

Luzak, J. A.

Conference 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 user's right to online privacy

24th European Regional Conference of the International Telecommunications Society (ITS): "Technology, Investment and Uncertainty", Florence, Italy, 20th-23rd October, 2013

Provided in Cooperation with:

International Telecommunications Society (ITS)

Suggested Citation: Luzak, J. A. (2013) : 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 user's right to online privacy, 24th European Regional Conference of the International Telecommunications Society (ITS): "Technology, Investment and Uncertainty", Florence, Italy, 20th-23rd October, 2013, International Telecommunications Society (ITS), Calgary

This Version is available at:

<https://hdl.handle.net/10419/88468>

Standard-Nutzungsbedingungen:

Die Dokumente auf EconStor dürfen zu eigenen wissenschaftlichen Zwecken und zum Privatgebrauch gespeichert und kopiert werden.

Sie dürfen die Dokumente nicht für öffentliche oder kommerzielle Zwecke vervielfältigen, öffentlich ausstellen, öffentlich zugänglich machen, vertreiben oder anderweitig nutzen.

Sofern die Verfasser die Dokumente unter Open-Content-Lizenzen (insbesondere CC-Lizenzen) zur Verfügung gestellt haben sollten, gelten abweichend von diesen Nutzungsbedingungen die in der dort genannten Lizenz gewährten Nutzungsrechte.

Terms of use:

Documents in EconStor may be saved and copied for your personal and scholarly purposes.

You are not to copy documents for public or commercial purposes, to exhibit the documents publicly, to make them publicly available on the internet, or to distribute or otherwise use the documents in public.

If the documents have been made available under an Open Content Licence (especially Creative Commons Licences), you may exercise further usage rights as specified in the indicated licence.

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 user’s right to online privacy

1. Introduction

The basic objection to such practices as the cookies’ use² 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.³ 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.⁴ Internet users not only do not know what cookies are, but usually are also not informed or not clearly informed that cookies are set on their computers or for what purposes the information gathered through the cookies’ use is processed.⁵ 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.⁶ This paper argues for the European guidelines’ introduction that would specify the design, content and form of the privacy notice 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.⁷ Following the old adage ‘if you can’t beat them join them’, the increased transparency about the cookies’ use should enable better consumer choices as far as data protection is concerned.

¹ Assistant Professor at the Centre for the Study of European Contract Law, University of Amsterdam.

² ‘Cookies’ are small text files that are set on an internet user’s computer when he browses the internet. Due to these cookies the webpages that internet users visit as well as other data on internet users may be tracked and stored. See more on this, e.g.: A.D. MIYAZAKI, ‘Online Privacy and the Disclosure of Cookie Use: Effects on Consumer Trust and Anticipated Patronage’, *JPP&M (Journal of Public Policy & Marketing)* 27 (2008): 19, at 20-21; D. CHARTERS, ‘Electronic Monitoring and Privacy Issues in Business-Marketing: The Ethics of the DoubleClick Experience’, *Journal of Business Ethics* 35 (2002): 243, at 245.

³ I. POLLACH, ‘A Typology of Communicative Strategies in Online Privacy Policies: Ethics, Power and Informed Consent’, *Journal of Business Ethics* 62 (2005): 221, at 225; D. CHARTERS (n. 2), pp. 248-250; D.P. MICHELFELDER, ‘The moral value of informational privacy in cyberspace’, *Ethics and Information Technology* 3 (2001): 129, at 135; J. LUZAK, ‘Much Ado about Cookies: The European Debate on the New Provisions of the ePrivacy Directive regarding Cookies’, *European Review of Private Law* 1 (2013), pp. 225-227.

⁴ A.D. MIYAZAKI (n. 2), p. 21.

⁵ I. POLLACH (n. 3), p. 222; D. CHARTERS (n. 2), p. 245; S.M. KIERKEGAARD, ‘How the cookies (almost) crumbled: Privacy & lobbyism’, *CLSR (Computer Law and Security Report)* 21 (2005): 310, at 317.

⁶ Y.J. PARK, S.W. CAMPBELL, N. KWAK, ‘Affect, cognition, and reward: Predictors of privacy protection online’, *Computer in Human Behavior* 28 (2012), pp. 1024-1025.

