The current issue and full text archive of this journal is available on Emerald Insight at:
https://www.emerald.com/insight/0959-3845.htm

Enhancing consumer perceptions of privacy and trust: a GDPR label perspective

Grace Fox
Irish Institute of Digital Business, Dublin City University, Dublin, Ireland, and
Theo Lynn and Pierangelo Rosati
Dublin City University Business School, Dublin, Ireland

Received 17 September 2021
Revised 7 December 2021
17 January 2022
Accepted 18 February 2022

Abstract

Purpose – The General Data Protection Regulation (GDPR) introduces significant data protection obligations on all organizations within the European Union (EU) and those transacting with EU citizens. This paper presents the GDPR privacy label and uses two empirical studies to examine the effectiveness of this approach in influencing consumers' privacy perceptions and related behavioral intentions.

Design/methodology/approach – The paper tests the efficacy of two GDPR privacy label designs, a consent-based label and a static label. Study 1 examines the effects of each label on perceptions of risk, control and privacy. Study 2 investigates the influence of consumers' privacy perceptions on perceived trustworthiness and willingness to interact with the organization.

Findings – The findings support the potential of GDPR privacy labels for positively influencing perceptions of risk, control, privacy and trustworthiness and enhancing consumers' willingness to transact and disclose data to online organizations.

Practical implications – The findings are useful for organizations required to comply with the GDPR and present a solution to requirements for transparent communications and explicit consent.

Originality/value – This study examines and demonstrates the efficacy of visualized privacy policies in impacting consumer privacy perceptions and behavioral intentions.

Keywords Privacy policies, Communication privacy management, Perceived privacy, GDPR

Paper type Research paper

1. Introduction

Data gathered from all stages of consumers' interactions with an organization's website offer endless opportunities to predict behaviors and personalize offerings (Chang *et al.*, 2018). While consumers benefit from personalization, the ever-increasing volume of personal data collected creates undeniable risks to individuals' privacy and may exacerbate consumers' concerns regarding data misuse (Chang *et al.*, 2016). The fallout of this dilution in consumers' perception of privacy online can lead to negative outcomes for organizations such as consumers spreading negative word of mouth, falsifying data disclosed, reduced purchasing intentions (Son and Kim, 2008), reactance to personalized advertising (Tucker, 2014) and negative stock returns (Martin *et al.*, 2017). The importance of understanding the ways consumer privacy concerns impact technology use and how to alleviate these concerns is continually highlighted in the literature (Wang *et al.*, 2019; Yun *et al.*, 2019; Mousavi *et al.*, 2020).

The root of damaging privacy-protective behaviors is the vulnerability consumers feel when organizations collect excessive volumes of personal information (Martin *et al.*, 2017).

Information Technology & People
Vol. 35 No. 8, 2022
pp. 181-204
Emerald Publishing Limited
0959-3845
DOI 10.1108/ITP-09-2021-0706

Increasing perceptions of control (Tucker, 2014), reducing perceptions of risk (Xu *et al.*, 2011) and building trust (Dinev and Hart, 2006) represent mechanisms for restoring consumers' sense of privacy. To build these perceptions, organizations must be transparent in their privacy-related communications (Martin *et al.*, 2017). Institutional privacy assurances are efforts by organizations to inform consumers of the privacy protection measures in place (McKnight *et al.*, 2002). They are widely viewed as the primary mechanism to appease privacy concerns and foster trust (Pan and Zinkhan, 2006) and in turn reduce privacy-protective behaviors such as limiting information disclosure (Gong *et al.*, 2019).

Privacy policies, the dominant form of privacy assurance, are important communication tools for informing customers of an organization's privacy practices (Wedel and Kannan, 2016). Despite their popularity, privacy policies present many issues. First, they tend to be quite lengthy and difficult to read (Soumelidou and Tsohou, 2019; Kelley *et al.*, 2010). Furthermore, many consumers do not read privacy policies, and when they do, they often do not understand the contents (Park and Jang, 2014). For instance, a recent PEW Research Center study revealed that 38% of US adults sometimes read privacy policies, but only 8% understand the contents (Auxier *et al.*, 2019). Thus, privacy policies may have the opposite result than intended, exacerbating rather than appeasing confusion, and lead consumers to withhold data (Stutzman *et al.*, 2011).

The distributed nature of the Internet and associated information and communications technologies, including cloud computing, have introduced acute jurisdictional questions regarding the regulation of online activities and data protection and privacy specifically (Ryngaert and Taylor, 2020). Individual nation states have responded to this deterritorialization by introducing their own laws to govern transborder activities and data protection (Ryngaert and Taylor, 2020), the most significant of which being the European Union General Data Protection Regulation (GDPR). In 2016, the GDPR came into effect across Europe, and organizations were required to comply by May 25th, 2018. The GDPR created a uniform framework that provides consumers with greater control over their personal data, increases organizational accountability and enforces strict penalties for noncompliance (ICO, 2017). GDPR extends the geographical scope of EU data protection regulation to include organizations with a presence in Europe and organizations located outside of Europe engaged in processing the personal data of European citizens. As well as its significant extraterritorial reach, the GDPR introduced a number of regulatory features relevant to this paper. First, under the GDPR, valid consent is (1) freely given, that is, individuals must be able to withdraw or refuse consent without detriment; (2) specific, that is, covering all uses of data; (3) informed, clear and concise; and (4) includes affirmative action (ICO, 2017). Second, the GDPR introduces an accountability principle, which shifts the burden of proof to organizations collecting and using data. It specifically requires organizations to be able to demonstrate consent and compliance with the GDPR. 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. This includes where data is collected directly from the individual data subject (Article 13) or from third parties (Article 14). Failure to comply with the GDPR is substantial as Article 83 allows for fines of up to €10m, or 2% of worldwide annual revenue from the preceding financial year, whichever amount is higher.

The introduction of the GDPR means privacy policies are no longer optional, but a legal obligation of all organizations in the EU and those transacting with EU citizens. While the majority of existing privacy policies are built around the Fair Information Practice Principles (FIPPs), the GDPR introduces stringent requirements for the content, language and length of privacy disclosures recommending brief, easy to understand privacy notices (ICO, 2017). Thus, the current composition of most privacy policies not only fails to effectively communicate privacy practices to consumers but does not comply with the GDPR. There is a need to adjust privacy policies to better inform consumers how their information is used.

Existing research has explored the role of privacy policies from a number of angles beginning with whether the *presence* and the *length* of a privacy policy influenced consumer perceptions such as trust (Pan and Zinkhan, 2006) and behaviors such as willingness to transact with E-commerce vendors (Miyazaki and Fernandez, 2000), and if the *content* of the privacy policy influences perceptions of trustworthiness (Wu *et al.*, 2012), risk and control (Chang *et al.*, 2018). Despite recent research demonstrating the effectiveness of visualization techniques such as the P3P Expandable Grid visualization matrix (Reeder *et al.*, 2008), nutritional privacy labels (Kelley *et al.*, 2009) and privacy policy cards (Soumelidou and Tsohou, 2019), much of the extant research examines the influence of consumers' perceptions of the effectiveness FIPPs-based written privacy policies on privacy-related perceptions such as trust, risk (Wang *et al.*, 2019) and privacy concerns (Gong *et al.*, 2019). As discussed, the GDPR introduces more stringent requirements for organizations collecting data within the EU and from EU citizens, requirements that may not be met by FIPPs-based written privacy policies.

This study builds upon these visualization studies and adapts the nutrition privacy label developed by Kelley *et al.* (2009), to develop two GDPR-privacy labels and examine the influence of these labels on privacy perceptions and behaviors. This approach leverages common icons as recommended by researchers (Mutimukeye *et al.*, 2020; Soumelidou and Tsohou, 2019; Tsai *et al.*, 2011) and regulators (ICO, 2017). The FIPPs-based privacy policies used in many studies (e.g. Libaque-Sáenz *et al.*, 2021; Mutimukeye *et al.*, 2020) do not meet the requirements of GDPR, with the exception of Soumelidou and Tsohou (2019), who visualize Instagram's GDPR-compliant privacy policy and Railean and Reindhardt (2020), who visualize a GDPR-compliant privacy label for an Internet of Things (IOT) device. In contrast, this study employs two GDPR-compliant privacy policy labels representing a fictional E-commerce website. One label is static merely communicating one way to end users; the other is consent-based, thereby providing end users with some semblance of control. The choice of an e-commerce website is important as it represents a widely used and transactional context in contrast to IOT devices and social media. By using a fictional website, we remove any bias associated with existing brands and move beyond the tendency of existing studies to either compare visualized policies to written policies or focus on perceived effectiveness of written policies (Soumelidou and Tsohou, 2019).

Similar to recent privacy policy studies (e.g. Wang *et al.*, 2019; Chang *et al.*, 2018), we leverage communication privacy management (CPM) theory to examine the effectiveness of GDPR privacy labels on consumers' perceptions regarding online organizations. CPM is a form of boundary management that focuses on understanding how individuals manage their personal privacy and consists of three elements; boundary rule formation, coordination and turbulence (Metzger, 2007; Petronio, 2012), with the first two elements examined in this study. Individuals form rules to manage the sharing of their personal information (boundaries) based on five criteria: gender, culture, context, perceptions of costs and benefits and motivation (Petronio, 2012). Recent research has focused on the contextual nature of rule formation and the cost–benefit ratio, studying the role of risk and control (Chang *et al.*, 2018; Xu *et al.*, 2011). Existing literature and CPM contend that individuals hold perceptions related to privacy in a given context and these perceptions can be influenced by experiences and interventions such as privacy policies (Awad and Krishnan, 2006). Boundary turbulence occurs when the parties to personal information are not *ad idem* with regard to privacy rules and specifically the use of private information (Chang *et al.*, 2018; Petronio, 2012). In the context of the GDPR, unresolved boundary turbulence may result in a complaint to a data protection commissioner and potentially financial penalties.

Privacy labels, in effect, are a means of mitigating or avoiding boundary turbulence by communicating privacy policies. As CPM posits that individuals define privacy boundaries based on their preexisting perceptions as well as boundary coordination in new situations such as transacting with an E-commerce vendor, this paper features two studies, one exploring how privacy labels might influence preexisting perceptions, and one on how they may influence intention to transact. Using the privacy label as a form of boundary coordination between the individual and the organization, the first study measures individuals' general perceptions of risk, control and privacy and investigates the potential of privacy labels to influence these perceptions as they relate to a specific fictional organization. Trust is fundamental to e-commerce (Gefen *et al.*, 2003) and transactional relationships (Chang *et al.*, 2016). While extant research has explored the negative correlates between trust and privacy variables (e.g. Kim, 2008; Hong and Thong, 2013; Dinev *et al.*, 2013), there is a need to explore positive privacy correlates and trust. To further our understanding of boundary coordination and consumers' privacy-related behaviors, study 2 examines how privacy perceptions influence perceived trust and willingness to transact with the organization.

