

A Legal-Psychological Approach to Understanding Online Attitudes and Behaviours

Eoin Carolan

M. Rosario Castillo-Mayén

eoin.carolan@ucd.ie, rosario.castillomayen@ucd.ie
University College Dublin (Ireland)

Doi:10.5901/mjss.2013.v4n10p473

Abstract

This paper seeks to combine insights from two distinct disciplinary fields, Law and Psychology, in order to develop an integrated understanding of the relationship between attitudes to, and the regulation of, online technologies. Specifically, this paper focuses on concerns about the right to privacy that are raised because of the development of new technologies. One of the legal responses to this concern has been a new EU Directive on Privacy and Electronic Communication, which requires, amongst other measures, that websites obtain the informed consent of users to the use of tracking devices ('cookies'). This study seeks to test how the application of Law, and in particular of this Directive, is affecting individuals' attitudes and behaviour when online. Given that both the manner of website compliance with the Directive and the efficacy of the measures introduced have been questioned, an empirical approach of the effectiveness of these measures seems necessary. With this purpose, university students were invited to participate in an online experiment, which was conducted to evaluate the impact of different approaches to compliance with the new Directive on users' online attitudes and behaviours. The effect of making users more aware of warnings about cookies' use was also tested. Results allow for an inter-disciplinary analysis of the types of measure which may be more effective in protecting individuals' right to privacy when online.

1. Introduction

This study was conducted as part of a larger research project which seeks to investigate the relationship between legal regulation of online technologies and the way in which those technologies are used by individuals. The project is funded by the Irish Research Council for Humanities and Social Sciences.

The specific focus of this study was the recently introduced European Union Directive 2009/136/EC on universal service and users' rights relating to electronic communications networks and services. More commonly known as the 'Cookies Directive', this measure was intended to provide an enhanced level of legal protection for users of online technologies.

In particular, the Directive aimed to improve respect for the privacy of users by obliging technology providers to obtain consent from the user before storing the users' information, or gaining access to information already stored.

There are a number of reasons why the Directive provided a suitable subject for this type of study. One of the challenges with research of this sort is determining the relationship between legal regulation and the attitudes or actions of users. The fact that the Directive was recently introduced provided an opportunity to assess whether the changes to the law may have had any discernible impact on users. This was particularly so given that the Directive required changes to be introduced to a pre-existing approach to data collection with which most users may have been (even unwittingly) familiar.

More generally, the Directive is also suitable subject for psycho-legal research because of the importance it attaches to the concept of informed consent. It requires technology providers to obtain consent after having provided clear and comprehensive information. This emphasis on informed consent reflects a conception of privacy as a means of facilitating the autonomous actions of individuals (Carolan & Delany, 2008; Rossler, 2004). However, this raises questions concerning what constitutes informed consent, what type of information is necessary to enable consent to be truly informed and, more generally, whether the law is capable of securing a situation in which users can be said to have provided informed consent to all consequences of their actions.

2. Cookies and the Cookies Directive

A cookie is a small data file which is stored on the computer of the individual user. Cookies take a variety of forms and

can be used for a variety of purposes.

Some, such as authentication or analytics cookies, assist in the operation of an individual website. An authentication cookie might, for example, allow a website to verify a user's account or to recognise and remember a returning user. An analytic cookie may allow the operator of a website to identify patterns in user behaviour and optimise the design or layout of the site as a result.

Others, however, are designed to facilitate behavioural advertising by collating information on an individual's internet use with a view to allowing for more targeted advertising based on the user's browsing habits.

These cookies may be operated by the site that a user is visiting at the time ('first party') or may be operated by a third party. Third party cookies are frequently 'persistent cookies' rather than 'session cookies' in that they do not expire when a person leaves one website but rather track the user across multiple websites.

This latter category of third party persistent cookies are most commonly used for advertising purposes. They are also the form of cookie that tends to give rise to the greatest privacy concerns. The ability to monitor and record user behaviour is one which could potentially imperil the privacy of the user, whether by disclosing private information to a third party or, more generally, by allowing the construction of a comprehensive profile of that person without their knowledge or consent.

