obtain their consent to this use, the ICC guidelines are more specific as to the information notice's content. They provide specific standard notices' wording that could be directly transcribed by the marketers into their privacy notices (ICC April 2012, pp. 1–15). It is believed that if the marketers use the same notice to explain to internet users what cookies are and how they are used, harmonizing the language used by the marketers, this should facilitate better understanding and easier learning by internet users (Bond 2012, p. 215; ICC April 2012, pp. 2–3). Since cookies serve different functions and, therefore, the data's amount and sort that they gather varies significantly, the ICC drafted various exemplary privacy notices dependent on the cookies' category. Cookies have been divided into four main categories: strictly necessary, performance, functionality, and targeting/advertising cookies (Bond 2012, p. 215; ICC April 2012, pp. 7–9). This practice is noteworthy since it disproves a belief that disclosures on cookies could never be standardized due to their varied functions and roles. As the ICC shows, at least the basic disclosures could be harmonized. Moreover, the ICC advises the information's layering, with the most important, basic information about cookies being visible immediately upon accessing the website. The marketers could entice internet users to read this information by using certain icons, e.g., even a picture of a cookie, that would attract their attention and convey information in a contextual way (ICC April 2012, p. 5). More detailed information about the cookies' use could be given through a privacy notice or some other notice that the home page would refer to (ICC April 2012, pp. 3–4).

It needs to be said that while the UK's authorities and self-regulatory bodies provided detailed guidelines on the transparency of cookies' disclosures, due to a lack of efficient enforcement there is a lot of divergence as to the compliance therewith in practice. Even after the additional year granted to the marketers to adjust their disclosure practices has passed, the ICO refrained from taking any strong measures to assure compliance, which reluctance could constitute a ground for infringement of Article 15a of the ePrivacy Directive (BBC 2012; Lee 2012). In theory, just like Article 15a requires, the ICO has "the necessary investigative powers and resources, including the power to obtain any relevant information they might need to monitor and enforce national provisions adopted pursuant to this Directive." However, in practice, the ICO originally announced that it would only act upon complaints, meaning it would not actively investigate non-compliance with these rules. Additionally, while it has the authority to sanction the marketers' misconduct, it is more likely in practice to suggest to the non-compliant websites what steps to take to remove the infringement instead of taking legal

actions against them (BBC 2012; Evans 2012; ICO May 2012, p. 27). This original weak point has been only partially remedied, since the ICO examined 200 most visited websites without waiting for consumers' complains.[12] Additionally, in May 2013, the ICO joined an international group of enforcement authorities in a sweep intended to improve online privacy policies. The intention of the ICO was to examine 250 websites based in the UK out of their own initiative, not upon a complaint, and, among others, to check the language of their cookies' disclosures, that is whether the wording is sufficiently clear and comprehensible (Williams 2013).[13]

Dutch Guidelines

There was a long debate in the Dutch Parliament on some of the new provisions of ePrivacy Directive that resulted in a 1-year later transposition of these rules into Dutch law. After the new law was adopted, the Dutch authority responsible at that time for enforcing the new rules, the OPTA issued its guidelines on how to comply with the new legislation (OPTA 2012, pp. 1–5).[14] Even just upon a marginal check, it is obvious that these guidelines are of a more general nature and contain only basic explanations as to how to interpret the new provisions. They do not provide the marketers with examples on how to properly convey the information to internet users, nor do they aim at standardizing this practice. The guidelines mention that it is up to the parties to decide how the information should be provided. However, it is suggested that a general reference to a marketer's privacy notice or his standard contract terms would not be considered as sufficiently clear information on the cookies' use. Such a reference would not inform internet users to what they are giving their consent nor what its scope is (OPTA 2012, p. 3).