The study advances privacy literature in the domain of institutional privacy assurances in three ways. First, it answers calls for research on effective privacy policy visualization (Soumelidou and Tsohou, 2019) and builds on privacy visualization studies to develop GDPR privacy labels, which meet regulatory requirements for privacy notices. Second, the study examines the effectiveness of this approach by comparing two labels, which differ in the level of explicit consent, and moves beyond the emphasis on perceived effectiveness of written privacy policies. Specifically, we compare a proxy privacy control mechanism (privacy policy and static trust label) with a user customizable privacy mechanism. While the former is subject to change without notice or consent, the latter is not. As Mousavi *et al.* (2020) note, these types of assurance mechanisms act differently and therefore considering them in isolation is not sufficient. Such a comparison of privacy mechanisms has not been considered for trust labels in the extant literature and answers calls for research on explicit consent mechanisms in communications with consumers (Bradlow *et al.*, 2017). Third, the study builds on recent work harnessing CPM to link privacy assurances to privacy perceptions (e.g. Wang *et al.*, 2019). While Wang *et al.* (2019) focus on how perceived privacy risks and self-efficacy jointly determine privacy concerns in a social media context, we extend our understanding of the boundary rule formation and coordination processes among a broader range of privacy perceptions in an e-commerce context, while also incorporating trust and behavioral intentions. In this way, we also build on and extend previous research on trust and behavioral intentions in e-commerce (e.g. Liu *et al.*, 2005; Eastlick *et al.*, 2006) and the application of CPM to e-commerce (e.g. Xu *et al.*, 2011; Metzger, 2007).

The paper proceeds with a brief outline of the background to privacy policies and the label design process. Each study is discussed separately beginning with theory, proposed model and hypotheses, prior to outlining the research design, analysis and results. The discussion outlines the study's empirical and theoretical contributions. Practical implications are provided along with limitations and directions for future research.

2. Institutional privacy assurances

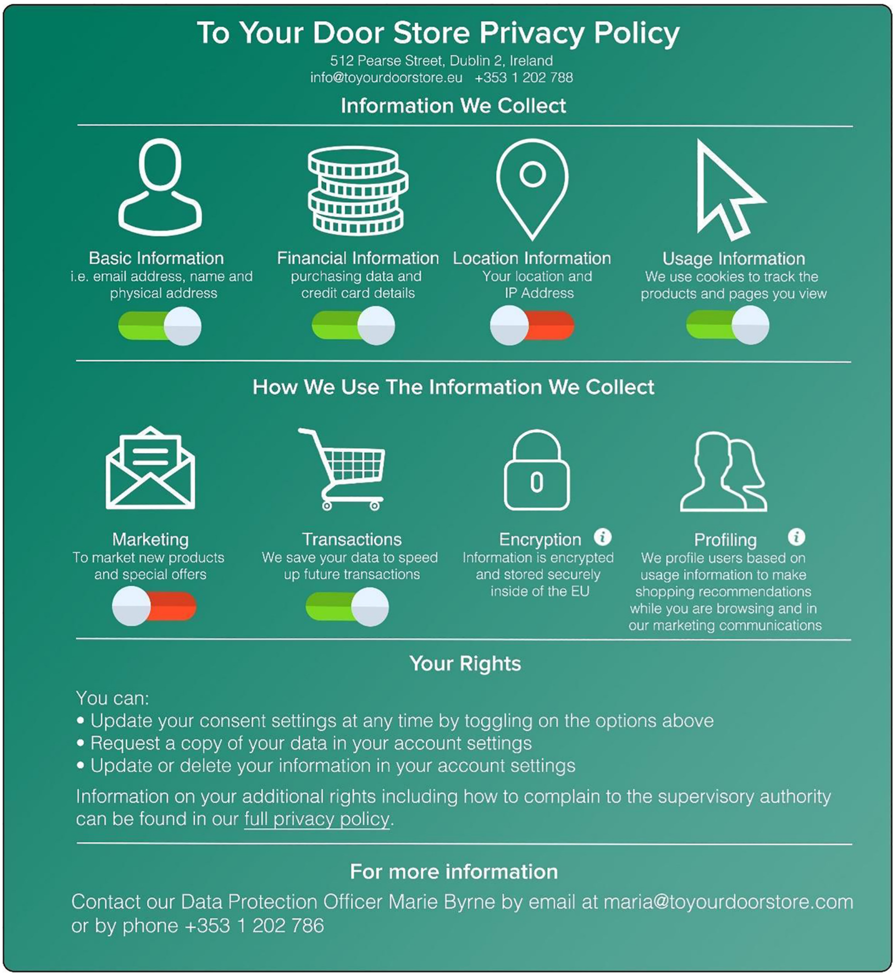
Institutional privacy assurances are interventions that a firm makes to assure consumers that efforts have been made to protect personal information (Xu *et al.*, 2011). They emerged as an attempt by E-commerce organizations to address consumers' privacy concerns (Tsai *et al.*, 2011). Privacy assurances include privacy seals, privacy-enhancing technologies and, most commonly, privacy policies (Mutimukeye *et al.*, 2020). The aim of privacy policies is to communicate an organization's privacy practices (Tsai *et al.*, 2011). Privacy laws and privacy-enhancing technologies have lagged advances in data collection and analytics (Wedel and Kannan, 2016) enabling vendors to largely self-police. This has resulted in a disjointed approach to privacy policies. While it is likely stricter regulation will be introduced in the USA in the coming years (Wedel and Kannan, 2016), most privacy policies currently follow the FIPPs, highlighting notice, choice, access and security. Research has highlighted the potential of privacy policies to empower consumers with control over their personal data (Steinfeld, 2016), inform consumers of how their data will be utilized (Xu *et al.*, 2011) and build trust (Mutimukeye *et al.*, 2020). However, the current instantiation of privacy policies as long, technical, confusing documents can obfuscate consumers rather than educate them. From an ethical and regulatory standpoint, it is important to rejuvenate these privacy communication tools toward a more consumable approach.

The recently introduced EU GDPR stipulates clear communication with consumers regarding information privacy practices. GDPR applies to all organizations in Europe and organizations outside of the EU collecting personal data on European citizens. Articles 13 and 14 of the GDPR lay out the requirements of transparent communication and content requirements for privacy notices (ICO, 2017). The GDPR recommends the development of privacy notices as opposed to privacy policies. The format of privacy notices is flexible, but they must be brief and easily understood. Research has demonstrated the potential of visualization techniques such as privacy icons (Tsai *et al.*, 2011), privacy policy cards and privacy clouds (Soumelidou and Tsohou, 2019) and nutritional privacy labels (Kelley *et al.*, 2009). This study adopts the nutritional privacy label validated in work on trust labels and FIPPs-based privacy labels (Kelley *et al.*, 2009, 2010; van der Werff *et al.*, 2019). This approach enables the level of detail required to meet GDPR requirements and the incorporation of visualization recommendations.

2.1 GDPR privacy label development

The labels were developed and presented based on guidelines from the UK Information Commissioner's Office (ICO, 2017). Each label detailed: (1) contact details of the data controller; (2) processing purposes for the personal data and the legal basis for processing; (3) categories of recipients of the personal data; (4) safeguards if transferring data to a third country; (5) the data subject's rights to request access, rectification, restriction of processing, erasure and data portability; (6) the right to withdraw consent at any time; (7) the right to complain to the supervisory authority, (8) whether the disclosure of personal data is a statutory or contractual requirement and the consequences of nondisclosure; (9) the use of automated decision-making such as profiling, the logic and impact of such processing; (10) contact details of the data protection officer; and (11) information on further processing. For the purpose of the studies presented in this paper, retention period was not included as it is use-specific. It is important to note that outside the EU, FIPPs-based written privacy policies are common; however, they may not meet the requirements of the GDPR, while a GDPR-compliant privacy policy should meet FIPPs. As such, a significant design principle for the proposed privacy labels was that it could meet the requirements of both approaches.

In the design of the label, best practices outlined by Kelley *et al.* (2010) were followed including: placing a box around the label to clearly mark the boundaries, using bold rules to mark important information and assist readers in working through the label and including a clear title to communicate the label's purpose. Recommendations made by the ICO (2017) for privacy notices were followed including using commonly understood icons and a layered approach allowing consumers to click to expand sections of the label such as a clickable link to the full privacy policy. The labels were reviewed by design and GDPR experts and pilot tested across multiple conditions following the approach outlined by Kelley *et al.* (2010). The two refined labels are provided in Figure 1 and 2A



To Your Door Store Privacy Policy

512 Pearse Street, Dublin 2, Ireland
info@toyourdoorstore.eu +353 1 202 788

Information We Collect

Basic Information
i.e. email address, name and physical address

Financial Information
purchasing data and credit card details

Location Information
Your location and IP Address

Usage Information
We use cookies to track the products and pages you view

How We Use The Information We Collect

Marketing
To market new products and special offers

Transactions
We save your data to speed up future transactions

Encryption
Information is encrypted and stored securely inside of the EU

Profiling
We profile users based on usage information to make shopping recommendations while you are browsing and in our marketing communications

Your Rights

You can:

- Update your consent settings at any time by toggling on the options above
- Request a copy of your data in your account settings
- Update or delete your information in your account settings

Information on your additional rights including how to complain to the supervisory authority can be found in our full privacy policy.

