Behaviour & Information Technology

ISSN: 0144-929X (Print) 1362-3001 (Online) Journal homepage: www.tandfonline.com/journals/tbit20

Transparency by design: the effect of privacy policies visualisation on brand trust and perceived intrusion

Solon Magrizos, Martina Campora, Grigorios Lamprinakos, Apostolos Giovanis & Michael Christofi

To cite this article: Solon Magrizos, Martina Campora, Grigorios Lamprinakos, Apostolos Giovanis & Michael Christofi (17 Jun 2025): Transparency by design: the effect of privacy policies visualisation on brand trust and perceived intrusion, Behaviour & Information Technology, DOI: 10.1080/0144929X.2025.2520594

To link to this article: https://doi.org/10.1080/0144929X.2025.2520594

Published online: 17 Jun 2025.

BEHAVIOUR & INFORMATION TECHNOLOGY
https://doi.org/10.1080/0144929X.2025.2520594

Taylor & Francis
Taylor & Francis Group

Transparency by design: the effect of privacy policies visualisation on brand trust and perceived intrusion

Solon Magrizos[a], Martina Campora[b], Grigorios Lamprinakos[a], Apostolos Giovanis[c] and Michael Christofi[d]

[a]Department of Marketing, Birmingham Business School, University of Birmingham, Birmingham, UK; [b]Adam Smith Business School, University of Glasgow, Glasgow, UK; [c]Department of Business Administration, University of West Attica, Egaleo, Greece; [d]Faculty of Economics and Business Administration, Vilnius University, Vilnius, Lithuania

ABSTRACT
Recent technological trends have led to the development of a data driven society where technological companies are strengthening their capability in accessing, collecting and tracking consumers' data. However, communication of privacy policies has mostly remained the same since the beginning of the internet, rather than evolving alongside technological development, posing an ongoing risk for consumers. This study aims to explore the relationship between consumers and IoT privacy policies observing the effects of diverse policies developed with different transparency levels. By manipulating the levels of transparency with the use of explanatory infographics we examine the effect of a visualisation of information tool. Findings from 286 individuals taking part a 2 × 2 experiment confirm extensive benefits resulting from visualisation of privacy policies leading to increased trust to the advertising company and lower perceived intrusiveness of the ad. Justification for the collection of user data mediated the effect of visualisation to perceived company trust.

ARTICLE HISTORY
Received 27 April 2024
Accepted 4 June 2025

KEYWORDS
Trust; intrusiveness; wearables; transaparency

Introduction

Newly developed Internet of Things (IoT) technologies are increasingly permeating our lives and are expected to double from 15.9 billion in 2023 to more than 32.1 billion IoT devices in 2030 (Statista 2024a). Consumers, however, perceive IoT benefits more clearly compared to the associated risks, which tend to be highly underestimated (Tudoran 2024). Smart devices may contribute to the communication of sensitive customers' data to IoT companies and may be vulnerable to hacking. For instance, IoT companies have been proven to track consumers' patterns regarding food consumption, online expenditures and even pornographic movie preferences (De Cremer, Nguyen, and Simkin 2017). The sensibility of information is accentuated even more for wearable IoT since companies may record location preferences, health-related information and biometric data such as fingerprints, voice and facial recognition, as well as behavioural characteristics (Donner and Steep 2021). Additionally, third malicious parties may have access to these data. Data leakages are increasing, having tremendous consequences on enterprises and their customers, as providing the chance for hackers to access personal information such as bank account details, healthcare information, home addresses, or direct access to home CCTV systems (Cheng, Liu, and Yao 2017; Tudoran 2024).

It is in this background that consumers still underestimate risks associated with IoT devices mainly due to the difficult and time-consuming task of reading and understanding privacy policies that accompany the purchases of products and services (Rudolph, Feth, and Polst 2018). As a result, current privacy policies' design fails to effectively communicate privacy implications to consumers (Waldman 2018). This lack of transparency creates a communication gap negatively weighing on consumers' decision-making processes (Rossi and Lenzini 2020). Hence, to address this lack of information and further explore this problem, we build on previous research demonstrating that graphical representation of texts increases memorisation, comprehension, attention levels, and positive attitude towards communicated topics (Aleixo and Sumner 2017; Schaub, Balebako, and Cranor 2017; Soumelidou and Tsohou 2020).