As far as the information notice's design and content is concerned, the guidelines point out only to the fact that such information should be easily visible on a website and easily understandable to internet users. The marketers are obliged to inform internet users about the fact that they use cookies and for what purposes. It is indicated that the assessment whether a marketer complied with these requirements may depend on whether a typical internet user visiting the website would have considered the information as visible and understandable (OPTA 2012, p. 3). There is no mention as to whether the link to the cookies' disclosure should be placed on the top or bottom of a website, what language it should be drafted in, whether the notice should be fully visible on a main page or layered. While the Dutch authorities have to be aware of the consumer behaviour research findings suggesting answers to some of these questions, contrary to their English counterparts they have avoided to make any recommendations to the marketers as to what disclosure could allow internet users to become more "informed."

The only similarity between these national guidelines is that in both cases the information notice's scope and form is related to the knowledge of a typical internet user visiting the website. Aside this specification, the British authorities provided the marketers with more guidelines on proper compliance with the new rules, basing some of them on the principles recognized in consumer behaviour research as facilitating information provision. It is likely

[12] As a comparison, the ICO received 53 complaints in the period October–December 2013 (http://ico.org.uk/enforcement/action/cookies).
[13] The results of this sweep are not yet announced.
[14] As of 1 April 2013, the OPTA constitutes a part of the ACM (Autoriteit Consument en Markt)—the Authority for Consumers and Markets.

that British companies would either use one of the standard text notices provided by the self-regulatory body, the ICC, to inform internet users on the cookies' use or they would follow the ICO's guidelines and draft their own disclosures based thereon. If these guidelines' enforcement was more strict, we could possibly witness privacy notices' standardisation in the UK. On the other hand, the Dutch marketers have not received any specific instructions as to how they should inform internet users about cookies. Since it could be expected that they would be directed by what fits best their business practice, they are likely to differently draft their privacy notices. Therefore, the information given to internet users on the cookies' use by the Dutch marketers would differ from one website to another. Obviously, this could also contribute to the lack of clarity in cross-border transactions. Therefore, despite the OPTA promising to enforce compliance with new provisions either upon complaints or as a result of its own investigations into infringements, it is also difficult to recognize Dutch compliance with Article 15a of ePrivacy Directive, even if the reasons for it differ.[15]

European Guidelines

This paper's previous chapters made it clear that currently there are no uniform European guidelines as to how a privacy notice should be drafted or how internet users should be informed about the cookies' use.[16] The requirement of the ePrivacy Directive that the information given to internet users on the cookies' use should be "clear and comprehensive" could be and is variously interpreted. Some Member States may try to harmonize how the information should be drafted in their own legal system, e.g., the UK. Some other Member States may leave it to the marketers to choose for the best way to draft this information, e.g., the Netherlands. In neither of these two Member States, the standardisation of privacy policies has been achieved when it was left to the industry to provide the standards. However, at least partially, the lack of standardisation may be attributed to the lack of efficient enforcement of the new rules. Considering the above-mentioned, it may be argued that the lack of European guidelines stands in the way of the internal market's further development by not facilitating internet users' trust and confidence in concluding safe online cross-border transactions (Jennings 2012, p. 197). Leaving some options open as to the method in which this information should be provided to internet users can be understood, since it could help accommodating new technological advances. However, as it has been mentioned, it is in both internet users' and the marketers' interest that internet users are made aware of the cookies' existence and the way they operate. Based on the consumer behaviour research, it seems that to achieve this purpose at least the basic information about cookies should be standardized. Moreover, such a standardisation should help the Member States to achieve the goal mentioned in Article 15a of ePrivacy Directive: of effective national and cross-border enforcement of privacy protection rules. Some recent developments of European consumer law also support the standardisation's idea, e.g., new Consumer Rights Directive[17] provides a model form in its Annex IA that could be used to inform consumers about their withdrawal rights and how to use them. It remains to

[15] OPTA started its enforcement of the new cookies' rules by sending a letter in September 2012 to over 100 governmental websites to urge them to comply therewith (http://optajaarverslag2012.acm.nl/jaarverslag/consumenten/internetveiligheid/handhaving-cookies/). There is no mention of any fine or non-compliance actions that it had to take against Dutch marketers since the adoption of the new rules.