For more information

Contact our Data Protection Officer Marie Byrne by email at maria@toyourdoorstore.com or by phone +353 1 202 786

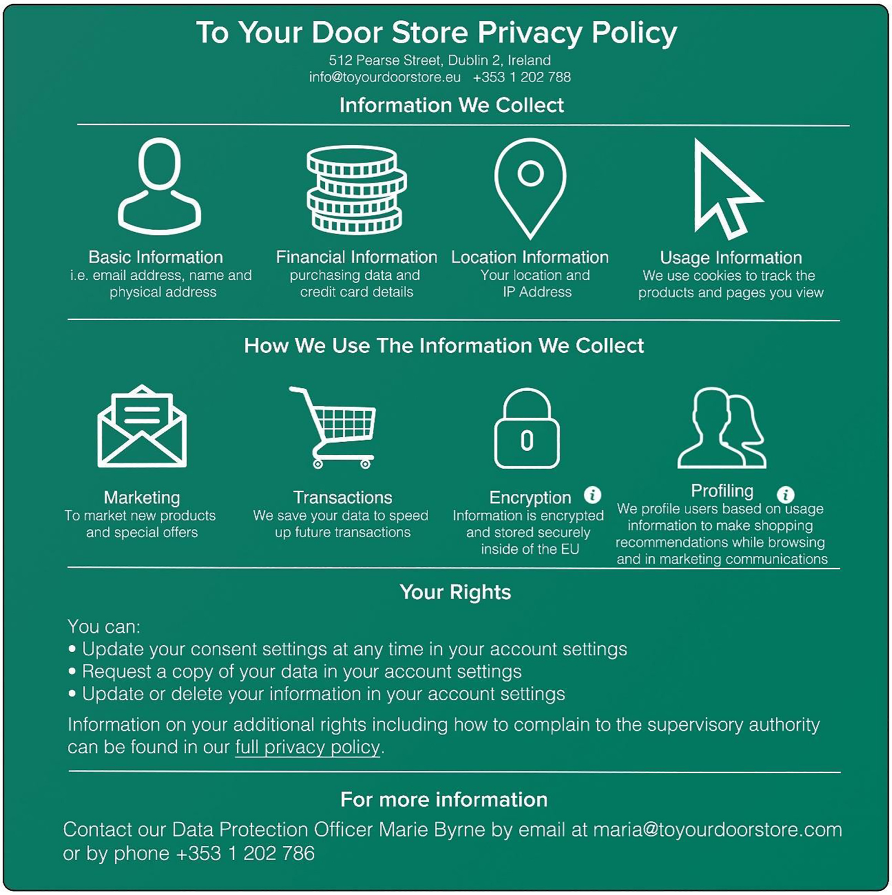
Figure 1.
Icon-based GDPR-compliant privacy label with consent mechanisms

Both labels are icon-based; however, the label depicted in Figure 1 includes consent mechanisms to allow users to toggle on and off and provide explicit consent for different activities. The second label, depicted in Figure 2, is a static icon label without consent mechanisms. This enables the examination of the influence of consent mechanisms on individuals' perceptions. For more information on the label development (see Fox *et al.*, 2018).

3. Study 1: privacy labels and consumer privacy perceptions

3.1 Study 1: theoretical background

CPM theory is a rule-based theory, which uses a boundary metaphor to describe how consumers determine what information to disclose to what parties (Petronio, 2012). CPM was traditionally leveraged to study personal information disclosure in interpersonal relationships such as marital relationships (Petronio, 2012), but has been extended to online contexts such as social media (Wang *et al.*, 2019; Liu and Wang, 2018) and individual–



To Your Door Store Privacy Policy

512 Pearse Street, Dublin 2, Ireland
info@toyourdoorstore.eu +353 1 202 788

Information We Collect

Basic Information
i.e. email address, name and physical address

Financial Information
purchasing data and credit card details

Location Information
Your location and IP Address

Usage Information
We use cookies to track the products and pages you view

How We Use The Information We Collect

Marketing
To market new products and special offers

Transactions
We save your data to speed up future transactions

Encryption ⓘ
Information is encrypted and stored securely inside of the EU

Profiling ⓘ
We profile users based on usage information to make shopping recommendations while browsing and in marketing communications

Your Rights

You can:

- Update your consent settings at any time in your account settings
- Request a copy of your data in your account settings
- Update or delete your information in your account settings

Information on your additional rights including how to complain to the supervisory authority can be found in our full privacy policy.

For more information

Contact our Data Protection Officer Marie Byrne by email at maria@toyourdoorstore.com or by phone +353 1 202 786

Figure 2. Icon-based GDPR-compliant privacy label with no consent mechanisms (static)

organization relationships in E-commerce (Xu *et al.*, 2011; Metzger, 2007) and digital services (Karwatzki *et al.*, 2017).

CPM consists of three elements: boundary rule formation, coordination and turbulence (Petronio, 2012). As consumers own their personal information, they have the right to control how it is shared and used (Petronio, 2012). Under this principle, consumers decide what data to disclose based on their perception of their current level of privacy (Chang *et al.*, 2018; Xu *et al.*, 2011). In other words, individuals decide to transact with the organization if they feel that they currently possess their desired level of privacy. Individuals form rules to manage the sharing and withholding of their personal information (boundaries) based on five criteria: gender, culture, context, perceptions of costs and benefits and motivation (Petronio, 2012). Recent research has focused on the contextual nature of rule formation and the cost–benefit privacy calculus studying the role of perceived risk and control (Xu *et al.*, 2011).

When an individual discloses information in an interpersonal context such as when transacting with E-commerce vendors, they are defining a collective boundary, under which this personal information is coowned by the individual and organization (Petronio, 2012). This involves a degree of vulnerability due to the risk the information may be misused

(Metzger, 2007). It is thus important to develop mutually agreed privacy rules to guide how the information in the collective boundary can be shared and used (Petronio, 2012). When deciding to share information with an online organization, the consumer must be comfortable with how the organization will collect and utilize their personal data. If mutually agreed privacy rules are not defined, privacy (boundary) turbulence can occur and information can be used in a way that the individual is uncomfortable with (Petronio, 2012). When transacting with an online organization, privacy rules are developed through privacy policies (Chang *et al.*, 2018).

CPM represents a suitable lens for this study as the aim is to understand how individuals form a collective privacy boundary with a new organization, while exploring the role of risk and control-based variables (Xu *et al.*, 2011). As individuals' perceptions are influenced by their past experience and the specific context, we follow the approach of previous research (Chang *et al.*, 2018; Xu *et al.*, 2011) and focus on consumers' perceptions of risk and control in the situational context of E-commerce. According to CPM, individuals are likely to assess the risk and control associated with data disclosure prior to determining their level of perceived privacy and deciding whether to create a collective privacy boundary and share data (Xu *et al.*, 2011; Petronio, 2012). CPM posits that individuals define privacy boundaries based on their preexisting perceptions as well as boundary coordination in new situations such as transacting with an E-commerce vendor. Indeed, when harnessing CPM, Wang *et al.* (2019) assert that individuals' privacy perceptions are not static and may be highly influenced by institutional assurances such as privacy policies. Thus, we adopt a different approach to prior work (Chang *et al.*, 2018; Xu *et al.*, 2011) and include both general perceptions related to privacy online and situational perceptions related to the E-commerce vendor.

3.2 Study 1: model development

As illustrated in our research model below (see Figure 3), this study considers individuals' preexisting perceptions of privacy, control and risk associated with privacy disclosure online as a representation of existing privacy boundaries. We propose that the privacy label represents the boundary coordination process and the development of agreed privacy rules for the use of information shared with the E-commerce vendor. We argue that boundary coordination will impact individuals' perceptions of risk, control and privacy related to the E-commerce vendor.

Disclosure of information inherently involves a level of risk (Metzger, 2007), and the online transaction environment can heighten consumers' risk perceptions (Chang *et al.*, 2016). In this study, perceived privacy risk is described as an individual's expectation that disclosing personal information to an E-commerce vendor will result in a negative outcome (Dinev *et al.*, 2013). CPM posits that individuals will not disclose information if they believe a negative outcome is likely to occur (Petronio, 2012). Prior research has supported the negative relationship between perceived Internet privacy risk and willingness to transact with E-commerce websites (Chang *et al.*, 2016). Thus, we argue that it is important to consider individuals' held beliefs regarding privacy risk associated with online transactions and their newly formed beliefs of privacy risks associated with an E-commerce vendor. We posit that individuals' general perceptions of risk online can be partly appeased through boundary coordination, leading to lower perceptions of risk regarding the E-commerce vendor. Extant research has evidenced the potential written privacy policies to reduce perceptions of risk associated with a website (Pan and Zinkhan, 2006; Miyazaki and Fernandez, 2000) or mobile application (Libaque-Sáenz *et al.*, 2021) and perceived effectiveness of the privacy policy to reduce privacy risk (Wang *et al.*, 2019). The privacy label details the company's privacy practices and is thus likely to lead to lower perceptions of risk.

H1. The GDPR privacy label will negatively impact (reduce) end-user perceptions of privacy risk associated with the e-commerce vendor.

Perceived control is a core concept in privacy research, with many definitions and theories highlighting the role of control. However, privacy and control are conceptually distinct (Laufer and Wolfe, 1977) and negatively correlated. Control is a perception-based variable defined as an individual's beliefs in their ability to manage the collection and use of their personal data (Dinev *et al.*, 2013; Xu *et al.*, 2011). Lack of control can heighten privacy concerns (Dinev and Hart, 2004). Under CPM, it can be posited that if individuals believe the control communicated via privacy assurances is insufficient, they may be unwilling to disclose information to the organization. Conversely, strong perceptions of control may empower consumers to share more information. Prior research has found perceived effectiveness of privacy policies positively impacted control perceptions (Mutimukeye *et al.*, 2020; Xu *et al.*, 2011). As the privacy label represents a means of informing individuals how they can control the use of their information disclosed within the privacy boundary, the label will foster perceived control regarding the E-commerce vendor.

Recent research has proposed that online organizations should request explicit consent from consumers regarding the collection and use of their data (Bradlow *et al.*, 2017). Explicit consent is also required under the GDPR. The consent-based label enables consumers to decide how their data can be used via a toggle function, whereas the static label informs consumers of the different types of control they have. As individuals in the consent-based label condition can determine the privacy rules and exercise control, we argue this label will have a stronger influence on perceived control.

H2. The GDPR privacy label will positively impact (increase) end-user perceptions of control over their private information associated with the e-commerce vendor.

While many studies measure privacy concerns as a proxy for privacy, privacy concerns have a negative connotation and do not directly represent privacy (Dinev *et al.*, 2013). Thus, we focus on perceived privacy. Privacy is defined as "an individual's self-assessed state in which external agents have limited access to information about him or her" (Dinev *et al.*, 2013, p. 299). CPM posits that individuals reflect on their perceptions of risk and control prior to determining the level of privacy they will be afforded if they disclose their data (Petronio, 2012). Individuals hold general perceptions of their level of privacy when transacting online, formed from their risk–benefit calculation and past experience. However, boundary coordination via privacy labels can establish agreeable rules for the use of information. Upon viewing the privacy label, it is argued that individuals will hold high perceptions of privacy. In other words, individuals will believe the data shared within the collective boundary will remain private, in that they will co-own it and have the ability to control its use. Additionally, we argue that explicit control offered by the consent-based label will have a stronger effect on perceived privacy.