Diverse studies have investigated how current privacy policies, even if in compliance with the GDPR, fail

CONTACT Solon Magrizos s.magrizos@bham.ac.uk Department of Marketing, Birmingham Business School, The University of Birmingham, Edgbaston, Birmingham, B15 2TT, UK

to appropriately inform consumers (Chassidim et al. 2021). Presently, literature concerning privacy policies and their influences on customers is limited (Cheng et al. 2024) and even less so if we consider studies in the wearables IoT domain (for a notable exception, see: Soumelidou and Tsohou 2020). Since technology is increasingly permeating our lives, the relationship concerning customers' relationships with IoT privacy policies should be further investigated (Fox, Lynn, and Rosati 2022). In this respect, previous literature concerning how images influence consumers' perception of privacy policies is limited to online consumption and social media while failing to represent consumers' relationships with the privacy policies of a physical object such as a wearable IoT. In fact, due to the higher amount of information that these interconnected devices collect, consumers might perceive graphical representations of privacy policies differently (Lee, Yang, and Kwon 2018). Such a difference may arise due to the fact that IoT devices' privacy policies have been considered less transparent compared to websites' privacy policies and were described as legal covers (Paul et al. 2018) and by the fact that consumers may perceive wearable devices specifically as extensions of their selves and judge them differently (Rapp 2023).

In this respect, to the best of our knowledge no previous study has investigated how images in privacy policies would influence the way consumers perceive IoT data collection and adopt wearable devices, hence highlighting a gap in our understanding of privacy policies. Therefore, we aim to investigate how IoT consumers perceive the application of explanatory infographics in privacy policies and whether visualisation of the often long and difficult to understand text will enhance trust in the company and reduce perceived intrusiveness of data collected. In doing so, we address a practical issue applicable to many everyday situations and theoretically, we respond to calls asking for alternative ways to communicate privacy policies (Fox, Lynn, and Rosati 2022) and pronouncing 'an urgent need for an interactive method for data owners to explore privacy' (Guo et al. 2023, 2). Finally, we help advance the communication privacy literature by including a new variable, that of justification for the data collected, in the relationship between visualisation and increased consumer trust.

In this study, we employ the theoretical lens of privacy calculus theory (PCT) (Gutierrez et al. 2019) to study how visualisation of privacy policies and justification for collecting user data affect consumer behaviour in the context of wearable devices. From a theoretical perspective, our work is placed among increasing calls for more transparency on how companies collect consumers' data (e.g. Lamprinakos et al. 2022). Increasing ads' transparency (e.g. by providing explanations on process of collecting information) leads to higher acceptance and decreases perceived intrusiveness (Broeck, Poels, and Walrave 2017; Dogruel 2019). However, the key question remains whether higher levels of privacy policies' transparency, derived by the enclosure of images and a more practical and aesthetically pleasing method to communicate the key points, will affect privacy perceptions.

In this context, the first research question is presented:

> RQ 1: How does the visualisation of privacy policies influences perceived data use intrusiveness?

While much attention has been paid to how privacy information is presented, less focus has been given to what is actually said about why data is being collected. Yet this seems to matter a great deal. People are more likely to accept data collection when they feel there's a clear, understandable reason behind it. Some studies have shown that offering a justification – such as explaining that data helps lower costs or improve personalisation – can reduce scepticism and make users feel more in control (John, Kim, and Barasz 2019; Kim and Kim 2017). This ties in with privacy calculus theory, which suggests that people weigh risks against perceived benefits when deciding whether to share their data (Gutierrez et al. 2019).