[16] This is true not only in Europe but also in the USA, see, e.g., Culnan 2000, p. 24.

[17] Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights ("Consumer Rights Directive") [2011] OJ L304/64.

be seen whether upon implementation and enforcement of this standardized information form, European consumers' knowledge about their right of withdrawal will increase.

At this moment, the European guidelines on the "clear and comprehensive information" on the cookies' use are very limited. It is recommended that this information should be provided directly on the screen, interactively, and be easily visible and understandable (Opinion 2/2010, p. 18). This suggests that the information should not be hidden among longer texts, e.g., of standard terms and conditions or privacy policies that are published on the website (Opinion 2/2010, p. 18). It seems that these guidelines focus only on assuring the information design's clarity. In order to ascertain that European internet users learn to recognize a privacy notice regarding the cookies' use at a glance and do not miss it on any websites, it could be advisable to promote one, specific design.[18] Based on the presented consumer behaviour studies, the European guidelines should require the marketers to publicize a link that would lead to their privacy notices, titled, e.g., "find out more about the cookies we use and how we put you in control." The title should clearly refer to the information's personal relevance for internet users. In order to further attract internet users' attention, a standard icon or a cookies' picture could be attached to that missive. The disclosure's design about the cookies' use could also prescribe that this missive was made visible at a specific part of the website. Whether it were a website's top or side could depend on further conducted empirical research. For example, by tracking eyeball movement of internet users, it could be measured when they are more likely to notice such disclosure, depending on its position, or even different font used.

The next step would be for the European institutions to focus on standardizing the information's content and form across Europe. Currently, cookies used by various websites differ significantly. Therefore, the guidelines might need to differentiate the privacy notices' content with regard to the cookies' category they pertain to, just like the ICC's guidelines have done, e.g., strictly necessary, performance, functionality, or targeting/advertising cookies. For the sake of visibility, such categories could be distinctively marked by differently designed icons. The marketers should be allowed to build upon the privacy notice's standard content, but the text explaining the cookies' basic mechanisms could be easily harmonized per cookie category and required to be literally taken over by the marketers. If the European guidelines contained such a basic cookies' description, their drafters could make sure that the form in which the information is phrased is accessible to laymen and that the information is not overly legalistic and technical. Additionally, through the use of layering, it could be ascertained that internet users' attention is always diverted to the basic disclosure on cookies. If internet users want to find out more about the website's privacy policy, they can always proceed to read it further, e.g., on a different website.

The above-mentioned ideas on how to standardize disclosure on the cookies' use are certain suggestions that would need to be empirically tested in order to see whether they could improve internet users' understanding of cookies. We have tried many solutions to protect internet users' privacy, but standardisation was not yet given a chance in practice. At the moment, every survey conducted outlines a sad reality that despite the recently changed European provisions on disclosure about cookies, European internet users are still ignorant thereof. As a result of the changes suggested in this paper, European internet users could get their "privacy notice for dummies" which should facilitate a widespread understanding of what cookies are and how they operate. Then, and only then, we could talk about internet users' potential capability to protect their online privacy by making an informed choice as to whether they want to consent to a particular cookies' use.

[18] The research on standardization in advertising sector mostly shows benefits thereof. See footnote 11.

References

BBC. (2012). *Thousands of websites in breach of new cookie law*. Available at http://www.bbc.com/news/technology-18206810.

Bond, R. (2012). The EU e-Privacy directive and consent to cookies. *Business Lawyer, 68*, 215.

Castro, C., Tornay, F. J., Horberry, T., Martínez, C., Gale, A., & Martos, F. J. (2007). Worded and symbolic traffic sign stimuli analysis using repetition priming and semantic priming effects. *Advances in Psychology Research, 53*, 17–46.

Caudill, E. M., & Murphy, P. E. (2000). Consumer online privacy: Legal and ethical issues. *Journal of Public Policy & Marketing, 19*, 7–19.

Charters, D. (2002). Electronic monitoring and privacy issues in business-marketing: The ethics of the doubleclick experience. *Journal of Business Ethics, 35*, 243–254.