⁷ M. JENNINGS, ‘To Track or Not To Track: Recent Legislative Proposals To Protect Consumer Privacy’, *Harvard Journal on Legislation* 49 (2012), pp. 193-194.

In order to ensure the protection of the right to online privacy, the new Article 5(3) ePrivacy Directive⁸ states that internet users should receive ‘*clear and comprehensive information*’ about the fact that their data may be accessed, stored and processed online. 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.⁹ If the privacy notice was standardised 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.¹⁰ 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.¹¹

Therefore, this paper’s normative aim is to develop guidelines for future regulation of European privacy notices. The following two sections show that a lack of European guidelines leads to divergent interpretation and implementation of information requirements regarding the cookies’ use in 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.¹² This paper presents divergent implementation measures on an example of first English and then Dutch law. The UK’s Information Commissioner’s Office (the “ICO”) recently issued very specific guidelines¹³ on how to formulate privacy notices, which allow for an interesting comparison with more general Dutch guidelines. Fourth section

⁸ 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. For a detailed description of the ePrivacy Directive’s history see: V. PAPAKONSTANTINOUS, P. DE HERT, ‘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 (2011), p.29.

⁹ J. LUZAK, (n. 3), pp. 229-231.

¹⁰ See further on this in section 4 of this paper.

¹¹ 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, see: D.L. HOFFMAN, T.P. NOVAK, M. PERALTA, ‘Building Consumer Trust Online’, *CACM (Communications of the ACM)* 42 (1999): 80, at 82; Y.J. PARK et al. (n. 6), pp. 1024-1025.

¹² IMCO (Committee on the Internal Market and Consumer Protection of the European Parliament), ‘Consumer behaviour in a digital environment. Study.’, August 2011, << [¹³ A few guidelines have been issued by the ICO, the most recent one \(of May 2012\) will be referred to here: Information Commissioner’s Office, ‘Guidance on the rules on use of cookies and similar technologies’, v. 3, May 2012, << \[2\]\(http://www.ico.gov.uk/for_organisations/privacy_and_electronic_communications/the_guide/cookies.aspx>>”, p. 1-30.</p></div><div data-bbox=\)](http://www.europarl.europa.eu/committees/en/studiesdownload.html?languageDocument=EN&file=42591>>”, pp. 14, 16, 77, 102.</p></div><div data-bbox=)

of this paper introduces consumer behaviour research findings in order to identify what sort of information and its method of conveying could be perceived as clear and comprehensive by internet users. Additionally, it explores the link between an increased exposure to the same information and the consumers' learning process. In the final section, general findings from this paper are compiled in order to draft an example of what European guidelines at one point could look like.

2. 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 2011.¹⁴ 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.¹⁵ The report showed that most British internet users have limited understanding of cookies and the way they work.¹⁶ This might have led the British authorities to decide to focus their implementation efforts on increasing knowledge about and of cookies among internet users. 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.¹⁷ 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.¹⁸ 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. Alongside the ICO, also the International Chamber of Commerce (the "ICC") issued a cookie guide. While the ICO points out 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. Namely, the ICC guide contains specific standard notices' wording that could be directly transcribed by the marketers into their privacy notices.¹⁹ It is seen that if the marketers use the same notice to

¹⁴ ICO (n. 13), p. 2.

¹⁵ Department for Culture, Media and Sport (the "DCMS"), 'Research into consumer understanding and management of internet cookies and the potential impact of the EU Electronic Communications Framework', April 2011, <<http://www.culture.gov.uk/images/consultations/PwC_Internet_Cookies_final.pdf>>, p. 1-91.

¹⁶ ICO (n. 13), p. 3. See also: S. FURNELL & A. PHIPPEN, 'Online privacy: a matter of policy?', *Computer Fraud & Society* August 2012, pp. 12-18.

¹⁷ ICO (n. 13), p. 3; R. BOND, 'The EU e-Privacy Directive and Consent to Cookies', *Business Lawyer* 68 (2012), p. 215.

¹⁸ ICO (n. 13), p. 8.

¹⁹ International Chamber of Commerce, 'ICC UK Cookie Guide', April 2012, <<http://www.international-chamber.co.uk/components/com_wordpress/wp/wp-content/uploads/2012/04/icc_uk_cookie_guide.pdf>>, p. 1-15.

explain to internet users what cookies are and how they are used, this should facilitate better understanding and easier learning by internet users.²⁰

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.²¹ In this respect, the ICO notices that internet users are more likely to read the information if it is a website’s integral part and when it fits in the website’s design.²² 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’. 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.²³ 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., he 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.²⁴ 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 that would attract their attention and convey information in a contextual way.²⁵ 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.²⁶

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

²⁰ ICC (n. 19), pp. 2-3; R. BOND (n. 17), p. 215.