This concern is especially important in the context of wearables, where the collected data is highly personal and often sensitive (e.g. related to health, location, preferences). Therefore, a further question is related to consumers' perceptions once they are provided with a clearer understanding of how companies handle their data. Are they going to consider the brand as more trustworthy? Would higher perceived data use transparency affect their purchase intentions? Additionally, if consumers have a clearer understanding of data policies, their perception might change towards both device's manufacturer and third parties with whom the brand interacts. Hence, if consumers increase their understanding concerning how companies sell their data to third parties for marketing purposes, how would this influence their relationship with the company collecting their data? Concepts expressed in these questions are grouped in the second research question:

> RQ 2: How does justification for collecting data affects the link between the visualisation of privacy policies, brand trust, and consumers' perception of intrusive advertising?

Literature review

The Internet of Things and smart wearables

IoT is an online system where interconnected devices (or ‘‘things’’) exchange data through the internet. These devices are physical objects developed to collect and register data. The information gathering occurs thanks to technological sensors that record diverse types of data (such as location, blood pressure, air temperature, body temperature) and communicate it with the other devices connected to the system (Onu, Mireku Kwakye, and Barker 2020). This information is organised and communicated effectively and efficiently, bringing extensive benefits. Examples of IoT devices are smart lights recording sleep patterns or home occupancy (smart homes), smartwatches measuring your daily activities (wearables), smart footballs that record launch speed and direction, self-driving cars (mobile IoT) and many others (Perez, Zeadally, and Cochran 2018). These benefits are driving a consumption transition from standalone devices to interconnected ones, showing IoT increased consumption and accessibility in terms of availability and price (Zheng et al. 2018).

The boundaries separating the physical and the virtual world are starting to vanish with the increasing adoption of IoT wearables. These are technological devices attached to the human body and connected to other linked devices. Wearables include wrist wearables such as smartwatches or wristbands, smart glasses, but also intelligent clothes and diapers (De Arriba-Pérez, Caeiro-Rodríguez, and Santos-Gago 2016). They are provided with sensors that record, track and communicate data resulting in the registration of behaviours, preferences and individuals’ routines (Aktypi, Nurse, and Goldsmith 2017). In terms of wearables’ benefits, smartwatches can record health data such as heart rate, sleep patterns, stress levels as well as eating or smoking habits (Gill et al. 2023). These reports were confirmed to help monitor patients’ health along with individuals who want to increase their self-awareness and begin a behavioural change (Gabriele and Chiasson 2020). Smartwatches among other things, have also shown to be able to predict drivers’ sleepiness and effectively diminish car crashes (Udoh and Alkharashi 2016).

Users’ operation of IoT technologies offers incredible business benefits from the utilisation of customers’ data. The vast amounts of information collected by companies can assess patterns of political, socio-cultural, and economic trends and nudge consumers towards behaviours most beneficial to them (Sadeghian and Otarkhani 2023). In fact, many technological companies that have currently access to an enormous amount of data (e.g. Facebook, Snapchat, Google, etc.,) are investing in the wearables’ business to increase their knowledge about users. Combining customers’ information collected by these industries with wearables’ information would lead to the determination of an unprecedented specific customer profile. From a marketing perspective, this implies a transition towards the individualisation of advertisements, shifting from consumer persona to advertising single consumers (Donner and Steep 2021). Finally, in terms of wearables’ circulation in the market, as their functions increase, their prices decrease, with the 560 million users of wearables in 2024 (Statista 2024b) projected to grow even more in the coming years.

Privacy in IoT devices

It is quite straightforward to imagine the privacy implications that will arise from such an interconnected world (Magrizos 2020). In fact, the growth in data collection is not going to stop, with the increase in IoT devices, the development of smart homes and cities will pose humans in the condition of needing additional help to administer the consent of their data. From a customers’ perspective, privacy and risks associated with IoT technologies are often less clear to consumers compared to the benefits they derive (Schaub, Balebako, and Cranor 2017). The complexity of these technological systems and their increased presence led individuals to deal with a considerable amount of privacy policies and notices that are presumably all different in their form, data usage, treatment of sensitive information, etc.