These privacy concerns led to the introduction of a Directive in 2002 to regulate the use of cookies. The Directive accepted that cookies, along with other tracking technologies, could have legitimate purposes but articulated a concern that the use of such devices "without [users] knowledge in order to gain access to information, to store hidden information or to trace the activities of the user ... may seriously intrude upon the privacy of ... users". (Recital 24). The solution was to allow the "use of such devices ... only for legitimate purposes, with the knowledge of the users concerned". Specifically, Article 5 of the Directive obliged operators to inform individuals about the use of tracking technologies and to offer them the ability to opt-out.

The 2009 Directive sought to further protect the privacy of users by replacing this opt-out system with an opt-in one. Article 5 (3) now provides that:

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

This more rigorous regime was justified on the basis that, while information might be stored for some valid purposes, it could also be used for other purposes involving "unwarranted intrusion into the private sphere". The Directive thus proclaimed that

It is therefore of paramount importance that users be provided with clear and comprehensive information when engaging in any activity which could result in such storage or gaining of access. The methods of providing information and offering the right to refuse should be as user-friendly as possible. (Recital 66).

2.1 Information and consent: what do these concepts mean under the Directive?

It is clear from the reference to user-friendliness that the Directive is intended to facilitate the effective and informed exercise by an individual of their entitlement to decide whether or not to opt-in to the technology in question.

However, this concern with user-friendliness also speaks to one of the difficulties with a legal approach to technology regulation which is premised on consent, namely whether it is realistic to expect that individuals engaged in casual activities can be given sufficiently comprehensive or detailed information in the course of those activities to enable them to provide truly informed consent. In addition, psychological studies have indicated that "the relationship between consumers' privacy concerns and actual behaviour is neither straightforward nor has any link been established incontrovertibly" (Joinson, Reips, Buchanan, & Paine-Schofield, 2010, p. 3). Furthermore, research has suggested that online privacy concerns may be influenced by multiple factors including trust, risk taking, self-efficacy, personality factors, and so on (e.g., Fogel & Nehmad, 2009; Joinson et al., 2010; Junglas, Johnson, & Spitzmüller, 2008; Yao, Rice, & Wallis, 2007). Therefore, it seems essential to also consider psychological research in order to test the effective application of legal regulations.

The question of the ability of users' to use information provided to make informed choices is particularly important because of the lack of detail provided in the Directive about methods of compliance. Article 5, as set out above, simply requires that consent be obtained following the provision of clear and comprehensive information. The Directive provides little, if any, clarity as to what constitutes 'clear and comprehensive' information or when consent will be found. This has

led to substantial differences in methods of implementation both across Member States (Rittweger, Krone and Wendler, 2011) and individual websites. It is unknown whether these different methods have a different impact on individuals' online interaction. For that reason, this study aimed to compare the effect of different methods of implementation on users' attitudes and behaviours.

Some additional guidance was provided by the publication by the Article 29 Working Party in 2011 of an Opinion on consent. The Working Party comprises representatives of national and EU data protection authorities and, although independent, has an advisory role under European legislation. In its report, it expressed the view that consent to the processing of personal data will be valid were it is freely given, specific and fully informed. Consent must also be sought in advance of any processing. Furthermore:

The need for consent to be 'informed' translates into two additional requirements. First, the way in which the information is given must ensure the use of appropriate language so that data subjects understand what they are consenting to and for what purposes. This is contextual. The use of overly complicated legal or technical jargon would not meet the requirements of the law. Second, the information provided to users should be clear and sufficiently conspicuous so that users cannot overlook it. The information must be provided directly to individuals. It is not enough for it to be merely available somewhere.

Taken cumulatively, this suggests that the new Cookies Directive assumes that (i) requiring the provision of consent permits persons to engage in privacy-protective behaviour; (ii) the clarity and saliency of information has a positive impact on the ability of persons to engage in privacy-protective behaviour; and (iii) requiring the provision of information and obtaining of consent in advance will have a positive impact on the possibility of persons exercising greater control over the disclosure of information. These assumptions are, in part, tested in this study.

However, as stated before, the methods used by websites to inform internet users about their use of cookies do not always seem to meet with the Directive's requirement of informed consent. In fact, in a general review of multiple websites, the most common approach to the provision of information about their use of cookies was to include a general warning when the site is visited. Some other sites did not even include such. Moreover, it was difficult to identify websites which both clearly inform individuals about their use of cookies and then enable them to make an informed and autonomous choice about whether or not to permit access to their information. Even websites which informed about their cookie policy typically provided users with a binary choice between acceptance of the policy or non-use of the site.