²¹ ICO (n. 13), p. 18.

²² ICO (n. 13), p. 8.

²³ ICO (n. 13), p. 18.

²⁴ ICO (n. 13), p. 23.

²⁵ ICC (n. 19), p. 5. Again, a picture of a cookies comes to mind as an attractive icon.

²⁶ ICC (n. 19), pp. 3-4.

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.²⁷ Taking into account the findings that most internet users nowadays are unaware of the cookies' existence and significance, the marketers can be expected to have to provide a more detailed explanation on how cookies work and what categories of cookies are used on a given website.²⁸ In this respect, the information would more likely be considered as 'comprehensive' if it explained what different cookies are used for, instead of just listing them all.²⁹ 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.³⁰ 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.³¹ 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.³²

Finally, the information would only then be clear and comprehensive to internet users if upon reading it, they understand it.³³ 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.³⁴ Highly technical language explaining how the website works would likely not be understood by most internet users. The ICC guide provides the marketers with standard notices' wording that could be given to internet users in order to harmonise the language used by the marketers. Since cookies fulfil various functions and, therefore, the data's amount and sort that they gather differs 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.³⁵

3. Dutch guidelines

The Dutch authority responsible for enforcing the new rules, the *Onafhankelijke Post en Telecommunicatie Autoriteit* (the "OPTA"), also issued its guidelines on how to comply with

²⁷ ICO (n. 13), p. 8, 17, 22.

²⁸ ICC (n. 19), pp. 3-4; R. BOND (n. 17), p. 215.

²⁹ ICO (n. 13), p. 17.

³⁰ ICO (n. 13), p. 21.

³¹ ICO (n. 13), p. 22-23.

³² ICO (n. 13), p. 25.

³³ ICO (n. 13), p. 17.

³⁴ ICO (n. 13), p. 8.

³⁵ ICC (n. 19), pp. 7-9. See also: R. BOND (n. 17), p. 215.

the new legislation.³⁶ 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 standardising 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.³⁷

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.³⁸

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. It is likely that British companies would either use one of the standard text notices provided by the ICC to inform internet users on the cookies' use, or draft a different text, following closely the ICO's guidelines. This may contribute to the privacy notices' standardisation in the UK. On the other hand, the Dutch marketers have not received any specific instructions 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 would also contribute to the lack of clarity in cross-border transactions.

4. Consumer behaviour findings

It has been argued in the legal literature that consumer's consent should only be seen as such when it was an informed consent.³⁹ Internet users may only then be seen as having given

³⁶ OPTA, 'Veelgestelde vragen over de nieuwe cookieregels', 7.06.2012, pp. 1-5, <<
<http://www.opta.nl/nl/actueel/alle-publicaties/publicatie/?id=3595>>>.

³⁷ OPTA (n. 36), p. 3.

³⁸ OPTA (n. 36), p. 3.

³⁹ See on informed consent: R. SEFTON-GREEN, 'Duties to Inform versus Party Autonomy: Reversing the Paradigm (from Free Consent to Informed Consent)? – A Comparative Account of French and English Law', in *Information Rights and Obligations*, eds G. HOWELLS, A. JANSSEN, R. SCHULZE (Aldershot: Ashgate, 2005), at 171-173; P. GOZZO, 'The Strategy and the Harmonization Process within the European Legal System: Party Autonomy and Information Requirements', in *Information Rights and Obligations*, eds G. HOWELLS, A. JANSSEN, R. SCHULZE (Aldershot: Ashgate, 2005), at 22-30. See also: Opinion 2/2010 on online behavioural advertising issued by Article 29 Data Protection Working Party, 22.10.2010, 00909/10/EN WP171, <<
http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_en.pdf>>, at 12; Opinion 15/2011 on the

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.