Owners of wearable devices lack an understanding of the nature of data extracted and how their sensitive data is treated (Zheng et al. 2018). Particularly, they are less concerned about data collection from interconnected devices compared to smartphones and the internet (Lee, Yang, and Kwon 2018). Additionally, users may be completely unaware of the presence of an IoT device that is collecting data (Chow 2017). Imagine entering a friend’s house and that (s)he just installed an IoT system. You may be uninformed of the system’s presence and about the privacy implications derived from the data collected by the system. Hence, it would collect and register your data even if you had not expressed consent (for a discussion between overt and covert data collections in online settings, see Lamprinakos et al. 2022). This issue, defined as ‘‘bystander’s privacy’’, becomes even more salient in highly interconnected environments such as smart cities (Perez, Zeadally, and Griffith 2017).

A key realisation around privacy and consumer protection is that data being collected is not a mere side-effect of using the technology but a key part of the business models of technology-based companies. In many platform-based companies (e.g. Facebook, Instagram, X) consumers are not paying for products or services but agree to provide access to their personal information, effectively becoming the product being sold. This information is collected by the IOT companies and then analysed, and often shared or sold to third parties – particularly advertisers – as part of a broader strategy to monetise user behaviour (Boerman, Kruikemeier, and Zuiderveen Borgesius 2021). This is especially relevant in the context of wearable technologies discussed here, where firms gain access to highly sensitive data such as health indicators, location patterns and behavioural routines (Donner and Steep 2021). With this business model in mind, it shouldn't come as a surprise that privacy policies are often designed to be long and vague, and overall difficult to understand. This way, they provide a legal shield for companies and enable data extraction with almost no consumer resistance. Our study responds to this broader landscape by examining how more transparent forms of communication such as visualisation and clear justification can improve consumer trust and reduce perceptions of intrusiveness.

To solve the abovementioned problem researchers are developing systems able to translate privacy policies into machine-readable formats that allow computers to evaluate, compare and translate into easier terms the policies to users (Onu, Mireku Kwakye, and Barker 2020). For instance, Palmirani et al. (2020) developed a system able to translate particular words of privacy policies into icons that were designed to be easily understood globally. Similarly, scientists are developing Interactive Tools for translating privacy policies in graph drawings (Albalawi and Ghazinour 2016; Guo, Rodolitz, and Birrell 2020). In relation to smart cities, AI companies are developing virtual agents aimed at administering and communicating potential privacy collection of data to human beings living in smart cities (Cui et al. 2018). These ultimate technological systems can register users' preferences and communicate them personalised privacy policies and notices containing more relevant information based on their preferences (Pappachan et al. 2017). However, these systems are still in development limiting their current applications to protect consumers.

A final challenge for consumers to protect their data is the underestimation of cyberattacks. Users tend to ignore the security aspects of technological gadgets, overlooking both devices' vulnerabilities and consequences arising from the theft of their digital identities (Aktypi, Nurse, and Goldsmith 2017). In fact, poorly secured IoT devices or accounts expose the whole IoT network to cyber-attacks (Tawalbeh et al. 2020).

The ineffectiveness of privacy policies

The increasing threat directed at customers' privacy has pushed governments at a global level to establish regulations aimed at protecting consumers' data. In 2018, the European Union has put into effect the General Data Protection Regulation (GDPR) to empower consumers, enhancing their privacy protection. GDPR focuses on the protection of online customers' data that includes the domain of IoT devices (Badii et al. 2020). This regulation attempts to elevate customers' position granting them the right to ask companies specifically the data they have collected and possibly delete them (Right of Access to Data & Right to be Forgotten). Moreover, companies' inobservance of the regulation may result in large fines such as the French case of Google where the multinational company has been charged with a fine of 50 million euros (Barrett 2020). Even though this Regulation has increased consumers' protection, consumers are still highly unaware of the information they provide when accepting privacy policies (Rudolph, Feth, and Polst 2018).