H3. The GDPR privacy label will positively impact (increase) end-user perceptions of privacy associated with the e-commerce vendor. The effect will be stronger for the consent-based label.

3.3 Study 1: methodology

Following the approach of other studies in this context, an online experiment was developed (Soumelidou and Tsohou, 2019; Tsai *et al.*, 2011) with participants randomly assigned to one version of the privacy label (consent or static). The survey included four sections: A. prelabel exposure (T1), participants' general perceptions of privacy, control and privacy risk were examined. B. Control variables gender, age, education level, privacy invasion experience, regulatory expectations and GDPR awareness were examined. C. Participants were instructed to imagine they were considering signing up to a new E-commerce website and were presented with the label. D. Postexposure (T2), individuals' perceptions of privacy, risk and control specific to the fictional website were measured. All items were adapted from validated measures. General and specific perceptions of control and privacy were adapted from Dinev *et al.* (2013) using four and three items, respectively. Perceived privacy risk was measured with four items from Dinev and Hart (2006). The survey was pretested among a sample of citizens to ensure all items were clear and unambiguous.

The online questionnaire was distributed on Qualtrics with participants of varying gender, age, education levels and employment status included. All participants were from native English-speaking countries within the EU, namely Ireland and the United Kingdom. A total of 389 participants commenced the survey. The data were screened and cleaned, and incomplete responses and responses failing the attention check were dropped resulting in 349 responses. Participants were assigned equally across conditions but after data cleaning, consent label $n = 182$ and static label $n = 167$. A series of independent *t*-tests to confirm random assignment revealed no significant differences across all control variables. The demographic characteristics of the sample are illustrated in Appendix 1.

3.4 Study 1: data analysis

All variables met skewness and kurtosis requirements of ±2.2. Preliminary analyses to explore validity, reliability and test for common method variance (CMV) were conducted in AMOS v25. The proposed model fit was explored using confirmatory factor analysis (CFA) in AMOS. The six-factor model with T1 and T2 variables demonstrated strong fit meeting recommended fit thresholds; cmin/df: 2.451, CFI: 958, RMSEA: 0.065, SRMR: 0.0654 (Hair *et al.*, 2010).

As shown in Table 1, the AVE for each construct was above 0.50, indicating convergent validity (Hair *et al.*, 2010). The square root of the AVE was greater than the interfactor correlations, indicating discriminant validity for all factors (Fornell and Larcker, 1981). The reliability of constructs was tested by calculating the composite reliability (CR). All constructs were reliable with CR scores exceeding 0.70 (Bagozzi *et al.*, 1991). Table 1 also shows that some correlation coefficients are quite high suggesting potential multicollinearity. In order to check whether multicollinearity represents an issue in our dataset, we assessed the variance inflation factors (VIFs) using the stringent 5.0 threshold for reflective constructs (Kline, 1998; Kock and Lynn, 2012). The results of the analysis are reported in Appendix 2 and show that the VIFs for all constructs are below the threshold; therefore, the results of our analysis are not affected by multicollinearity. The testing of endogenous and exogenous

Table 1. Composite reliability, AVE, square root of AVE and correlation between constructs (study 1)

Constructs	CR	AVE	PCT1	PPT1	PRT1	PCT2	PPT2	PRT2
Perceived control T1 (PCT1)	0.92	0.73	**0.86**					
Perceived privacy T1 (PPT1)	0.90	0.74	*0.65****	**0.86**				
Perceived risk T1 (PRT1)	0.87	0.60	*−0.27****	*−0.47****	**0.79**			
Perceived control T2 (PCT2)	0.92	0.75	*0.41****	*0.36****	*−0.14**	**0.86**		
Perceived privacy T2 (PPT2)	0.89	0.73	*0.33****	*0.41****	*−0.17***	*0.77****	**0.85**	
Perceived risk T2 (PRT2)	0.92	0.74	*0.03*	*−0.04*	*0.37****	*−0.32****	*−0.32****	**0.86**

Note(s): The values in bold are square roots of AVE. Values in italic are correlation coefficients. ***$p < 0.001$; **$p < 0.01$

variables simultaneously can foster concerns regarding common method variance (CMV). In order to reduce such concerns, procedural and statistical remedies were implemented as recommended by Podsakoff *et al.* (2003). More specifically, these included promising full confidentiality and ensuring all items were unambiguous (Podsakoff *et al.*, 2003). To statistically test for CMV, the common latent factor approach (CLF) was followed as this was identified by Podsakoff *et al.* (2003) as the optimal method for research settings where predictor and criterion variables cannot be collected from different sources or in different contexts and where the source of CMV cannot be identified. A CLF was added to the CFA, and the standardized regression weights were compared before and after adding the CLF. As none of the items experienced a notable change, CMV was not a concern. Composites were imputed for subsequent analyses in SPSS (Gaskin, 2012).

3.4.1 Hypotheses testing. Hypotheses were tested in SPSS using a series of repeated measures ANOVAs (RMANOVA). The purpose of the RMANOVA is to test whether the average value of the dependent variable varies across different measurement intervals (Huck, 2012). As such, this method is suitable for detecting within-subject change in dependent variables (Huck, 2012). In this study, we examine the within-subject change in perceptions of privacy, control and risk between prelabel and postlabel conditions. We also investigate any differences between individuals in both conditions. The Type 1 error rate was set at 0.05. H1 proposed individuals would express lower perceptions of risk after exposure to the label. The results of the RMANOVA provided support for H1. A significant interaction effect between time and label condition was found (Wilks' Lambda = 0.990, F = 3.45, p < 0.10). Changes across conditions over time are shown in Figure 4, which shows both labels reducing perceived risk. Post-hoc independent t-tests revealed there were no significant differences in perceived risk between label conditions at T1 (t = 0.807, p > 0.05). At T2, those in the consent condition expressed lower perceptions of risk, but the difference was not significant (t = − 1.105, p > 0.05).

H2 proposed that individuals would express higher perceptions of control after exposure, and this effect would be stronger in the consent-based label condition. The results provided support for H2 (Figure 5). A significant interaction effect between time and label condition was found (Wilks' Lambda = 0.947, F = 19.34, p < 0.001). Changes across conditions over time are shown in Figure 5, with both labels increasing perceptions of control. Post-hoc independent t-tests revealed that the mean between both conditions was approaching significance for perceived control at T1 (t = −1.944, p < 0.10) with those in the static label condition expressing slightly higher perceived control. At T2, those in the consent label condition expressed significantly higher perceptions of control (t = 2.362, p < 0.05), indicating that this approach was more effective in increasing perceived control.

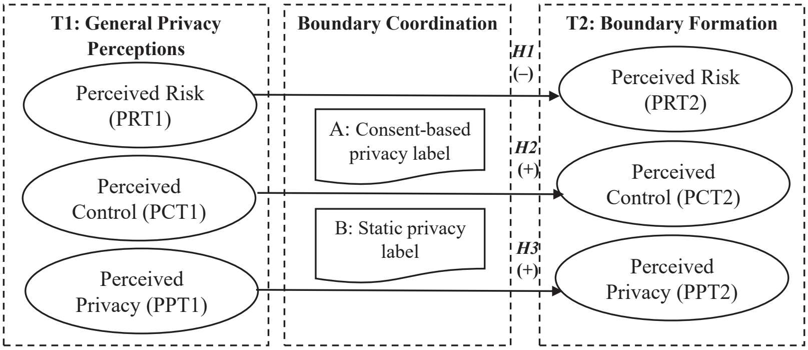


Figure 3.
Study 1 model

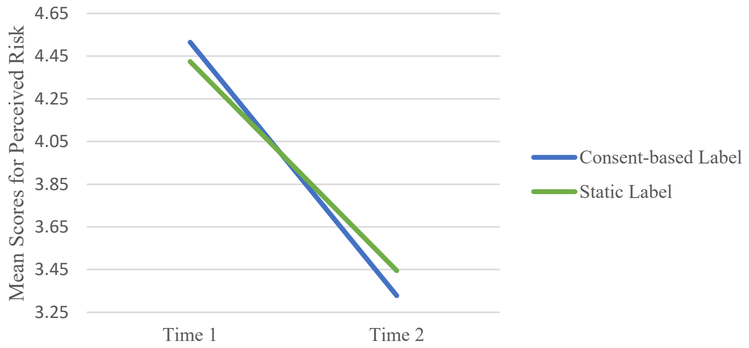


Figure 4.
Change in perceived risk Pre (time 1) and post exposure (time 2)

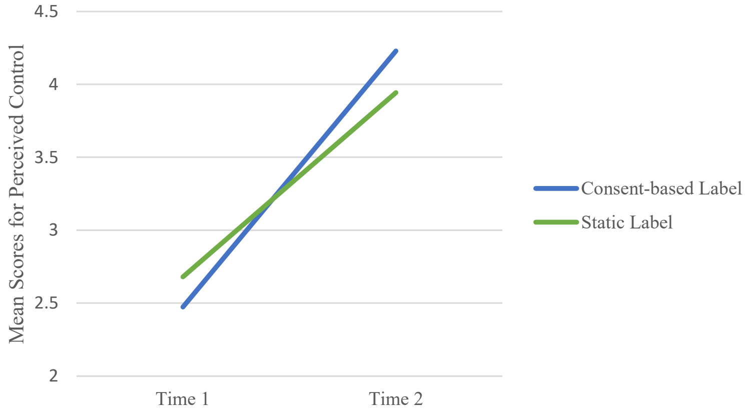


Figure 5.
Change in perceived control pre (time 1) and post exposure (time 2)

H3 proposed individuals would express higher perceptions of privacy after exposure, and this effect would be stronger for the consent-based label condition. The results provided support for H3 (Figure 6). A significant interaction effect between time and label condition was found (Wilks' Lambda = 0.971, F = 10.50, p < 0.001). Between person effects were approaching significance (F: 3.28, p < 0.10). Changes across conditions over time are shown in Figure 6. While both labels increased individuals' perceptions of privacy, participants viewing the consent-based label expressed higher privacy perceptions. Post-hoc independent t-tests revealed that the mean between both conditions was not significant at T1 (t = –0.003, p > 0.05). At T2, those in the consent label condition expressed significantly higher perceptions of privacy (t = 2.911, p < 0.01).