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.⁴⁰ However, studies showed that this will only hold true upon fulfilment of three conditions. Firstly, a privacy notice needs to be read by internet users. 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.⁴¹

Internet users need to be enticed to read privacy notices. A study showed that internet users often do not read privacy notices since they are too long, too boring, hard to understand and often the same.⁴² Across the European Union, 41% of internet users admits to not reading privacy notices on websites.⁴³ Internet users are more likely to read privacy notices when they perceive them as understandable.⁴⁴ Attractiveness of the privacy notice's display, e.g., giving it a prominent place on a website, may also contribute to its clarity and increase the internet users' chances of actually reading it.⁴⁵ Moreover, 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 the text should be concise in order to be comprehensive.⁴⁶ For clarity's sake, it may 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

definition of consent issued by Article 29 Data Protection Working Party, 13.07.2011, 01197/11/EN WP187, <<http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf>>, p. 9.

⁴⁰ G.R. MILNE & M.J. CULNAN, 'Strategies for reducing online privacy risks: why consumers read (or don't read) online privacy notices', *JIM* 18 (2004): 15, pp. 16, 24; J. WIRTZ, M.O. LWIN, J.D. WILLIAMS, 'Causes and consequences of consumer online privacy concern', *International Journal of Service Industry Management* 18 (2007), p. 341; C. LIAO, C. LIU, K. CHEN, 'Examining the impact of privacy, trust and risk perceptions beyond monetary transactions: An integrated model', *Electronic Commerce Research and Applications* 10 (2011), p. 712; K.S. SCHWAIG, A.H. SEGARS, V. GROVER, K.D. FIEDLER, 'A model of consumers' perceptions of the invasion of information privacy', *Information & Management* 50 (2013), p. 9.

⁴¹ G.R. MILNE & M.J. CULNAN (n. 40), p. 16.

⁴² G.R. MILNE & M.J. CULNAN (n. 40), p. 23. One of the surveyed consumers asked: "How about the 'Privacy Notice for Dummies' version?"

⁴³ IMCO (n. 12), p. 80-81. Similar data comes from the US research, see, e.g.: J.B. EARP & D. BAUMER, 'Innovative Web Use To Learn About Consumer Behavior And Online Privacy', *Communications of the ACM* 46 (2003), pp. 81-83. Other research shows that at least 60% of British primary and secondary school respondents do not read privacy policies: S. FURNELL & A. PHIPPEN (n. 16), p. 15.

⁴⁴ G.R. MILNE & M.J. CULNAN (n. 40), p. 24. The following paragraphs discuss how to make the content of privacy notices more understandable to internet users.

⁴⁵ G.R. MILNE & M.J. CULNAN (n. 40), p. 17, 19, 25; S. HARRIDGE-MARCH, 'Can the building of trust overcome consumer perceived risk online?', *Marketing Intelligence & Planning* 24 (2006): 746, at 754-755; J. WIRTZ et al. (n. 40), p. 341.

⁴⁶ G.R. MILNE & M.J. CULNAN (n. 40), p. 23.

itself.⁴⁷ 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.⁴⁸

As far as the privacy notice's content is concerned, the most important factor 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.⁴⁹ The marketers should be truthful in their disclosure.⁵⁰ 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.⁵¹ Other studies pointed out that if consumers feel that a message is personally relevant to them, they would be more likely to read it.⁵² 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.⁵³ Since the information's comprehensiveness depends to 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.⁵⁴ 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.⁵⁵

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.⁵⁶ American researchers found that in order to understand 80% of the examined privacy notices more than a college degree was necessary.⁵⁷ Recent British survey tested privacy notices of various popular social websites, e.g., Facebook, Twitter, LinkedIn, Club Penguin, and evaluated their

⁴⁷ R. JONES & D. TAHRI, 'EU law requirements to provide information to website visitors', *CLSR* 26 (2010): 613, at 620.

⁴⁸ L. VAN WEL & L. ROYAKKERS, 'Ethical issues in web data mining', *Ethics and Information Technology* 6 (2004): 129, at 134.

⁴⁹ G.J. NOWAK & J. PHELPS, 'Direct Marketing and the Use of Individual-Level Consumer Information: Determining how and When "Privacy" Matters', *JDM (Journal of Direct Marketing)* 9 (1995): 46, at 57; S. HARRIDGE-MARCH (n. 45), p. 752; D.P. MICHELFELDER (n. 3), p. 132; R. JONES & D. TAHRI (n. 47), p. 619.