To enforce clearer privacy policies, GDPR imposes the principle of transparency to be applied, stating the following: 'any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used' (EU General Data Protection Regulation 2016). Even though the Regulation obliges companies to disclose clear information concerning the collection of data, it does not impose guidelines regarding how the information must be disclosed to consumers. This is contrary to food labelling, where the EU is forcing companies to follow precise norms on how to disclose information imposing strict norms of fonts minimum sizes and places where food labelling information should be, suggesting the implementation of pictograms and symbols.

Currently, the GDPR partially protects users. On one side, the enforcement of the regulation has led privacy policies to be more comprehensible increasing the easiness of the terminology used; on the other, the principle of readability is not sufficient for users to perceive a document to be easy and comprehensible failing to enhance transparency (Rossi and Lenzini 2020). In fact, privacy regulations have led privacy policies to be increasingly lengthy and visually flat (Garg and Murthy 2019). Paradoxically, certain privacy policies designed as 'walls of text' that make consumers lose between diverse links, have proved to be compliant with the law (Geradin, Karanikioti, and Katsifis 2021). As a result, users either ignore privacy policies or barely give attention to them, and passively accept the terms (Kreuter et al. 2020). It is estimated that 80% of

Europeans do not entirely read and or comprehend data policies (Rudolph, Feth, and Polst 2018) due to complexity (Waldman 2018) and time restrictions are the major reasons why consumers deliberately avoid privacy policies (Rudolph, Feth, and Polst 2018).

The privacy paradox

The privacy paradox is a complex dichotomy concerning users' lack of actions directed to protect their privacy albeit their privacy concern (Barth and de Jong 2017). Several products or services pose consumers to face a trade-off. On one side consumers have personalised benefits provided by the product or service, on the other, they need to authorise the company to collect very useful information about them. Even though individuals perceive this data collection process as negative, they tend to proceed with the disclosure of their data as they prioritise connectedness and convenience over the disclosure of their information (Aiolfi, Bellini, and Pellegrini 2021; Zheng et al. 2018). Hence, the understanding and risk concerns of privacy policies are still insufficient motives to proactively conduct measures to protect personal privacy resulting in a paradox (Barth and de Jong 2017).

This dichotomy is supported by the privacy calculus theory (PCT) which is based on the principle that consumers' decisions regarding the risk of information disclosure are weighed against the benefits derived by the revealing of such information (Gutierrez et al. 2019). In fact, customers adopt a risk-benefit analysis and increasingly ignore privacy policies based on the perception of future gains (Sun, Willemsen, and Knijnenburg 2020). Hence, users are inclined to extensively reveal private information the more they are rewarded, the disclosure diminishes the more people perceive the associated risks (Bol et al. 2018). For instance, discounts or coupons have proved to be an effective strategy for increasing users' data disclosure (Brinson, Eastin, and Bright 2019). Additionally, privacy calculus influences personal information disclosure as well as the perception of advertisers (De Keyzer, Dens, and De Pelsmacker 2021).

Hypotheses development: the visualisation of privacy policies

Consumers' obstacle in understanding privacy policies is increasing at the same pace as the amount of data companies collect. This gap is expanding aided by the fast technological development and the growth of interconnected devices. Data collected from a single IoT device may retain limited sensitive data, whereas the aggregation of diverse devices may generate the disclosure of an unthinkable amount of confidential information (Menard and Bott 2020). In this respect, IoT devices should strengthen even more the transparency of their privacy policies due to their integration of users' data and their increased presence in consumers' lives (Perez, Zeadally, and Cochran 2018).

To reduce this gap researchers are tackling the issue striving to develop more transparent alternatives of privacy policies. AI is taking the lead in this transition; scientists are working on extractors able to select keywords for a specific audience, and tools for visualising privacy policies (Albalawi and Ghazinour 2016; Chang et al. 2019; Guo, Rodolitz, and Birrell 2020). In fact, the design strongly influences the perception of privacy policies, factors as text dimension, paragraphs divisions, length of text, or line spacing contribute to texts' readability (Rossi and Lenzini 2020; Waldman 2018). However, the sole modification of the text design has proved to merely have moderate effects on texts' readability (Albalawi and Ghazinour 2016).