4. Study 2: privacy labels, consumer trust and intentions

4.1 Study 2: theoretical background

Study 2 moves beyond the formation of privacy perceptions to examine the influence of these perceptions on trust and intentional behaviors (Dinev *et al.*, 2013). In classical privacy calculus theory, risks and benefits are independently assessed and then weighted against each other (Dinev and Hart, 2006). In contrast, CPM considers the dynamics between the variables operationalized in the privacy calculus (Karwatzki *et al.*, 2017) and extended privacy calculus, namely trust (Dinev and Hart, 2006). Furthermore, the creation of shared disclosure boundaries

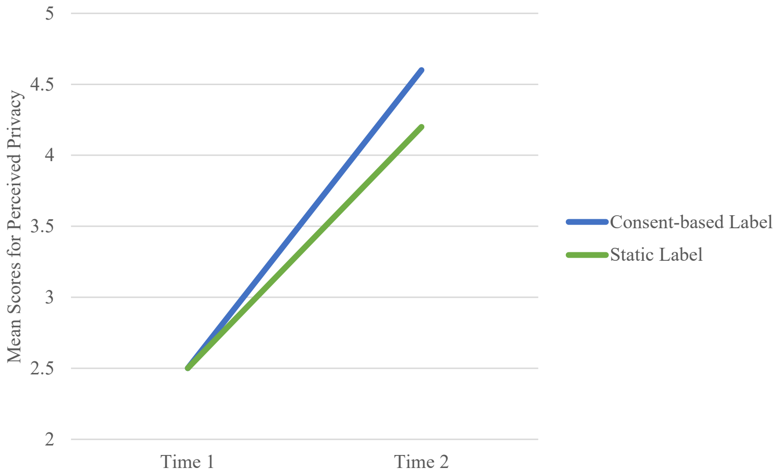


Figure 6.
Change in perceived privacy pre (time 1) and post exposure (time 2)

with organizations involves some vulnerability on the individual's behalf (Metzger, 2007), and the foundation of trust is the acceptance of vulnerability (McKnight *et al.*, 2002). Furthermore, the creation of shared disclosure boundaries with organizations involves some vulnerability on the individual's behalf (Metzger, 2007), and the foundation of trust is the acceptance of vulnerability (McKnight *et al.*, 2002). The privacy label again represents the boundary coordination process. It can be argued that individuals may be unwilling to transact with the organization unless they deem privacy practices trustworthy (Pan and Zinkhan, 2006). The privacy label represents a means of communicating privacy practices to consumers to engender trust and encourage a transactional relationship as a result.

4.2 Study 2: model development

Trust is fundamental to E-commerce (Gefen *et al.*, 2003) and transactional relationships (Chang *et al.*, 2016). However, the existing literature is rife with differing approaches to measuring trust online (Bélanger *et al.*, 2002) with some studies examining trust as a general belief in the vendor and others viewing trust as a set of beliefs (Gefen *et al.*, 2003). Trust in this study relates to an individual's willingness to be vulnerable when transacting with an E-commerce vendor (McKnight *et al.*, 2002) and their perception of the organization's dependability with their personal data (Mutimukeye *et al.*, 2020). Individuals' willingness to trust is based on their beliefs of the organization's benevolence, integrity and competence (Gefen *et al.*, 2003). Benevolence is the belief the organization has the individual's best interests in mind, integrity refers to belief in the morals and principles of the organization, and competence is the belief the organization has the knowledge and skills to transact online (Bélanger *et al.*, 2002).

Trust is typically developed over time as opposed to being formed based on a one-time interaction (Gefen *et al.*, 2008). Thus, it can be difficult to build trust in the online context, particularly for unknown organizations (van der Werff *et al.*, 2019). Over time, individuals are likely to form perceptions of the trustworthiness of the institutional environment, that is, the Internet, which may influence their perceptions of the trustworthiness of a specific vendor (McKnight *et al.*, 2002). Thus, E-commerce vendors must develop mechanisms to build initial trust based on consumers' first interaction with the website (Gao *et al.*, 2017). The privacy label represents a method for organizations to communicate their trustworthiness to consumers. Research has shown that privacy policies can improve perceptions of trustworthiness of an E-commerce vendor (Mutimukeye *et al.*, 2020; Wu *et al.*, 2012).

Extant research has explored the negative correlates between trust and privacy variables with studies finding that online privacy concerns reduced trust in online organizations (e.g. Kim, 2008; Hong and Thong, 2013), and perceived risk negatively impacted Internet trust (Dinev *et al.*, 2013). However, there is a need for further examination of positive privacy correlates and trust. Study 1 found that the privacy label fostered perceived control among consumers. Privacy assurances can potentially lead individuals to form positive perceptions related to privacy and control and heighten individuals' beliefs in the trustworthiness of the E-commerce vendor (Culnan and Armstrong, 1999) as well as social networking and e-government sites (Mutimukeye *et al.*, 2020). Moreover, offering clear privacy controls can enhance trust perceptions among consumers (Aïmeur *et al.*, 2016). It is therefore conceivable that individuals' perceived control post label exposure will influence their perception of the E-commerce vendor's trustworthiness.

> *H4*. Perceived control over their private information by the end user will positively impact the end user's perception of the trustworthiness of the e-commerce vendor.

Research found that perceived privacy positively impacted perceived trust in the online environment (Joinson *et al.*, 2010). Upon viewing the GDPR label, if individuals believe they maintain some privacy, they are more likely to view the organization as trustworthy and be willing to create a shared boundary.

> *H5*. Perceived privacy by an end user will positively impact the end user's perception of the trustworthiness of the e-commerce vendor.

Willingness to transact is described as a consumer's intention to engage in commerce transactions with an organization through its website (Kim, 2008). It has been argued that trust in the form of specific beliefs regarding an E-commerce vendor is an antecedent to participation in the online environment (Gefen *et al.*, 2003) as if individuals hold positive beliefs regarding the benevolence, integrity and competence of the E-commerce vendor, they will express positive intentions toward interacting with them. Research has found that trust in the Internet (Kim, 2008; Dinev and Hart, 2006) and the Internet as a transaction channel (Kim *et al.*, 2016) can positively impact willingness to transact online, and cognitive trust can positively influence purchase intention (Chang *et al.*, 2016). It is important to explore this relationship in the context of specific trust perceptions and transactional intentions. We argue that perceived trustworthiness will leave consumers amenable to transacting with the E-commerce vendor, due to the belief the privacy rules outlined in the label will be upheld.

When consumers believe their personal data will not be protected, they may engage in privacy-protective behaviors such as falsifying data disclosed (Son and Kim, 2008). It is conceivable to argue that the privacy label and the perceptions of trust it engenders will impact individuals' willingness to disclose accurate data. Prior research has supported the link between general trust in the Internet and willingness to disclose information online (Joinson *et al.*, 2010) and to online vendors (Wu *et al.*, 2012). We argue that in the context of E-commerce vendors, if individuals believe the privacy rules will be upheld, they will see no cause to falsify or withhold data. We thus, present the following hypothesis:

> *H6*. End-user perceptions of the trustworthiness of the e-commerce vendor will positively impact the end user's intentions to (a) transact with the e-commerce vendor, and (b) disclose accurate information.

4.3 Study 2: methodology

All the constructs included in the model were measured postexposure (T2) (see Figure 7). Perceptions of privacy and control were measured as per Study 1. Perceived trustworthiness of the E-commerce vendor was measured with nine items representing benevolence, integrity and competence from McKnight *et al.* (2002). Intention to transact was measured with four items based on Bian and Forsythe (2012), and willingness to disclose accurate data was measured with two items from Wang *et al.* (2004). The survey was pilot tested and amended accordingly. The online questionnaire was distributed on Qualtrics to recruit participants from the United Kingdom and Ireland. Approximately 325 participants commenced the survey. All incomplete responses were dropped resulting in 270 responses, 135 in each condition. Independent *t*-tests revealed no significant differences between both conditions.

4.4 Study 2: data analysis

The sample characteristics are illustrated in Appendix 1. All variables met skewness and kurtosis requirements. As shown in Table 2, convergent validity and discriminant validity thresholds were met for all constructs. All constructs also indicated reliability with CR scores exceeding 0.70. Similar to study 1, there is evidence of strong correlation between some of the constructs, so we assessed the VIF of the dependent variables included in our model to make sure that multicollinearity did not affect the results of our SEM. The results of this analysis are presented in Appendix 2 and show that all VIFs were below the critical threshold of 5 (Kline, 1998; Kock and Lynn, 2012) suggesting that multicollinearity does not represent an

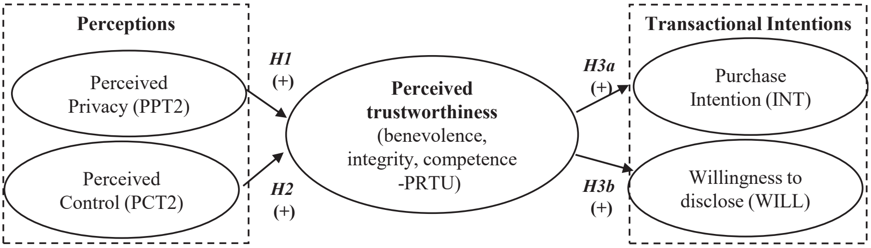


Figure 7. SEM model

Constructs	CR	AVE	T1PC	T2PC	T1PP	T2PP	INT	Will	PRTU
Perceived control T1 (PCT1)	0.93	0.78	**0.88**						
Perceived control T2 (PCT2)	0.95	0.81	*0.45****	**0.90**					
Perceived privacy T1 (PPT1)	0.93	0.81	*0.69****	*0.36****	**0.90**				
Perceived privacy T2 (PPT2)	0.95	0.86	*0.41****	*0.81****	*0.56****	**0.93**			
Purchase intention (INT)	0.95	0.83	*0.32****	*0.65****	*0.39****	*0.75****	**0.91**		
Willingness to disclose (WILL)	0.88	0.78	*0.26****	*0.48****	*0.33****	*0.57****	*0.59****	**0.89**	
Perceived trustworthiness (PRTU)	0.98	0.93	*0.43****	*0.73****	*0.45****	*0.81****	*0.79****	*0.71****	**0.96**

Note(s): The values in bold are square roots of AVE. Values in italic are correlation coefficients. ***$p < 0.001$

Table 2. Composite reliability, AVE, square root of AVE and correlation between constructs (study 2)

issue in our dataset. We also examined factors cross-loading (Appendix 4), and the scores are smaller than the item loadings on their corresponding constructs providing further assurance of satisfactory discriminant validity. The proposed model fit was explored using CFA in AMOS. Perceived trustworthiness (PTRU) was modeled as a second-order factor with three first-order dimensions (benevolence, integrity, competence). The proposed seven-factor model with T1 and T2 variables demonstrated strong fit meeting recommended fit thresholds (Hair *et al.*, 2010): cmin/df: 2.383, CFI: 943, RMSEA: 0.072, SRMR: 0.04. CMV was explored using the CLF approach. As no notable changes were found after the addition of the CLF, CMV was not a concern, and composites were imputed for subsequent analyses.