The aim of the study was to preliminarily investigate to what extent if any, three different methods of implementation of the Cookies Directive affect users' online interaction. From a legal perspective, the primary objective of the study was to examine the efficacy of the rules introduced by the Directive in encouraging persons to exercise greater individual control over the disclosure of potentially private information. From a psychological perspective, the primary objective of the study was to examine the effects of the EU's so-called Cookies Directive on individuals' online attitudes and behaviours. Specifically, this study evaluated individuals' behavioural and attitudinal intentions after visiting a website. In order to compare different approaches, we selected three websites which have implemented the Directive to a different extent. These were a website which used a message to inform about the use of cookies and allowed the individual the choice of changing the website's cookies settings (Website A); a website which used a message to inform users about its cookie policy but which gave no option to change or amend the website's cookie policy (Website B); and a third one which provided no specific information (Website C).

Due to the relationship reported between these two variables in online research (e.g., Joinson et al., 2010), we chose the willingness to disclose personal information as the behavioural measure and on the trust in the website as the attitudinal one. We also considered the possible effect of these different methods in light of other psychological variables involved in the online context, that is, online privacy concerns, privacy related behaviour and internet self-efficacy. Additionally, the study also sought to explore the effect of advance warnings about the use of cookies on users' online behaviours and attitudes. For that reason, saliency was included as a variable by asking users before visiting the website to pay attention to any message about cookies which might appear.

Considering the characteristics of the three different websites, we hypothesized that when websites allow internet users to choose their cookie settings, they would trust and be more willing to disclose than when they are only informed about the use of cookies. However, it was also expected that when users are only informed about the use of cookies, there would be no differences on trust or willingness to disclose when compared with websites that take no specific steps to comply with the Directive at all. We aimed to explore the effect of the saliency about cookies information as well as the impact on the remaining variables of interest, so there were no specific predictions concerning them.

3. Method

Participants. Sixty participants were considered for this preliminary study, where 43 of them were females (71.7%) and 17 males (28.3%). All participants were UCD School of Law's students, who voluntarily and anonymously responded an online study. The mean age of the sample was 23.32 years ($SD = 6.18$). In relation to their internet experience, 95% of participants reported a daily use of the internet. The mean number of years being using the internet was 10.33 years (range 5-20 years, $SD = 3.12$).

Instruments. The instruments considered in this study were the following:

- Trust measure (McKnight, Choudhury, and Kacmar, 2002). This is a 10-items measure, which assesses *trusting beliefs* (items 1-6) and *structural assurance* (items 7-10). Items were adapted to fit the objectives of the study. An example of items was "This website is sincere and genuine". Responses were made on a 7-point Likert-type scale, from *Disagree strongly* to *Agree strongly*.
- Disclosure measure (Rifon, LaRose, and Choi, 2005). This 10-items scale was adapted to measure the willingness to disclose on the website objective information, such as name, e-mail address or birth date. Six more additional items were included to assess the willingness to disclose other personal information, such as thoughts, emotions, photographs or current location. Two subscales were established considering the *disclosure of objective information* (items 1-10, 15-16) and the *disclosure of subjective information* (items 11-14) Participants were instructed to answer "How likely is it that you will disclose the following information on this website if it would ask you to do so?" The final 16-items scale was presented in a 5-point scale, from *Not at all likely* to *Completely likely*.
- Privacy-related attitudes scale (Buchanan, Paine, Joinson, and Reips, 2007). This 16-items scale assesses privacy concerns regarding online privacy attitudes (e.g., "Are you concerned about online identity theft?"). Responses were made on a 5-point scale from *Not at all* to *Very much*.
- Privacy-related behaviours scale (Buchanan et al., 2007). This is a 12-items scale which measures general and online privacy behaviour (e.g., "Do you clear your browser history regularly?"). It presents a 5-point scale from *Never* to *Always*.
- Internet Self-efficacy Survey (Kao, Wu, and Tsai, 2011). This is a 14-items scale, which measures perceived confidence and self-evaluation toward the utilization of the Internet. Some items were also adapted to fit the objectives of the study. An example of items was "I feel confident of using a Web browser like "Internet Explorer", 'Firefox', 'Safari' or 'Chrome'". Responses were made on a 7-point scale, from *Strongly confident* to *Strongly unconfident*.