On the other hand, and particularly relevant to this study the enclosure of images positively contributes to comprehension and memory. Table 1 offers a selection of previous work in the visualisation of privacy policy and a summary of their key findings.

According to the dual coding theory, combining texts with images increases the understanding and memorability of texts (Paivio 1971, 1975). The enclosure of images in privacy policies has confirmed the applicability of the theory resulting in lower cognitive effort needed to read and understand the policy (Perdana, Robb, and Rohde 2019), higher user awareness (Tabassum et al. 2018) and increased trust (Fox, Lynn, and Rosati 2022). Soumelidou and Tsohou (2020) have demonstrated that the enclosure of images or infographics aimed at visualising privacy policies increases the awareness and comprehension of Instagram privacy policies. Similarly, comics and texts combination improve readability and additionally increases a positive attitude towards the topic (Aleixo and Sumner 2017). In fact, anthropomorphic designs and animated clues offer

Table 1. Selected literature in visualisation of privacy policies.

Reference	Key Findings
Kelley et al. (2010)	Adapting nutrition labels for privacy policies increase accuracy and reading enjoyment
Soumelidou and Tsohou (2020)	Visualising Instagram's GDPR-compliant privacy policy leads to higher privacy awareness levels
Fox, Lynn, and Rosati (2022)	GDPR privacy labels positively influence perceptions of risk, control, privacy and trustworthiness
Tabassum et al. (2018)	A comic-based policy increased user attention
Perdana, Robb, and Rohde (2019)	Data Visualisation reduced cognitive effort to read privacy policies
Barth et al. (2021)	A Privacy Rating combined with data visualisation had a significant effect on users' trust in the online service.

mental shortcuts diminishing the mental effort requested for the accomplishment of a task while increasing readability and comprehension (Kitkowska et al. 2020).

Consequently, juxtaposing an explanatory infographic to the privacy policy text is expected to increase users' comprehension leading to a higher level of perceived data use transparency. Hence, with the aid of dual coding theory, hypothesis 1 is formulated:

> H1: The visualisation of privacy policies reduces perceived IoT Intrusiveness

Brand trust, defined as the confidence to rely on an exchange partner (Moorman, Zaltman, and Deshpande 1992) is a significant success factor in online settings due to the 'lack of a personal touch and the geographical locations of the consumers and the firm'. The notion of trust suggests individuals are exposed to a certain degree of risk (Brinson, Eastin, and Bright 2019). In this respect, consumers' trust in a company derives from a risk evaluation and consequently drives purchasing behaviour. While the relationship between brand trust and purchase intention has been extensively investigated, a connection between brand trust and privacy concerns is limited, specifically regarding IoT devices (Surucu, Yesilada, and Maslakci 2020; Wottrich, Verlegh, and Smit 2017).

In the context of privacy policies brand trust emerges from the evaluation of the perceived risk concerning the reliability of the company in treating customers' data (Portal, Abratt, and Bendixen 2019; Riva et al. 2024). But the difficulties individuals facing when reading privacy policies, create barriers to establish a trustful relationship between consumers and brands. On the contrary, simplifying privacy policies should increase trust in the company. As exemplified by Esmaeilzadeh's empirical study (2019), higher perceived transparency of privacy policies of health care providers increased patients' trust towards the electronic system storing their health data. Similarly, as seen in Table 1, using privacy labels (Fox, Lynn, and Rosati 2022) or privacy ratings (Barth et al. 2021) has increased users' trust in the online provider.