4.4.1 Hypotheses testing. The proposed model was tested using structural equation modeling (SEM) in AMOS. The model was tested across the two label conditions to explore differences based on condition. The structural model demonstrated strong fit (cmin/df:2.306, CFI: 0.98, RMSEA: 0.070, SRMR: 0.019). The results are visualized in Figure 8. H4 proposed a positive relationship between perceived control and perceived trustworthiness of the E-commerce vendor. This relationship was significant and positive across both groups (consent-based: $\beta = 0.220, p < 0.01$, static: $\beta = 0.217$ $p < 0.05$), supporting H4. In H5, a positive relationship between perceived privacy and perceived trustworthiness was posited. The data provided strong support across both conditions (consent-based: $\beta = 0.669, p < 0.01$, static: $\beta = 0.629$ $p < 0.01$). H6a proposed that perceived trustworthiness would positively impact intentions to purchase from the E-commerce vendor. This was supported among both conditions (consent-based: $\beta = 0.818, p < 0.01$, static: $\beta = 0.807$ $p < 0.01$). Lastly, H6b posited that perceived trustworthiness would positively impact intentions to disclose accurate information. This was also supported (consent-based: $\beta = 0.759, p < 0.01$, static: $\beta = 0.721$ $p < 0.01$). Among the consent-label group, the model explained 73.2% of variance in perceived trustworthiness, 70.3% of variance in intention to transact and 58.3% of variance in willingness to disclose accurate data. The model for static label group explained 68% of variance in perceived trustworthiness, 65.9% of variance in transaction intention and 60.1% of variance in willingness to disclose data. Despite slightly higher variance explained and effect sizes among the consent-based label, there were no significant differences in the relationships between both groups.

Even though the model included variables to control for a range of demographics characteristics, endogeneity may still represent a potential bias in our model. To rule out this scenario, we adopted a Gaussian Copula Approach (Park and Gupta, 2012) as recommended by Hult *et al.* (2018). The results are presented in Appendix 5 and suggest that endogeneity is not an issue in our analysis.

In order to check the robustness of the proposed research model, an alternative model specification was tested, which included direct paths between perceived privacy and intention to transact (consent-based: $\beta = 0.433, p < 0.01$, static: $\beta = 0.722$ $p < 0.01$) and willingness to disclose (consent-based: $\beta = 0.393, p < 0.01$, static: $\beta = 0.549$ $p < 0.01$) and between perceived control and intention to transact (consent-based: $\beta = 0.296, p > 0.10$, static: $\beta = 0.128$ $p > 0.10$) and willingness to disclose (consent-based: $\beta = 0.158, p > 0.10$,

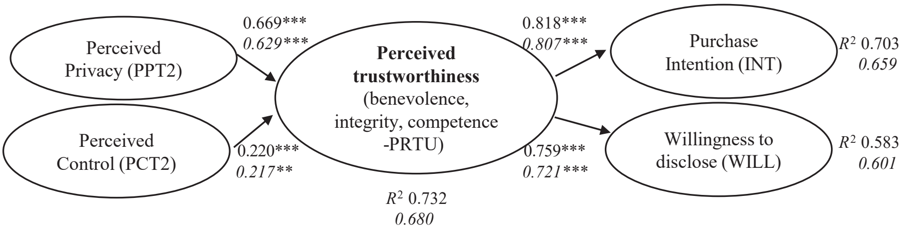


Figure 8.
Structural equation model results (values in *italic* refer to the static group)

static: $\beta = 0.111$ $p > 0.10$). Even though some of these paths are statistically significant, their inclusion in the model does not change our conclusions (see Appendix 6).

5. Discussion

Privacy assurances have been positioned as a means for organizations to overcome the negative impacts of consumers' diluted privacy perceptions (Xu *et al.*, 2011). Existing privacy assurance literature forms two categories; (1) research exploring potential new approaches, which overcome the weaknesses of privacy policies such as visualization techniques; and (2) research examining how consumers' perceptions of privacy policy effectiveness impact their privacy perceptions and behaviors. Our study contributes to both categories building upon privacy policy visualization approaches and exploring the efficacy of GDPR privacy labels in influencing privacy perceptions and intended behaviors. In terms of the first category, recent privacy regulation across Europe renders lengthy, FIPPs-based privacy policies unfit for purpose. Thus, we respond to calls for a simplified approach to privacy policies (Martin and Murphy, 2017) and develop GDPR privacy labels, which meet GDPR requirements for privacy notices and explicit consent. Our results strongly support the efficacy of privacy labels and thus further support studies advocating visualized privacy policies (e.g. Soumelidou and Tsohou, 2019; Kelley *et al.*, 2010).

Our study also contributes to our understanding regarding privacy assurances and three core privacy perceptions. First, the role of perceived risk has remained uncertain with recent research finding perceived effectiveness of privacy policies reduced risk perceptions for social networking and e-government sites, but not for E-commerce (Mutimukeye *et al.*, 2020), and written FIPPs policies did not significantly influence risk perceptions regarding mobile apps (Libaque-Sáenz *et al.*, 2021). Our study demonstrates the efficacy of the labels in reducing risk perceptions associated with E-commerce vendors. Second, the study builds upon recent work linking perceived effectiveness of written privacy policies and perceived control (Mutimukeye *et al.*, 2020; Xu *et al.*, 2011) and unravels the impact of implicit versus explicit consent mechanisms, highlighting that while both static and consent-based labels positively impact perceived control regarding the E-commerce vendor, this effect is significantly higher when explicit consent mechanisms are included. Third, research has found that perceived effectiveness of written privacy policies can reduce privacy concerns (Gong *et al.*, 2019). We extend this to the context of visualized labels and perceived privacy, an arguably more accurate proxy for privacy, and find that both labels positively heighten perceptions of privacy associated with the E-commerce vendor.

To examine the role of privacy labels within transactional relationships, we conducted a second study. The study extends knowledge on the role of trustworthiness and intentions to interact with E-commerce organizations and disclose accurate information (Chang *et al.*, 2016; Wu *et al.*, 2012) and demonstrates the potential of GDPR privacy labels as a mechanism for building this trust. Following label exposure, consumers' perceptions of control and privacy related to the E-commerce vendor positively influenced their perceptions of trustworthiness. This clarifies conflicting findings of Mutimukeye *et al.* (2020), who found that perceived control positively influenced trust in social networking and e-government sites but not E-commerce, and suggests visualized policies are more effective in developing this link between control and trustworthiness in this context. We also extend the findings of Joinson *et al.* (2010), who found perceived privacy influenced trust perceptions online, with perceived privacy enhancing perceived trustworthiness of the vendor in both conditions. For both labels, perceived trustworthiness positively impacted consumers' behavioral intentions toward the E-commerce vendor. Specifically, when consumers believe the E-commerce vendor is trustworthy, they are more likely to purchase from the retailer and disclose accurate personal data. This finding adds a possible explanation to recent contradictory findings on the relationship between transparency and information disclosure in Karwatzki *et al.* (2017), who proposed that transparency not only indicated fairness but highlighted privacy issues. We build upon these assertions and argue that transparency alone is not sufficient, but rather combining transparent communications with information on how individuals can exercise control will strengthen the rule formation aspect of boundary coordination and lead to greater information disclosure.

Our findings provide both contributions to theory and actionable insights for practice. The study extends CPM theory to the online retail context and provides support for its use to understand how individuals develop collective boundaries with an unknown E-commerce website. By providing insights into how individuals assess the control, risk and privacy associated with the E-commerce vendor, the study makes an important contribution to privacy literature around this decision-making (Chang *et al.*, 2018). In line with CPM (Petronio, 2012), this study shows that individuals consider control and risk when deciding whether to create a collective privacy boundary with E-commerce vendors. With GDPR labels, privacy rules for the use of data can be established in a manner that boosts consumers' privacy perceptions. If individuals believe they have control over data disclosed, the risk of negative outcomes is low, and they retain some privacy, they are more likely to possess positive views toward interacting with the organization (Chang *et al.*, 2018).

Previous research has explored how written privacy policies impact general perceptions of trustworthiness of the E-commerce vendor (Mutimukeye *et al.*, 2020). However, recent research highlights the importance of new approaches to privacy policies and calls out E-commerce as a context where data control can offer consumers the opportunity to determine what information disclosure is fair (Aïmeur *et al.*, 2016). To further understand the boundary coordination and formation process, this study positions privacy labels as a transparent privacy assurance approach for organizations to form a collective boundary with consumers and demonstrates the potential of this approach to trigger positive perceptions of the E-commerce vendor's benevolence, integrity and competence. Previous research investigated the impact of privacy policies on either consumer perceptions of the general Internet context and not a specific vendor or general perceptions of trust as opposed to the three dimensions, which comprise perceived trustworthiness. This study provides a greater understanding of the relationship between the interrelated privacy constructs in the E-commerce context and the influence of privacy labels as a method of boundary coordination, which impacts consumers' willingness to develop collective boundaries with organizations, within which they intend to transact and disclose accurate information.