Design and procedure. A 3 (*Method of implementation of the Directive: Website A vs Website B vs Website C*) x 2 (*Cookies use saliency: salient vs. non-salient*) between-subject factorial design was used in this online experiment. It was sought that all sites were related with the same topic to avoid any influence on this respect. It was also aimed that, although a lack of familiarity would not be ensured, the sites were related to another country. For these reasons, three telecommunications companies based in the UK were selected (see Figures 1-3).

In relation to the saliency of cookies use, some participants received the following instruction before browsing the website "Please pay attention to any message about cookies that appears before you start browsing".



Figure 1. Information provided by website A about their use of cookies.

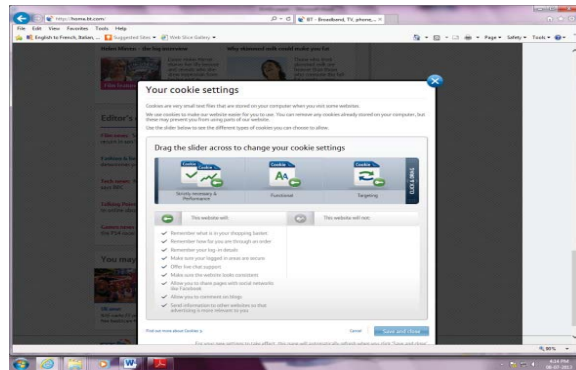


Figure 2. Website's cookie settings options provided by Website A.

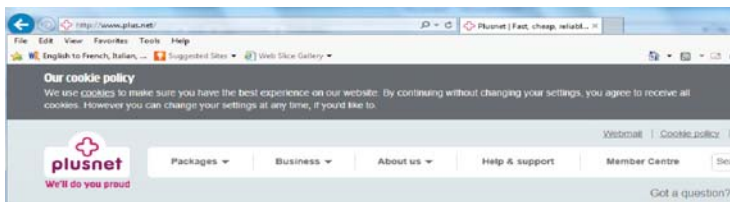


Figure 3. Information provided by website B about their use of cookies.

Participants were invited by e-mail to participate in the study and were randomly assigned to one of each 6 experimental conditions. Once informed consent was agreed, they were presented with the general instructions of the study and asked to complete questions regarding their demographic data and use of new technologies. Then, they were asked to browse for 2 minutes the website assigned. As stated before, approximately half of participants were also instructed to pay attention to any messages about cookies. Participants were asked to come back to the online survey after their visit to the website, and complete the remaining instruments.

4. Results

Firstly, descriptive analyses were performed to examine the mean and standard deviation of each experimental condition on every dependent variable (see Table 1).

Secondly, a two-way ANOVA was performed to test the effect of the different approaches and of the saliency of the information about cookies on participants' attitudes and behaviours. In relation to the measures which assessed individuals' reactions toward the website just visited, results showed no significant differences on website trust or willingness to disclose personal information amongst the conditions, $p_s > .05$. When the subscales of that measures were considered, only marginal differences were found in the disclosure measure. Specifically, there was a marginally significant main effect of the method of implementation on the disclosure of objective information, $F(2, 54) = 2.83, p = .068, \eta_p^2 = .095$, indicating a trend for higher disclosure in participants who visited Website A. There was also a marginally significant effect of the saliency condition on the disclosure of subjective information, $F(1, 54) = 2.99, p = .089, \eta_p^2 = .053$, which indicated a trend for lower disclosure in participants to whom the information about cookies use was made salient.

With regard to the remaining measures, results showed a main effect of the method of implementation on privacy-related attitudes, $F(2, 54) = 3.66, p = .032, \eta_p^2 = .119$, and on internet self-efficacy, $F(2, 54) = 7.86, p = .001, \eta_p^2 = .225$. According to pairwise comparisons, participants who visited Website C showed a higher level of online privacy concerns ($M_{estimated} = 3.41$) than those who visited Website A ($M_{estimated} = 2.44$), $p = .027$. Regarding internet self-efficacy, it was found that participants who visited Website A reported higher levels of confidence using the internet ($M_{estimated} = 1.56$), than participants who visited Website B ($M_{estimated} = 2.82$) and Website C ($M_{estimated} = 2.84$), $p = .002$ and $p = .001$ respectively.

