Communicating Compliance: Developing a GDPR Privacy Label

Emergent Research Forum (ERF)

Grace Fox
Irish Centre for Cloud Computing and Commerce, Dublin City University
grace.fox@dcu.ie

Colin Tonge
Irish Centre for Cloud Computing and Commerce, Dublin City University
colin.tonge@dcu.ie

Theo Lynn
Irish Centre for Cloud Computing and Commerce, Dublin City University
theo.lynn@dcu.ie

John Mooney
Pepperdine University
john.mooney@pepperdine.edu

Abstract

The growing pervasiveness of technology enables the collection of copious volumes of personal data which creates risks for consumer privacy and makes data protection increasingly complex for organizations. The difficulties facing organizations are further exasperated by the EU General Data Protection Regulation (GDPR), which introduces stringent requirements for gaining consent, communicating privacy practices, and transparency. Furthermore, consumers’ current lack of privacy knowledge can heighten privacy concerns. This study aims to (1) build consumer privacy knowledge and (2) assist organizations in gaining explicit consent and communicating their privacy practices to current and potential customers, through the development of a GDPR privacy label. The paper contributes to practice by providing actionable guidelines for developing GDPR compliant privacy notices and advances privacy literature by extending the privacy knowledge gap model and testing the effectiveness of the GDPR label in improving consumers’ privacy knowledge thereby building self-efficacy and enabling informed decision making.

Keywords

GDPR, General Data Protection Regulation, Privacy Label, Privacy knowledge.

Introduction

Due to the increasing prevalence and habitualization of consumer surveillance in recent decades, privacy has become and remains an increasingly important issue for policymakers, organizations, and individual citizens. The ever-growing pervasiveness of technology in every aspect of our lives enables the collection of copious volumes of personal data on individuals which creates undeniable risks for the privacy of the individual (Bélanger and Xu, 2015). This ubiquity combined with the liquid nature of technology-based surveillance, makes data protection increasingly complex for organizations (Bauman and Lyon, 2013). However, for many organizations privacy is simply not viewed as a priority. This was evidenced in an Ernst and Young (2016) report in which 38% of 630 privacy professionals stated their organization addresses data security, but not privacy. In addition to shortcomings in current privacy practices, privacy is thwarted by other challenges including communicating compliance with consumers. Previously, efforts to ensure consumers were informed of an organization’s privacy practices held importance only among organizations described as privacy differentiators, or companies who engage in enhanced privacy practices in an effort to gain strategic advantage (Greenaway et al., 2015). However, the EU General Data Protection Regulation (GDPR) extends the territorial scope for organizations required to comply and introduces stringent requirements for transparency and consent. As a result, the challenges around effectively communicating privacy practices become pertinent to all organizations processing personal data on European citizens.
For consumers, privacy concerns have reached all-time highs with numerous studies showing that privacy concerns can lead to negative outcomes for organizations such as consumers refusing to disclose data, falsifying data disclosed, resisting adoption of a technology, and spreading negative word of mouth (Son and Kim, 2008). In addition, consumers currently lack privacy knowledge, or an understanding of the implications associated with technology use and information disclosure (Croselier and Bélanger, 2017). This lack of knowledge may be partly attributed to the approaches organizations use to communicate with consumers. For instance, privacy policies tend to be quite lengthy and written in a manner which can obfuscate rather than explain their privacy practices (Ciocchetti, 2008). Recent literature has demonstrated the potential of a nutrition label approach to communicate privacy practices to consumers (e.g. Kelley et al., 2010). This study adopts the label approach to develop a GDPR label to communicate organizations’ privacy practices to consumers. The study has two objectives. First, the paper develops the GDPR privacy label to help organizations communicate their GDPR compliance to consumers. Second, the study examines the effectiveness of the GDPR label in building consumers’ privacy knowledge. The next section of the paper provides a brief overview of the pertinent aspects of the GDPR. The existing literature is then outlined, followed by a summary of the GDPR label design and a discussion of the next steps in the research.