Brand trust as a mediator

In this study, we were interested not only to confirm previous work on the effect of visualisation of privacy policies in increased brand trust in a novel context, (IOT and smart wearables) but also to extend our understanding by proposing brand trust as a mediator. Indeed, previous research has established a positive relation between transparency of privacy policies and trust in online companies, having a consequent positive impact on purchase intention (Lamprinakos et al. 2022; Wang and Herrando 2019). In other words, displacing clear and transparent privacy policies induces consumers to increase their trust towards the online platforms triggering their intention to purchase (Lăzăroiu et al. 2020). Similarly, higher-level transparency of privacy policies for a physical product generates higher trust towards the devices manufacturer, that subsequently is proved to increase purchasing behaviour (Brinson, Eastin, and Bright 2019; Zheng et al., 2018).

But while the link between trust and purchase intentions is well defined, we wanted to extend these findings by exploring the mediating effect of trust to the relationship between visualisation of privacy policies and perceived intrusiveness. The reason is threefold. *One*, in the context of our study, smart wearables, the consumers are less likely to use them to purchase products and services, compared to e.g. online platforms. *Two*, a risk to the adoption of smart wearables is their intrusive nature with associated loss of autonomy (Xue 2019). This risk is stronger if we consider that for many users, their wearables are big part of their identity, with consumers often seeing them as part of the self (Belk 2013; Liu, Yang, and Yao 2022) which may increase feelings of intrusiveness when they uncover access to private data. *Three* perceived intrusiveness is considered to have the greatest influence on the acceptance of personalised advertising (Gutierrez et al. 2019) which is an integral part of the wearable experience (Orazi and Nyilasy 2019). Personalised advertising (PA) refers to effectively targeted ads based on the personality, behaviour, and personal information of a consumer (Gironda and Korgaonkar 2018). Such a high level of personalisation has shown not to be invariably effective since targeted consumers have perceived it as too intrusive and a threat to privacy (De Keyzer, Dens, and De Pelsmacker 2021). In fact, when consumers feel their privacy to be violated, they negatively react to personalised advertisements not accepting it as it was planned to (Brinson, Eastin, and Bright 2019).

As a result, increasing transparency in privacy policies via their visualisation would decrease the barrier consumers face in developing a trustworthy relationship with IoT providers. Consequently, increasing trust in the IoT company will lead to lower perceived intrusiveness. Hence, we hypothesise that:

> H2: Perceived brand trust mediates the link between the visualisation of privacy policies and perceived IoT Intrusiveness

Increasing users' understanding of how their data is utilised, would increase their acceptance of selling their data to third parties to use for, while limiting the perception of intrusiveness (Brinson, Eastin, and Bright 2019). Users would be empowered with the possibility of choice and develop a more positive attitude towards the advertising which is also expected to increase its effectiveness (Kim, Barasz, and John 2021). By recalling Privacy Calculus theory, users' perception of the trade-off between privacy concerns and personalised advertising will shape their preference for the usage of IoT devices. These assumptions are based on the concept of perceived control, a principle that can be defined as ''one's ability to exert control over situations or events'' (Ly et al. 2019). Whenever individuals perceive a lack of control, they tend to exhibit negative feelings, whereas increased information helps them to restore control, intensifying positive attitudes (Reich and Infurna 2016). In this case, consumers would lack the power to elaborate their privacy calculus for personalised advertising. Meaning that they would be deprived of the evaluation of whether the benefits of personalised advertising outweigh the associated costs. Even though De Keyzer, Dens, and De Pelsmacker (2021) confirm such an outweigh, they underline the importance of perceived control which doubles the possibilities of ad clicking on personalised advertising.

As a result, supported by PCT and by the concept of perceived control hypothesis 3 is formulated:

> H3: The mediating effect of trust in the relationship between the visualisation of the privacy policies and perceived intrusiveness on purchase intention will be moderated by justification for user data collection such that the mediated relationship is stronger when a justification for user data collection is mentioned.

Figure 1 depicts our formulated hypotheses and conceptual model graphically.