⁵⁰ S. HARRIDGE-MARCH (n. 45), p. 756.

⁵¹ G.R. MILNE & M.J. CULNAN (n. 40), p. 18; T. DINEV & P. HART, 'An Extended Privacy Calculus Model for E-Commerce Transactions', *Information Systems Research* 17 (2006), pp. 73-74.

⁵² G.R. MILNE & M.J. CULNAN (n. 40), p. 18.

⁵³ J. TUROW, M. HENNESSY, A. BLEAKLEY, 'Consumers' Understanding of Privacy Rules in the Marketplace', *The Journal of Consumer Affairs* 42 (2008), p. 422.

⁵⁴ G.R. MILNE & M.J. CULNAN (n. 40), p. 19; G.J. NOWAK & J. PHELPS (n. 49), p. 57.

⁵⁵ L. VAN WEL & L. ROYAKKERS (n. 48), p. 134.

⁵⁶ I. POLLACH (n. 3), p. 223, 228.

⁵⁷ I. POLLACH (n. 3), p. 223.

text as at least ‘difficult’ if not ‘confusing’.⁵⁸ The British researchers estimated also that these privacy notices could not be understood by people with a reading age of under 16, while it has been suggested that about half the working adults in the United Kingdom have a reading age of 11 or lower.⁵⁹ 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.⁶⁰ 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. 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.⁶¹ 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’.⁶² 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 is used. The legal jargon should be avoided as much as possible; preferably layman terms should be used.⁶³

The consumer behaviour studies point to valid reasons why the information given to internet users on the cookies’ use should be harmonised across Europe. Firstly, it is likely that if internet users are exposed to the same information time and over again, they would learn to recognize it easier, start paying more attention to it, as well as know better what they should expect from it.⁶⁴ This could facilitate internet users’ education 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.⁶⁵ Again, when the marketers wanted consumers to focus on a specific information statement and, therefore, increased their exposure thereto, this caused consumers

⁵⁸ Pursuant to the Flesch Reading Easel standards, see: S. FURNELL & A. PHIPPEN (n. 16), pp. 14-15.

⁵⁹ Pursuant to the Flesch Kincaid Grade Level standards, see: S. FURNELL & A. PHIPPEN (n. 16), pp. 14-15.

⁶⁰ I. POLLACH (n. 3), p. 228.

⁶¹ G.R. MILNE & M.J. CULNAN (n. 40), p. 19; S. HARRIDGE-MARCH (n. 45), p. 756; D.D. SCHOENBACHLER & G.L. GORDON, ‘Trust And Customer Willingness to Provide Information in Database-Driven Relationship Marketing’, *Journal of Interactive Marketing* 16 (2002), p. 14.

⁶² I. POLLACH (n. 3), p. 228, 230; L. VAN WEL & L. ROYAKKERS (n. 48), p. 134; E.M. CAUDILL & P.E. MURPHY, ‘Consumer Online Privacy: Legal and Ethical Issues’, *JPP&M* 19 (2000): 7, at 13.

⁶³ E.M. CAUDILL & P.E. MURPHY(n. 62), p. 16; J. WIRTZ et al. (n. 40), p. 341.

⁶⁴ This strategy tends to be successful in making consumers pay attention to advertisements: C. PECHMANN & D.W. STEWART, ‘Advertising Repetition: A Critical Review of Wearing and Wearout’, *Current Issues and Research in Advertising* 11 (1988): 285, at 285-330. On the other hand, some researchers claimed that repeat exposure to the same information could desensitize consumers, e.g.: W. MAGAT, W.K. VISCUSI, J. HUBER, ‘Consumer Processing of Hazard Warning Information’, *Journal of Risk and Uncertainty* 1 (1988), pp. 201-232.

⁶⁵ L.A. MORRIS, M.B. MAZIS, D. BRINBERG, ‘Risk Disclosures in Televised Prescription Drug Advertising to Consumers’, *JPP&M* 8 (1989): 64, at 64-80.

to indeed be more likely to start paying attention to this information.⁶⁶ 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.⁶⁷ 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 risks⁶⁸.

5. European guidelines

This paper's previous sections 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.⁶⁹ 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 harmonise 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. 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.⁷⁰ 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 standardised.