**Background: GDPR**

The GDPR came into effect across Europe in 2016, with organizations required to comply by May 25th 2018. The GDPR seeks to overcome the fragmentation of current regulation through the creation of a uniform framework which provides consumers with greater control over their personal data, increases organizational accountability and enforces strict penalties for non-compliance (ICO, 2017). The geographical scope of the regulation is extended and includes organizations with a presence in Europe and organizations located outside of Europe engaged in processing the personal data of European citizens. Thus, the number organizations required to comply with GDPR is significantly greater than the existing directive. A number of aspects of the new regulation are relevant to this paper. First, the requirements of valid consent are significantly tighter under GDPR. To be considered valid, consent must (1) be freely given, individuals must be able to withdraw or refuse consent without detriment, (2) be specific covering all uses of data, (3) be informed, clear and concise, and (4) include affirmative action (ICO, 2017). These amendments necessitate the restructuring of current consent practices which often include privacy terms within the website’s terms and conditions. Second, the GDPR adds the accountability principle, which requires organizations to be able to demonstrate consent and compliance with GDPR and represents a dramatic shift in the burden of proof. Third, the GDPR stipulates that organizations must provide individuals with information about how they process their personal data in a concise, transparent, and easy to access format.

Online privacy policies are the dominant way in which organizations communicate their privacy practices to current and potential customers. However, the current instantiation of these policies is fraught with weaknesses. First, privacy policies tend to be quite lengthy and written in a complex manner making them difficult and time consuming to read (Kelley et al., 2010). Indeed, the time required to read the privacy policies of all websites visited by an average American Internet user was estimated as 201 hours annually (Mac Donald and Craner, 2008). Second, when consumers read privacy policies they often do not understand the contents (Martin, 2015; Ciocchetti, 2008). Thus, these policies fail to meet their purpose of communicating privacy practices to consumers. There is a need for alternative, more effective methods of communicating privacy to end users such as the nutritional privacy label approach which was developed and validated in prior work (van der Werff, et al., 2014; Kelley et al., 2009; 2010). Despite the potential of nutrition labels to improve individuals understanding of privacy, this approach has received limited attention in the literature (Ciocchetti, 2008). This study builds upon the nutritional label approach to develop a GDPR privacy label. We argue that the nutrition label approach can not only assist organizations in meeting regulatory requirements but can also improve citizens’ understanding of privacy practices and facilitate informed decision making regarding the disclosure of personal information.

**Literature Review**

Privacy has attracted a great deal of empirical research in the Information Systems (IS) discipline, with the majority of studies following Smith, Dinev and Xu’s (2011) APCO model exploring antecedents, privacy concerns, and outcomes of concern (Bélanger and Croselier 2011; Smith et al., 2011). This approach has been adapted to explore the influence of individuals’ privacy concerns on privacy behaviors across a range of...
contexts with numerous studies providing evidence to support the link between privacy concerns and privacy-protective behaviors such as refusal to disclose information, falsification of information and resistance towards technology usage and data disclosure (Son and Kim, 2008). However, the link between privacy concerns and behaviors has been called to question by studies which indicate that a privacy paradox exists; when individuals express high concerns but do not engage in privacy-protective behaviors (Bélanger and Crossler, 2011). A number of potential explanations exist for this paradox including cognitive biases (Dinev et al., 2015) and methodological limitations in the approaches used to examine this relationship (Alashoor, Fox, and Smith, 2017). Another possible explanation is the absence of measures of individuals’ privacy knowledge from existing models (Crossler and Bélanger, 2017). This is an important exclusion as privacy studies have highlighted that individuals lack an understanding of the privacy implications associated with technology use (Fox and Connolly, 2018). This lack of privacy knowledge may lead individuals to make uninformed decisions (Fox and Connolly, 2018; Crossler and Bélanger, 2017).

Crossler and Bélanger (2017) recently presented the Mobile Privacy-Security Knowledge Gap model and a research agenda for understanding the links between individuals’ privacy knowledge, beliefs and behavior. As shown in figure 1 below, we adapt this model to explore how a GDPR privacy label can narrow the gap between citizens’ privacy knowledge regarding an organization’s privacy practices, their privacy self-efficacy and resultant behaviors. The left side of the model focuses on the role of individuals’ past experiences and knowledge. In line with Crossler and Bélanger (2017), we propose that individuals’ awareness of privacy issues namely privacy media coverage and awareness of the GDPR will influence their current level of privacy knowledge. Individuals are likely to differ in their motivation to develop privacy knowledge, thus past privacy invasion experience and perception of privacy norms is likely to influence their motivation to learn about organizations’ privacy practices. Upon viewing the GDPR label if citizens believe the organization’s privacy practices meet privacy norms, they are likely to express higher privacy self-efficacy and willingness to interact with that website. Crossler and Bélanger (2017) posit that a knowledge-belief gap exists between individuals’ privacy knowledge in a specific domain and their privacy self-efficacy, or their perceived ability to manage the privacy of their information. In this study, we present the GDPR privacy label specific to the E-commerce context as a knowledge-building tool to help improve consumers’ privacy knowledge and narrow the gap between their knowledge, perceived control and privacy self-efficacy.