Table 1: Means (and Standard Deviations) of the dependent variables as a function of the method of implementation of the Cookies Directive and the saliency of the information about cookies

		Dependent Variables*								
Experimental condition	N	1	2	3	4	5	6	7	8	9
		Mean (SD)	Mean (SD)	Mean (SD)	Mean (SD)	Mean (SD)	Mean (SD)	Mean (SD)	Mean (SD)	Mean (SD)
Website A										
Salient	3	4 (1.5)	4.17 (1.44)	3.75 (2.16)	2.25 (1.03)	2.53 (1.14)	1.42 (0.72)	2.37 (0.88)	2.81 (0.58)	1.4 (0.35)
Not salient	9	4.44 (1.14)	4.41 (1.01)	4.5 (1.66)	2.2 (0.78)	2.29 (0.83)	1.94 (1.04)	2.5 (0.65)	2.81 (0.54)	1.72 (0.42)
Total	12	4.33 (1.18)	4.35 (1.07)	4.31 (1.72)	2.21 (0.8)	2.35 (0.87)	1.81 (0.97)	2.47 (0.67)	2.81 (0.53)	1.64 (0.42)
Website B										
Salient	10	3.67 (1.18)	3.52 (1.19)	3.9 (1.41)	1.76 (0.62)	1.92 (0.76)	1.25 (0.41)	3.22 (0.89)	3.12 (0.77)	3.01 (1.12)
Not salient	11	3.51 (0.95)	3.53 (0.91)	3.48 (1.14)	1.67 (0.65)	1.64 (0.56)	1.75 (1.07)	3.13 (1.05)	3.22 (0.6)	2.63 (1.12)
Total	21	3.59 (1.04)	3.52 (1.02)	3.68 (1.26)	1.71 (0.62)	1.78 (0.66)	1.51 (0.84)	3.17 (0.96)	3.17 (0.67)	2.81 (1.11)
Website C										
Salient	15	3.67 (0.78)	3.61 (0.8)	3.77 (1.2)	1.76 (0.53)	1.81 (0.51)	1.6 (0.88)	3.72 (1.04)	3.29 (0.43)	2.9 (0.83)
Not salient	12	4.02 (0.68)	3.92 (0.73)	4.19 (0.81)	1.91 (0.76)	1.87 (0.71)	2.02 (1.15)	3.1 (0.88)	2.9 (0.66)	2.78 (0.78)
Total	27	3.83 (0.74)	3.75 (0.77)	3.95 (1.05)	1.82 (0.63)	1.84 (0.59)	1.79 (1.02)	3.44 (1)	3.11 (0.57)	2.85 (0.79)
Total										
Salient	28	3.71 (0.98)	3.64 (1)	3.81 (1.33)	1.81 (0.62)	1.93 (0.69)	1.45 (0.73)	3.39 (1.03)	3.18 (0.59)	2.78 (1.01)
Not salient	32	3.97 (0.97)	3.92 (0.92)	4.03 (1.24)	1.91 (0.74)	1.91 (0.73)	1.91 (1.06)	2.94 (0.91)	2.98 (0.62)	2.43 (0.93)
Total	60	3.84 (0.97)	3.79 (0.96)	3.93 (1.28)	1.86 (0.68)	1.92 (0.7)	1.7 (0.94)	3.15 (0.99)	3.07 (0.6)	2.59 (0.98)

*Note: 1 = Trust (total); 2 = Trusting beliefs; 3 = Structural assurance; 4 = Disclosure (total); 5 = Disclosure of objective information; 6 = Disclosure of subjective information, 7 = Privacy-related attitudes; 8= Privacy-related behaviours; 9 = Internet Self-efficacy.

5. Discussion

The aim of the study was to conduct a preliminary examination and comparison of the effect of different methods of implementation of the EU Cookies Directive on participants' attitudes and behaviour. Results showed no significant differences for users' trust or disclosure under either the different approaches to compliance used, or the saliency of the information provided. This did not support our predictions.

From a legal point of view, this result suggests that the Cookies Directive may have limited, if any, impact on the attitudes or behaviour of users of online technology. Regardless of the approach to compliance adopted, users demonstrated similar patterns of trust in the website and willingness to disclose personal information. This raises questions over the value and efficacy of the requirements introduced by the Directive.