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.⁷¹ 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.⁷² 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. Based on the presented consumer behaviour studies, the European

⁶⁶ K. FRIEDMANN, 'The Effect of Adding Symbols to Written Warning Labels on User Behavior and Recall', *Human Factors* 30 (1988): 507, at 507-515.

⁶⁷ Y.J. PARK et al. (n. 6), pp. 1024-1025.

⁶⁸ J. TUROW et al. (n. 53), pp. 412, 420-422.

⁶⁹ This is true not only in Europe, but also in the United States, see: M.J. CULNAN, 'Protecting Privacy Online: Is Self-Regulation Working?', *JPP&M* 19 (2000): 20, at 24.

⁷⁰ Maintaining consumer trust has been mentioned as one of the crucial elements of online market's further development, see e.g.: M. JENNINGS (n. 7), pp. 197.

⁷¹ Opinion 2/2010 (n. 39), p. 18.

⁷² Opinion 2/2010 (n. 39), p. 18.

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 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. 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 harmonised 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. As a result, European internet users would get their ‘privacy notice for dummies’ which should facilitate a widespread understanding of what cookies are and how they operate.

BIBLIOGRAPHY

- R. BOND, 'The EU e-Privacy Directive and Consent to Cookies', *Business Lawyer* 68 (2012), p. 215.
- E.M. CAUDILL & P.E. MURPHY, 'Consumer Online Privacy: Legal and Ethical Issues', *Journal of Public Policy & Marketing* 19 (2000), pp. 7-19.
- D. CHARTERS, 'Electronic Monitoring and Privacy Issues in Business-Marketing: The Ethics of the DoubleClick Experience', *Journal of Business Ethics* 35 (2002), pp. 243-254.
- M.J. CULNAN, 'Protecting Privacy Online: Is Self-Regulation Working?', *Journal of Public Policy & Marketing* 19 (2000), pp. 20-26.
- Department for Culture, Media and Sport (the "DCMS"), 'Research into consumer understanding and management of internet cookies and the potential impact of the EU Electronic Communications Framework', April 2011, <<http://www.culture.gov.uk/images/consultations/PwC_Internet_Cookies_final.pdf>>, p. 1-91.
- T. DINEV & P. HART, 'An Extended Privacy Calculus Model for E-Commerce Transactions', *Information Systems Research* 17 (2006), pp. 61-80.
- J.B. EARP & D. BAUMER, 'Innovative Web Use To Learn About Consumer Behavior And Online Privacy', *Communications of the ACM* 46 (2003), pp. 81-83.
- K. FRIEDMANN, 'The Effect of Adding Symbols to Written Warning Labels on User Behavior and Recall', *Human Factors* 30 (1988), pp. 507-515.
- S. FURNELL & A. PHIPPEN, 'Online privacy: a matter of policy?', *Computer Fraud & Society* August 2012, pp. 12-18.
- P. GOZZO, 'The Strategy and the Harmonization Process within the European Legal System: Party Autonomy and Information Requirements', in *Information Rights and Obligations*, eds G. HOWELLS, A. JANSSEN, R. SCHULZE (Aldershot: Ashgate, 2005), pp. 22-30.
- S. HARRIDGE-MARCH, 'Can the building of trust overcome consumer perceived risk online?', *Marketing Intelligence & Planning* 24 (2006), pp. 746-761.
- D.L. HOFFMAN, T.P. NOVAK, M. PERALTA, 'Building Consumer Trust Online', *Communications of the ACM* 42 (1999), pp. 80-85.
- IMCO (Committee on the Internal Market and Consumer Protection of the European Parliament), 'Consumer behaviour in a digital environment. Study.', August 2011, <<<http://www.europarl.europa.eu/committees/en/studiesdownload.html?languageDocument=EN&file=42591>>>.
- Information Commissioner's Office, 'Guidance on the rules on use of cookies and similar technologies', v. 3, May 2012, <<http://www.ico.gov.uk/for_organisations/privacy_and_electronic_communications/the_guide/cookies.aspx>>, p. 1-30.

International Chamber of Commerce, 'ICC UK Cookie Guide', April 2012, <<http://www.international-chamber.co.uk/components/com_wordpress/wp/wp-content/uploads/2012/04/icc_uk_cookie_guide.pdf>>, p. 1-15.

M. JENNINGS, 'To Track or Not To Track: Recent Legislative Proposals To Protect Consumer Privacy', *Harvard Journal on Legislation* 49 (2012), pp. 193-206.