Figure 1. Adapted Privacy Knowledge Gap Model

Methodology

This study follows a multi-stage iterative design and testing methodology similar to that followed by Kelley et al. (2009; 2010). The first stage involved developing two GDPR privacy labels, one icon-based label and one text-based label for two fictitious E-commerce websites. In terms of content considerations, the labels capture all information organizations are required to include in their privacy notices (ICO, 2017). This includes: (1) the identity and contact details of the data controller, (2) the processing purposes for the personal data and the legal basis for the processing, (3) the recipients or categories of recipients of the...
personal data, (4) if the data will be transferred to a third country, the details of the safeguards in place, (5) retention period for the data, (6) the data subject’s rights to request: access to their data, rectification, restriction of processing, erasure of data, and data portability, (7) if data processing is based on consent, the right to withdraw consent at any time (8) the right to complain to the supervisory authority, (9) whether the disclosure of personal data is a statutory or contractual requirement and the consequences of non-disclosure (10) the use of automated decision-making such as profiling, the logic and impact of such processing (11) the contact details of the data protection officer and (12) information on further processing.

The labels were first reviewed by GDPR experts to ensure content met privacy notice requirements described by the Information Commissioner’s Office or the ICO (2017). In terms of design, best practices outlined by Kelley et al. (2010) were followed including using bold rules to highlight important information. Recommendations made by the ICO (2017) for GDPR privacy notices were also followed including using commonly understood icons and using a layered approach which allows consumers to click to expand sections of the label. For example, in the ‘your rights’ section, there is a clickable link to the full privacy policy. The labels were reviewed by design experts to ensure both designs followed best practice. The next stage of testing consisted of a pilot test among a group of 32 Postgraduate Students in an Irish University. Following the approach outlined by Kelley et al. (2010), respondents were randomly assigned (1) a full length written GDPR-compliant privacy policy and (2) one version of the GDPR label (either icon or text based). The order of these assignments was also randomized. Respondents were asked several knowledge-based questions based on the policy and label they viewed. Their level of satisfaction with each label and perceived trust were also explored. Following the survey, two focus groups were conducted to elicit feedback on the label design. The initial insights from testing suggest highly positive perceptions towards the icon-based label. Survey and focus group findings were analyzed to redesign the GDPR privacy labels. As illustrated in figure 2 below, the new labels are both icon-based but one includes consent mechanisms which allow users to toggle on and off and provide explicit consent for different activities. These labels were also reviewed by GDPR and design experts. The next stage will involve testing the adapted privacy knowledge gap model using an experimental design among a broader representative sample of Irish consumers. This will allow the empirical examination of the effectiveness of the GDPR privacy labels in developing individuals’ privacy knowledge and the influence of consent mechanisms on privacy self-efficacy, as well as the links between privacy knowledge, beliefs and behavior i.e. willingness to interact with a website.

![Figure 2. Icon based labels with and without consent mechanisms](image-url)

### Conclusion

Privacy represents an important issue for organizations and individuals alike. This research will provide actionable insights for organizations developing GDPR compliant privacy notices, thus not only achieving...
compliance but also realizing the benefits associated with privacy-friendly practices (Martin, 2015). The study advances the privacy literature by adapting the privacy knowledge gap model to the GDPR context and developing a method for improving consumers’ privacy knowledge in line with new data protection regulation, thereby building self-efficacy and enabling informed privacy decision making.

Acknowledgements

This research was supported by the Irish Centre for Cloud Computing and Commerce, an Irish National Technology Centre funded by Enterprise Ireland and the Irish Industrial Development Authority.

REFERENCES