However, with the necessity for caution in interpreting results of what was a preliminary study, it might be anticipated that a future study with a bigger sample size could show that when individuals visit websites which clearly inform about their use of cookies and allow users to change its cookies settings, they would be more willing to trust and disclose information than when visiting websites that just inform about their cookies use. This was supported by the mean values and marginally significant effects found in this study. It also seems possible that there will not appear to be differences on trust or disclosure between websites which only use warnings and those who do not use them.

These expected results of future studies are partially supported by the differences found on privacy attitudes and internet self-efficacy. Participants who visited the Website A felt less concerned about online privacy than those who

visited the Website C, and felt more confident about their internet use than participants from both groups. It is worth noting that these differences were found on the measures which assessed more malleable variables, such as attitudes (privacy concerns) and self-efficacy, but not when individuals were reporting their own behaviour. These results undoubtedly call for future investigations which explore these effects in greater depth and detail.

Such future investigations would also have value in assessing the efficacy of the Directive, and in considering how legal and regulatory authorities ought to interpret the concepts of “clear and comprehensive information” and “consent” in the Directive. More generally, such investigations may also allow comparisons to be drawn between the level of knowledge of cookies amongst users since the introduction of the Directive, as compared with the levels of knowledge demonstrated in surveys conducted prior to its introduction.

Although the aim of this study was to provide preliminary results on the topic, some limitations should be indicated. First of all, the sample size does not allow yet providing decisive conclusions about the results. Secondly, the sample was comprised only by Law students, which reduces the generalization of results. While students are one of the largest internet users segment (Baek and Morimoto, 2012) and then their participation in online research can be appropriate, our sample was homogeneous regarding the participants' background (only Law students) and unbalanced in relation to participants' sex (near to 72% were females). As stated before, it is our purpose to enhance the number of participants in future studies as well as to gather a more heterogeneous and sex-balanced sample which may, presumably, lead to even more relevant implications about the influence of online legal regulation on individuals' online interaction.

References

- Baek, T. H., & Morimoto, M. (2012). Stay away from me. *Journal of Advertising*, 41(1), 59-76.
- Buchanan, T., Paine, C., Joinson, A. N., & Reips, U-D. (2007). Development of measures of online privacy concern and protection for use on the internet. *Journal of the American Society for Information Science and Technology*, 58(2), 157-165.
- Carolan, E., & Delany, H. (2008). *The Right to Privacy: A Doctrinal and Comparative Analysis*. Dublin: Thomson Round Hall.
- Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector.
- Directive 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.
- Fogel, J., & Nehmad, E. (2009). Internet social network communities: risk taking, trust and privacy concerns. *Computers in Human Behaviour*, 25, 153-160.
- Joinson, A. N., Reips, U.-D., Buchanan, T., & Paine-Schofield, C. B. (2010). Privacy, trust, and self-disclosure online. *Human-Computer Interaction*, 25, 1-24.
- Junglas, I. A., Johnson, N. A., & Spitzmüller, C. (2008). Personality traits and concern for privacy: an empirical study in the context of location-based services. *European Journal of Information Systems*, 17, 387-402.
- Kao, C.-P., Wu, Y.-T., & Tsai, C.-C. (2011). Elementary school teachers' motivation toward web-based professional development, and the relationship with Internet self-efficacy and belief about web-based learning. *Teaching and Teacher Education*, 27, 406-405.
- McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). The impact of initial consumer trust on intentions to transact with a web site: a trust building model. *Journal of Strategic Information Systems*, 11, 297-323.
- Rifon, N. J., LaRose, R., & Choi, S. M. (2005). Your privacy is sealed: effects of web privacy seals on trust and personal disclosures. *Journal of Consumer Affairs*, 39(2), 339-362.
- Rittweger, C., Krone, D., & Wendler, J. (2011). New EU rules regarding cookies: Member States' different approaches to implementation. *World Data Privacy Report*, 11(7), 9-12.
- Rosler B. (2004). *The Value of Privacy*. Cambridge: Polity Press.
- Working Party Opinion 15/2011 on the definition of consent (WP 187), Article 29.
- Yao, M. Z., Rice, R. E., & Wallis, K. (2007). Predicting user concerns about online privacy. *Journal of the American Society for Information Science and Technology*, 58(5), 710-722.