R. JONES & D. TAHRI, 'EU law requirements to provide information to website visitors', *Computer Law and Security Report* 26 (2010), pp. 613-620.

S.M. KIERKEGAARD, 'How the *cookies* (almost) crumbled: Privacy & lobbying', *Computer Law and Security Report* 21 (2005), pp. 310-322.

C. LIAO, C. LIU, K. CHEN, 'Examining the impact of privacy, trust and risk perceptions beyond monetary transactions: An integrated model', *Electronic Commerce Research and Applications* 10 (2011), pp. 702-715.

J. LUZAK, 'Much Ado about Cookies: The European Debate on the New Provisions of the ePrivacy Directive regarding Cookies', *European Review of Private Law* 1 (2013), pp. 221-246.

W. MAGAT, W.K. VISCUSI, J. HUBER, 'Consumer Processing of Hazard Warning Information', *Journal of Risk and Uncertainty* 1 (1988), pp. 201-232.

D.P. MICHELFELDER, 'The moral value of informational privacy in cyberspace', *Ethics and Information Technology* 3 (2001), pp. 129-135.

G.R. MILNE & M.J. CULNAN, 'Strategies for reducing online privacy risks: why consumers read (or don't read) online privacy notices', *Journal of Interactive Marketing* 18 (2004), pp. 15-29.

A.D. MIYAZAKI, 'Online Privacy and the Disclosure of Cookie Use: Effects on Consumer Trust and Anticipated Patronage', *Journal of Public Policy & Marketing* 27 (2008), pp. 19-33.

L.A. MORRIS, M.B. MAZIS, D. BRINBERG, 'Risk Disclosures in Televised Prescription Drug Advertising to Consumers', *Journal of Public Policy & Marketing* 8 (1989), pp. 64-80.

G.J. NOWAK & J. PHELPS, 'Direct Marketing and the Use of Individual-Level Consumer Information: Determining how and When "Privacy" Matters', *Journal of Direct Marketing* 9 (1995), pp. 46-60.

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

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

OPTA, 'Veelgestelde vragen over de nieuwe cookieregels', 7.06.2012, pp. 1-5, <<<http://www.opta.nl/nl/actueel/alle-publicaties/publicatie/?id=3595>>>.

V. PAPAKONSTANTINO, P. DE HERT, '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 (2011), p.29-.

Y.J. PARK, S.W. CAMPBELL, N. KWAK, 'Affect, cognition, and reward: Predictors of privacy protection online', *Computer in Human Behavior* 28 (2012), pp. 1019-1027.

C. PECHMANN & D.W. STEWART, 'Advertising Repetition: A Critical Review of Wearing and Wearout', *Current Issues and Research in Advertising* 11 (1988): 285, at 285-330.

I. POLLACH, 'A Typology of Communicative Strategies in Online Privacy Policies: Ethics, Power and Informed Consent', *Journal of Business Ethics* 62 (2005), pp. 221-235.

D.D. SCHOENBACHLER & G.L. GORDON, 'Trust And Customer Willingness to Provide Information in Database-Driven Relationship Marketing', *Journal of Interactive Marketing* 16 (2002), pp. 2-16.

K.S. SCHWAIG, A.H. SEGARS, V. GROVER, K.D. FIEDLER, 'A model of consumers' perceptions of the invasion of information privacy', *Information & Management* 50 (2013), pp. 1-12.

R. SEFTON-GREEN, 'Duties to Inform versus Party Autonomy: Reversing the Paradigm (from Free Consent to Informed Consent)? – A Comparative Account of French and English Law', in *Information Rights and Obligations*, eds G. HOWELLS, A. JANSSEN, R. SCHULZE (Aldershot: Ashgate, 2005), pp. 171-173.

J. TUROW, M. HENNESSY, A. BLEAKLEY, 'Consumers' Understanding of Privacy Rules in the Marketplace', *The Journal of Consumer Affairs* 42 (2008), pp. 411-424.

L. VAN WEL & L. ROYAKKERS, 'Ethical issues in web data mining', *Ethics and Information Technology* 6 (2004), pp. 129-140.

J. WIRTZ, M.O. LWIN, J.D. WILLIAMS, 'Causes and consequences of consumer online privacy concern', *International Journal of Service Industry Management* 18 (2007), pp. 326-341.