Culnan, M. J. (2000). Protecting privacy online: Is self-regulation working? *Journal of Public Policy & Marketing, 19*, 20–26.

D'souza, G., & Rao, R. C. (1995). Can repeating an advertisement more frequently than the competition affect brand preference in a mature market. *Journal of Marketing, 59*, 32–42.

Department for Culture, Media and Sport (the "DCMS") (2011). *Research into consumer understanding and management of internet cookies and the potential impact of the EU Electronic Communications Framework*. Available at http://www.culture.gov.uk/images/consultations/PwC_Internet_Cookies_final.pdf (p. 1–91).

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for E-commerce transactions. *Information Systems Research, 17*, 61–80.

Earp, J. B., & Baumer, D. (2003). Innovative web use to learn about consumer behavior and online privacy. *Communications of the ACM, 46*, 81–83.

Evans, D. (2012). ICO blog: Education key to cookie law progress. Available at http://ico.org.uk/news/blog/2012/education-key-to-cookie-law-progress.

Friedmann, K. (1988). The effect of adding symbols to written warning labels on user behavior and recall. *Human Factors, 30*, 507–515.

Furnell, S., & Phippen, A. (2012). Online privacy: a matter of policy? *Computer Fraud & Society* 12–18.

Gozzo, P. (2005). The strategy and the harmonization process within the European legal system: Party autonomy and information requirements. In G. Howells, A. Janssen, & R. Schulze (Eds.), *Information rights and obligations* (pp. 22–30). Aldershot: Ashgate.

Harridge-March, S. (2006). Can the building of trust overcome consumer perceived risk online? *Marketing Intelligence & Planning, 24*, 746–761.

Helberger, N., Guibault, L., Loos, M., Mak, C., Pessers, L., & Van Der Slot, B. (2013). *Digital consumers and the law*. Alphen aan den Rijn: Kluwer Law International.

Hoffman, D. L., Novak, T. P., & Peralta, M. (1999). Building consumer trust online. *Communications of the ACM, 42*, 80–85.

IMCO (Committee on the Internal Market and Consumer Protection of the European Parliament) (2011). *Consumer behaviour in a digital environment. Study*. Available at http://www.europarl.europa.eu/committees/en/studiesdownload.html?languageDocument=EN&file=42591.

Information Commissioner's Office (2012). *Guidance on the rules on use of cookies and similar technologies*. v. 3. Available at http://www.ico.gov.uk/for_organisations/privacy_and_electronic_communications/the_guide/cookies.aspx (p. 1–30).

International Chamber of Commerce (2012). *ICC UK cookie guide*. Available at http://www.international-chamber.co.uk/components/com_wordpress/wp/wp-content/uploads/2012/04/icc_uk_cookie_guide.pdf (p. 1–15).

Jennings, M. (2012). To track or not to track: recent legislative proposals to protect consumer privacy. *Harvard Journal on Legislation, 49*, 193–206.

Jones, R., & Tahri, D. (2010). EU law requirements to provide information to website visitors. *Computer Law and Security Report, 26*, 613–620.

Kierkegaard, S. M. (2005). How the cookies (almost) crumbled: Privacy & lobbyism. *Computer Law and Security Report, 21*, 310–322.

Lee, D. (2012). *Cookies: Majority of government sites to miss deadline*. BBC. Available at http://www.bbc.com/news/technology-18090118.

Liao, C., Liu, C., & Chen, K. (2011). Examining the impact of privacy, trust and risk perceptions beyond monetary transactions: An integrated model. *Electronic Commerce Research and Applications, 10*, 702–715.

Luzak, J. (2013). Much ado about cookies: The European debate on the new provisions of the ePrivacy directive regarding cookies. *European Review of Private Law, 1*, 221–246.

Magat, W., Viscusi, W. K., & Huber, J. (1988). Consumer processing of hazard warning information. *Joural of Risk and Uncertainty, 1*, 201–232.