Our study also offers important insights from a practical perspective and answers calls for research on effective privacy policy visualization (Soumelidou and Tsohou, 2019) and privacy policy research in the E-commerce context (Libaque-Sáenz *et al.*, 2021). Organizations face challenges in balancing the need to leverage consumer data with potential negative consequences of perceived disregard for consumers' privacy (Gerlach *et al.*, 2019). Indeed, privacy research has long grappled with recommendations around finding the ideal balance of transparency (Gerlach *et al.*, 2019) and communicating with consumers in ways that inform them of privacy practices without raising concern (Karwatzki *et al.*, 2017). We provide further support for studies advocating visualized privacy policies (e.g. Soumelidou and Tsohou, 2019) as a means to not just inform consumers and meet regulatory requirements, but by providing consumers with the level of control they desire through a user customizable privacy mechanism, and consequently build their privacy and trust perceptions. It is thus recommended that E-commerce vendors based within Europe and all vendors transacting with European citizens consider adopting the privacy label approach to communicate their privacy practices to current and potential customers. Researchers have called for the inclusion of explicit consent mechanisms in communications with consumers (Bradlow *et al.*, 2017). By including consent mechanisms in privacy labels, E-commerce vendors further their transparency and empower consumers with control over how their data are collected and used. This, in effect, provides e-commerce vendors and consumers with a mechanism to comanage consumer data as envisioned by Wang *et al.* (2019). Forging this sense of control not only enables E-commerce vendors to comply with regulation but reduces consumer privacy concerns, fosters a perception of privacy and potentially increases consumer privacy self-efficacy.

Commerce is increasingly distributed and transborder in nature. While the GDPR is one of the most significant international responses to governing transborder online activities and data privacy, it is not the only one. Many new regulatory regimes are adopting similar requirements to the GDPR, for example, Brazil's Lei Geral de Proteção de Dados (LGPD), South Africa's Protection of Personal Information Act (POPIA) and Canada's Personal Information Protection and Electronic Documents Act (PIPEDA). In some cases, such as the LGPD, these laws, like the GDPR, also have extraterritorial effect. International organizations will need to consider whether their approach to data privacy will be what Lyons (2019) calls "doing privacy right or doing privacy rights." In effect, organizations will need to decide on whether data privacy is merely a box-ticking exercise or something more values-driven and strategic. If the latter, it requires both an integrated approach and model of data privacy that reflects the lowest minimum threshold to comply with the highest regulatory requirements in the markets in which the organization operates directly or indirectly. Such an approach requires organizations to have a clear understanding of their financial, ethical, legal and societal (or stakeholder) responsibilities and a shift from control-based approaches to privacy to justice-based approaches (Greenaway *et al.*, 2015; Lyons, 2021). This is not an insignificant challenge but if successful, it may provide benefits, not least greater consumer trust and less privacy incidents (Accenture and Ponemon, 2015).

It is not sufficient for organizations to espouse these values of transparency and control using privacy labels, the policies and practices must be in place to uphold this level of privacy. Indeed, 57% of American adults lack confidence in organizations' following their privacy practices (Auxier *et al.*, 2019). It is thus imperative that good practices underpin those communicated in the label. The privacy label represents a mechanism for communicating the compliance of the organization and potentially differentiating from other organizations. Furthermore, organizations should consider implementing additional privacy assurances to support the purchasing journey and act as trust cues. Informational callouts on why certain personal data are required, for example, may serve to deepen perceptions of trustworthiness and privacy.

5.1 Limitations and future research

While this study advances current knowledge on privacy policy visualization and consumer perceptions, there are limitations, which could be explored through future research. First, the sample is from the United Kingdom and Ireland. This decision was intentional and follows previous studies by studying one or similar cultures (Xu *et al.*, 2011). Furthermore, no study to date has explored the influence of privacy assurance tools among European samples. Second, the privacy labels only represent one instantiation of the label, as it would be impossible to include all potential options. Future research could untangle different instantiations of the privacy label and their impacts on consumer perceptions. Third, the privacy labels are based on the GDPR and not FIPPs. FIPPs represent the prevailing approach of privacy policies in the USA. Firstly, the GDPR enshrines the principles of FIPPs in law. Secondly, we argue that the GDPR label represents both an ethical approach for organizations irrespective of location and regulatory compliance for many organizations given the broad territorial scope of the GDPR. It would be interesting to explore GDPR privacy labels among a US sample as it offers more control and transparency than mandated, thus potentially offering further exploration of theories of justice in contrast to merely theories of control. This work illuminates additional avenues for future research such as comparing the impact of GDPR privacy labels on privacy perceptions in different contexts including sensitive health products (Chang *et al.*, 2018).

6. Conclusion

Privacy represents a challenge for organizations and consumers alike, which is only complicated by continual advances in technology and recently introduced stringent regulation. Existing methods to communicate with consumers fail to foster positive privacy perceptions and are not compliant. The GDPR privacy label approach provides an important tool for enabling organizations to be compliant and educate consumers on their privacy practices thereby boosting perceived privacy, control and trustworthiness and paving the way for a positive customer–organization relationship.

References

Accenture and Ponemon (2015), "How global organizations approach the challenge of protecting personal data", available at: http://www.ponemon.org/local/upload/file/ATC_DPP%20report_FINAL.pdf (accessed November 2021).

Aïmeur, E., Lawani, O. and Dalkir, K. (2016), "When changing the look of privacy policies affects user trust: an experimental study", *Computers in Human Behavior*, Vol. 58, pp. 368-379.

Auxier, B., Rainie, L., Anderson, M., Perrin, A., Kumar, M. and Turner, E. (2019), "Americans and privacy: concerned, confused and feeling lack of control over their personal information", available at: https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/ (accessed May 2020).

Awad, N.F. and Krishnan, M.S. (2006), "The personalization privacy paradox: an empirical evaluation of information transparency and the willingness to be profiled online for personalization", *MIS Quarterly*, Vol. 30, pp. 13-28.

Bagozzi, R.P., Yi, Y. and Phillips, L.W. (1991), "Assessing construct validity in organizational research", *Administrative Science Quarterly*, Vol. 36 No. 3, pp. 421-458.

Bélanger, F., Hiller, J.S. and Smith, W.J. (2002), "Trustworthiness in electronic commerce: the role of privacy, security, and site attributes", *The Journal of Strategic Information Systems*, Vol. 11 Nos 3-4, pp. 245-270.

Bian, Q. and Forsythe, S. (2012), "Purchase intention for luxury brands: a cross cultural comparison", *Journal of Business Research*, Vol. 65 No. 10, pp. 1443-1451.

Bradlow, E.T., Gangwar, M., Kopalle, P. and Voleti, S. (2017), "The role of big data and predictive analytics in retailing", *Journal of Retailing*, Vol. 93 No. 1, pp. 79-95.

Chang, S.H., Chih, W.H., Liou, D.K. and Yang, Y.T. (2016), "The mediation of cognitive attitude for online shopping", *Information Technology and People*, Vol. 29 No. 3, pp. 618-646.

Chang, Y., Wong, S.F., Libaque-Sáenz, C.F. and Lee, H. (2018), "The role of privacy policy on consumers' perceived privacy", *Government Information Quarterly*, Vol. 35 No. 3, pp. 445-459.

Culnan, M.J. and Armstrong, P.K. (1999), "Information privacy concerns, procedural fairness, and impersonal trust: an empirical investigation", *Organization Science*, Vol. 10 No. 1, pp. 104-115.

Dinev, T. and Hart, P. (2004), "Internet privacy concerns and their antecedents-measurement validity and a regression model", *Behaviour and Information Technology*, Vol. 23 No. 6, pp. 413-422.

Dinev, T. and Hart, P. (2006), "An extended privacy calculus model for e-commerce transactions", *Information Systems Research*, Vol. 17 No. 1, pp. 61-80.

Dinev, T., Xu, H., Smith, J.H. and Hart, P. (2013), "Information privacy and correlates: an empirical attempt to bridge and distinguish privacy-related concepts", *European Journal of Information Systems*, Vol. 22 No. 3, pp. 295-316.

Eastlick, M.A., Lotz, S.L. and Warrington, P. (2006), "Understanding online B-to-C relationships: an integrated model of privacy concerns, trust, and commitment", *Journal of Business Research*, Vol. 59 No. 8, pp. 877-886.

Fornell, C. and Larcker, D.F. (1981), "Evaluating structural equation models with unobservable variables and measurement error", *Journal of Marketing Research*, Vol. 18 No. 1, pp. 39-50.

Fox, Grace, Tonge, Colin, Lynn, Theo and Mooney, John (2018), "Communicating compliance: developing a GDPR privacy label", *24th Americas Conference on Information Systems, New Orleans, Louisiana..*

Gaskin, J. (2012), "Confirmatory factor analysis", available at: http://statwiki.kolobkreations.com/index.php?title=Confirmatory_Factor_Analysis (accessed March 2020).

Gefen, D., Benbasat, I. and Pavlou, P. (2008), "A research agenda for trust in online environments", *Journal of Management Information Systems*, Vol. 24 No. 4, pp. 275-286.

Gefen, D., Karahanna, E. and Straub, D.W. (2003), "Trust and TAM in online shopping: an integrated model", *MIS Quarterly*, Vol. 27 No. 1, pp. 51-90.

Gerlach, J.P., Eling, N., Wessels, N. and Buxmann, P. (2019), "Flamingos on a slackline: companies' challenges of balancing the competing demands of handling customer information and privacy", *Information Systems Journal*, Vol. 29 No. 2, pp. 548-575.

Gong, X., Zhang, K.Z., Chen, C., Cheung, C.M. and Lee, M.K. (2019), "What drives self-disclosure in mobile payment applications? The effect of privacy assurance approaches, network externality, and technology complementarity", *Information Technology and People*, Vol. 33 No. 6, pp. 1174-1213.

Greenaway, K., Chan, Y. and Crossler, R. (2015), "Company information privacy orientation. A conceptual framework", *Information Systems Journal*, Vol. 25, pp. 579-606.

Gu, J., Xu, Y.C., Xu, H., Zhang, C. and Ling, H. (2017), "Privacy concerns for mobile app download: An elaboration likelihood model perspective", *Decision Support Systems*, Vol. 94, pp. 19-28.

Hair, J.F., Black, W.C., Babin, B.J. and Anderson, R.E. (2010), *Multivariate Data Analysis: A Global Perspective*, Pearson Education, New Jersey.

Hong, W. and Thong, J.Y. (2013), "Internet privacy concerns: an integrated conceptualization and four empirical studies", *MIS Quarterly*, Vol. 37 No. 1, pp. 275-298.

Huck, S.W. (2012), *Reading Statistics and Research*, Pearson Education, Boston, MA.

Hult, G.T.M., Hair, J.F. Jr, Proksch, D., Sarstedt, M., Pinkwart, A. and Ringle, C.M. (2018), "Addressing endogeneity in international marketing applications of partial least squares structural equation modeling", *Journal of International Marketing*, Vol. 26 No. 3, pp. 1-21.