McDougall, S. (2011). *Cookie crumbles: confusion over data regulation*. Guardian 11. Available at http://www.guardian.co.uk/local-government-network/2011/aug/11/privacy-law-online-data-regulation.

Michelfelder, D. P. (2001). The moral value of informational privacy in cyberspace. *Ethics and Information Technology, 3*, 129–135.

Milne, G. R., & Culnan, M. J. (2004). Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices'. *Journal of Interactive Marketing, 18*, 15–29.

Miyazaki, A. D. (2008). Online privacy and the disclosure of cookie use: Effects on consumer trust and anticipated patronage. *Journal of Public Policy & Marketing, 27*, 19–33.

Morris, L. A., Mazis, M. B., & Brinberg, D. (1989). Risk disclosures in televised prescription drug advertising to consumers. *Journal of Public Policy & Marketing, 8*, 64–80.

Nowak, G. J., & Phelps, J. (1995). Direct marketing and the use of individual-level consumer information: Determining how and when "Privacy" matters. *Journal of Direct Marketing, 9*, 46–60.

Opinion 15/2011 on the definition of consent issued by Article 29 Data Protection Working Party, 13.07.2011, 01197/11/EN WP187. Available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf. (p. 9)

Opinion 2/2010 on online behavioural advertising issued by Article 29 Data Protection Working Party, 22.10.2010, 00909/10/EN WP171. Available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_en.pdf At 12.

OPTA (2012). *Veelgestelde vragen over de nieuwe cookieregels*. (pp. 1–5). Available at http://www.opta.nl/nl/actueel/alle-publicaties/publicatie/?id=3595.

Papakonstantinou, V., & De Hert, P. (2011). The amended EU Law on ePrivacy and Electronic Communications after its 2011 implementation; new rules on data protection, spam, data breaches and protection of intellectual property rights. *John Marshall Journal of Computer & Information Law, 29*, 29.

Park, Y. J., Campbell, S. W., & Kwak, N. (2012). Affect, cognition, and reward: Predictors of privacy protection online. *Computer in Human Behavior, 28*, 1019–1027.

Pechmann, C., & Stewart, D. W. (1988). Advertising repetition: A critical review of wearing and wearout. *Current Issues and Research in Advertising, 11*, 285. at 285–330.

Pollach, I. (2005). A typology of communicative strategies in online privacy policies: Ethics, power and informed consent. *Journal of Business Ethics, 62*, 221–235.

Schoenbachler, D. D., & Gordon, G. L. (2002). Trust and customer willingness to provide information in database-driven relationship marketing. *Journal of Interactive Marketing, 16*, 2–16.

Schwaig, K. S., Segars, A. H., Grover, V., & Fiedler, K. D. (2013). A model of consumers' perceptions of the invasion of information privacy. *Information & Management, 50*, 1–12.

Sefton-Green, R. (2005). Duties to inform versus party autonomy: Reversing the paradigm (from free consent to informed consent)?—A comparative account of French and English Law. In G. Howells, A. Janssen, & R. Schulze (Eds.), *Information rights and obligations* (pp. 171–173). Aldershot: Ashgate.

Turow, J., Hennessy, M., & Bleakley, A. (2008). Consumers' understanding of privacy rules in the marketplace. *The Journal of Consumer Affairs, 42*, 411–424.

Van Wel, L., & Royakkers, L. (2004). Ethical issues in web data mining. *Ethics and Information Technology, 6*, 129–140.

Williams, I. (2013). *Blog: ICO joins global sweep to improve website privacy policies*. http://ico.org.uk/news/blog/2013/ico-joins-global-sweep-to-improve-website-privacy-policies.

Wirtz, J., Lwin, M. O., & Williams, J. D. (2007). Causes and consequences of consumer online privacy concern. *International Journal of Service Industry Management, 18*, 326–341.

Yaveroglu, I., & Donthu, N. (2008). Advertising repetition and placement issues in on-line environments. *Journal of Advertising, 37*, 31–43.