ICO (2017), "Privacy notices, transparency and control. A code of practice on communicating privacy information to individuals", available at: https://ico.org.uk/for-organizations/guide-to-dataprotection/privacy-notices-transparency-and-control/ (accessed March 2019).

Joinson, A.N., Reips, U.D., Buchanan, T. and Schofield, C.B.P. (2010), "Privacy, trust, and self-disclosure online", *Human–Computer Interaction*, Vol. 25 No. 1, pp. 1-24.

Karwatzki, S., Dytynko, O., Trenz, M. and Veit, D. (2017), "Beyond the personalization–privacy paradox: privacy valuation, transparency features, and service personalization", *Journal of Management Information Systems*, Vol. 34 No. 2, pp. 369-400.

Kelley, P.G., Bresee, J., Cranor, L.F. and Reeder, R.W. (2009), "A nutrition label for privacy", *Proceedings of the 5th Symposium on Usable Privacy and Security*, Vol. 4, ACM.

Kelley, P.G., Cesca, L., Bresee, J. and Cranor, L.F. (2010), "Standardizing privacy notices: an online study of the nutrition label approach", *Proceedings of the SIGCHI Conference on Human factors in Computing Systems*, ACM, pp. 1573-1582.

Kim, D.J. (2008), "Self-perception-based versus transference-based trust determinants in computer-mediated transactions: a cross-cultural comparison study", *Journal of Management Information Systems*, Vol. 24 No. 4, pp. 13-45.

Kim, D.J., Yim, M.S., Sugumaran, V. and Rao, H.R. (2016), "Web assurance seal services, trust and consumers' concerns: an investigation of e-commerce transaction intentions across two nations", *European Journal of Information Systems*, Vol. 25 No. 3, pp. 252-273.

Kline, R.B. (1998), *Principles and Practice of Structural Equation Modeling*, The Guilford Press, New York, NY.

Kock, N. and Lynn, G. (2012), "Lateral collinearity and misleading results in variance-based SEM: an illustration and recommendations", *Journal of the Association for Information Systems*, Vol. 13 No. 7, pp. 546-580.

Laufer, R.S. and Wolfe, M. (1977), "Privacy as a concept and a social issue: a multidimensional developmental theory", *Journal of Social Issues*, Vol. 33 No. 3, pp. 22-42.

Libaque-Sáenz, C.F., Wong, S.F., Chang, Y. and Bravo, E.R. (2021), "The effect of fair information practices and data collection methods on privacy-related behaviors: a study of mobile apps", *Information and Management*, Vol. 58 No. 1, p. 103284.

Liu, C., Marchewka, J.T., Lu, J. and Yu, C.S. (2005), "Beyond concern—a privacy–trust-behavioral intention model of electronic commerce", *Information and Management*, Vol. 42 No. 2, pp. 289-304.

Liu, Z. and Wang, X. (2018), "How to regulate individuals' privacy boundaries on social network sites: a cross-cultural comparison", *Information and Management*, Vol. 55 No. 8, pp. 1005-1023.

Lyons, V. (2019), "Doing privacy right vs. doing privacy rights", in Fitzgerald, T. (Ed.), *CISO COMPASS: Navigating Cybersecurity Leadership Challenges with Insights from Pioneers*, 1st ed., CRC Press, Boca Raton, Florida, p. 389.

Lyons, V. (2021), "Justice vs control in cloud computing: a conceptual framework for positioning a cloud service provider's privacy orientation", in Lynn, T., Mooney, J.G., van der Werff, L. and Fox, G. (Eds), *Data Privacy and Trust in Cloud Computing*, Palgrave Macmillan, Cham, pp. 79-104.

Martin, K.D., Borah, A. and Palmatier, R.W. (2017), "Data privacy: effects on customer and firm performance", *Journal of Marketing*, Vol. 81 No. 1, pp. 36-58.

Martin, K.D. and Murphy, P.E. (2017), "The role of data privacy in marketing", *Journal of the Academy of Marketing Science*, Vol. 45 No. 2, pp. 135-155.

McKnight, D.H., Choudhury, V. and Kacmar, C. (2002), "Developing and validating trust measures for e-commerce: an integrative typology", *Information Systems Research*, Vol. 13 No. 3, pp. 334-359.

Metzger, M.J. (2007), "Communication privacy management in electronic commerce", *Journal of Computer-Mediated Communication*, Vol. 12 No. 2, pp. 335-361.

Miyazaki, A.D. and Fernandez, A. (2000), "Internet privacy and security: an examination of e-commerce vendor disclosures", *Journal of Public Policy and Marketing*, Vol. 19 No. 1, pp. 54-61.

Mousavi, R., Chen, R., Kim, D.J. and Chen, K. (2020), "Effectiveness of privacy assurance mechanisms in users' privacy protection on social networking sites from the perspective of protection motivation theory", *Decision Support Systems*, Vol. 135, 113323.

Mutimukeye, C., Kolkowska, E. and Grönlund, Å. (2020), "Information privacy in e-service: effect of organizational privacy assurances on individual privacy concerns, perceptions, trust and self-disclosure behavior", *Government Information Quarterly*, Vol. 37 No. 1, 101413.

Pan, Y. and Zinkhan, G.M. (2006), "Exploring the impact of online privacy disclosures on consumer trust", *Journal of Retailing*, Vol. 82 No. 4, pp. 331-338.

Park, S. and Gupta, S. (2012), "Handling endogenous regressors by joint estimation using copulas", *Marketing Science*, Vol. 31 No. 4, pp. 567-586.

Park, Y.J. and Jang, S.M. (2014), "Understanding privacy knowledge and skill in mobile communication", *Computers in Human Behavior*, Vol. 38, pp. 296-303.

Petronio, S. (2012), *Boundaries of Privacy: Dialectics of Disclosure*, SUNY Press, Albany, New York.

Podsakoff, P.M., MacKenzie, S.B., Lee, J.Y. and Podsakoff, N.P. (2003), "Common method biases in behavioral research: a critical review of the literature and recommended remedies", *Journal of Applied Psychology*, Vol. 88 No. 5, p. 879.

Railean, A. and Reinhardt, D. (2020), "OnLITE: on-line label for IoT transparency enhancement", *NordSec: Proceedings of the 25th Nordic Conference on Secure IT Systems*, Virtual Event, pp. 229-245.

Reeder, W.R., Kelley, P.G., McDonald, M.A. and Cranor, F.L. (2008), "A user study of the expandable grid applied to P3P privacy policy visualization", *WPES'08: Proceedings of the 7th ACM Workshop on Privacy in the Electronic Society*, New York, NY, pp. 45-54.

Ryngaert, C. and Taylor, M. (2020), "The GDPR as global data protection regulation?", *American Journal of International Law*, Vol. 114, pp. 5-9.

Son, J.Y. and Kim, S.S. (2008), "Internet users' information privacy-protective responses: a taxonomy and a nomological model", *MIS Quarterly*, Vol. 32 No. 3, pp. 503-529.

Soumelidou, A. and Tsohou, A. (2019), "Effects of privacy policy visualization on users' information privacy awareness level", *Information Technology and People*, Vol. 33 No. 2, pp. 502-534.

Steinfeld, N. (2016), "'I agree to the terms and conditions': (how) do users read privacy policies online? An eye-tracking experiment", *Computers in Human Behavior*, Vol. 55, pp. 992-1000.

Stutzman, F., Capra, R. and Thompson, J. (2011), "Factors mediating disclosure in social network sites", *Computers in Human Behavior*, Vol. 27, pp. 590-598.

Tsai, J.Y., Egelman, S., Cranor, L. and Acquisti, A. (2011), "The effect of online privacy information on purchasing behavior: an experimental study", *Information Systems Research*, Vol. 22 No. 2, pp. 254-268.

Tucker, C.E. (2014), "Social networks, personalized advertising, and privacy controls", *Journal of Marketing Research*, Vol. 51 No. 5, pp. 546-562.

van der Werff, L., Fox, G., Masevic, I., Emeakaroha, V.C., Morrison, J.P. and Lynn, T. (2019), "Building consumer trust in the cloud: an experimental analysis of the cloud trust label approach", *Journal of Cloud Computing*, Vol. 8 No. 1, p. 6.

Wang, L., Sun, Z., Dai, X., Zhang, Y. and Hu, H.H. (2019), "Retaining users after privacy invasions", *Information Technology and People*, Vol. 33 No. 6, pp. 1679-1703.

Wang, S., Beatty, S.E. and Foxx, W. (2004), "Signaling the trustworthiness of small e-commerce vendors", *Journal of Interactive Marketing*, Vol. 18 No. 1, pp. 53-69.

Wedel, M. and Kannan, P.K. (2016), "Marketing analytics for data-rich environments", *Journal of Marketing*, Vol. 80 No. 6, pp. 97-121.

Wu, K.W., Huang, S.Y., Yen, D.C. and Popova, I. (2012), "The effect of online privacy policy on consumer privacy concern and trust", *Computers in Human Behavior*, Vol. 28 No. 3, pp. 889-897.

Xu, H., Dinev, T., Smith, J. and Hart, P. (2011), "Information privacy concerns: linking individual perceptions with institutional privacy assurances", *Journal of the Association for Information Systems*, Vol. 12 No. 12, pp. 798-824.

Yun, H., Lee, G. and Kim, D.J. (2019), "A chronological review of empirical research on personal information privacy concerns: an analysis of contexts and research constructs", *Information and Management*, Vol. 56 No. 4, pp. 570-601.

Further reading

Capgemini (2019), "Championing data protection and privacy a source of competitive advantage in the digital century", available at: https://www.capgemini.com/de-de/wp-content/uploads/sites/5/2019/09/Report_GDPR_Championing_DataProtection_and_Privacy.pdf.

Fox, G., Tonge, C., Lynn, T. and Mooney, J. (2018), "Communicating compliance: developing a GDPR privacy label", *24th Americas Conference on Information Systems*, New Orleans, Louisiana.

PWC (2017), "Pulse survey: US companies ramping up general data protection regulation (GDPR) budgets", available at: https://www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/pwc-gdpr-series-pulse-survey.pdf (accessed November 2021).

Appendix

Appendix contents are available in online for this article.

Corresponding author

Theo Lynn can be contacted at: theo.lynn@dcu.ie