Methodology

An experimental design was employed to test our hypotheses. The study targeted adults over eighteen who possess a smartphone and ethical approval was obtained from a large UK University. 286 participants (56.3% females) aged between 18 and 55 (Mage = 36.12, SD = 11.11) were recruited in return for a small financial incentive (approximately $5), ostensibly to discuss their preference to a new wearable gadget – smart glasses created by a fictitious brand. They were presented with a shortened standard version of 'terms and conditions' which they needed to accept. They were then assigned to four different conditions (visualisation of privacy policy or not, justification for collecting personal information or not).

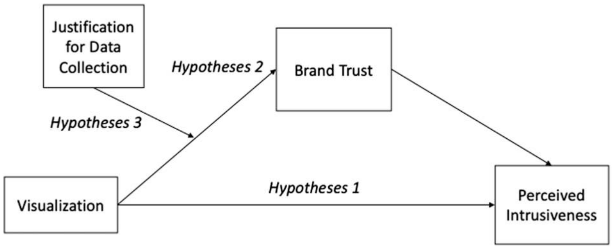

Figure 1. Conceptual model.

The visualisation of the communication policies was employed via the development of an explanatory infographics consisting of images and texts. Therefore, scenarios with visualisation were provided with a visual representation of the product's privacy policies aimed at increasing perceived data use transparency (Figure 2). To provide a balanced visual representation of the survey and to increase internal validity, the two scenarios characterised by non-visualisation still included the same text as in Figure 1 and an unrelated image, this time an irrelevant infographic (Creswell 2017) which in this case explained the product's functions

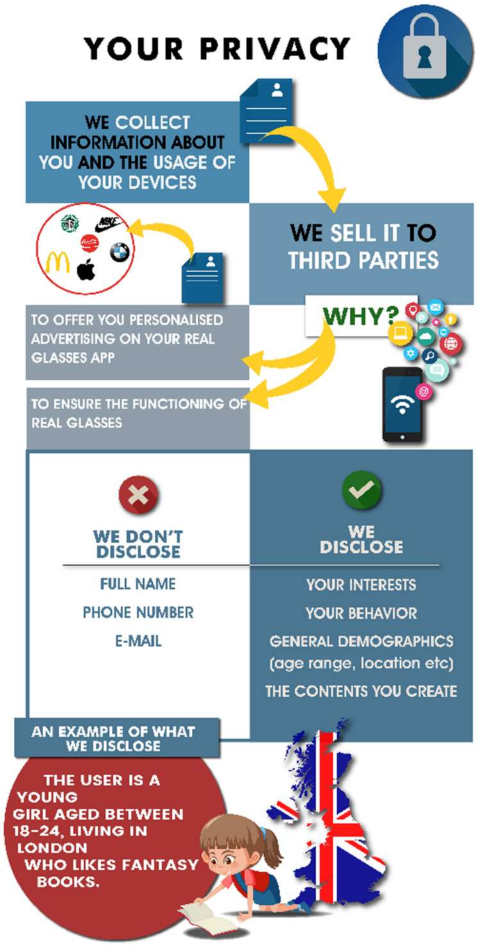
YOUR PRIVACY
WE COLLECT INFORMATION ABOUT YOU AND THE USAGE OF YOUR DEVICES
WE SELL IT TO THIRD PARTIES
WHY?
TO OFFER YOU PERSONALISED ADVERTISING ON YOUR REAL GLASSES APP
TO ENSURE THE FUNCTIONING OF REAL GLASSES
WE DON'T DISCLOSE
FULL NAME
PHONE NUMBER
E-MAIL
WE DISCLOSE
YOUR INTERESTS
YOUR BEHAVIOR
GENERAL DEMOGRAPHICS (age range, location etc)
THE CONTENTS YOU CREATE
AN EXAMPLE OF WHAT WE DISCLOSE
THE USER IS A YOUNG GIRL AGED BETWEEN 18-24, LIVING IN LONDON WHO LIKES FANTASY BOOKS.

Figure 2. Infographic developed for visualisation and justification scenario.

(Figure 3). The second author developed the infographics acknowledging that infographics' design is a crucial part of the study.

To manipulate whether the purpose of data collection was mentioned, two scenarios were created. For all cases the participants read that the customer-company agreement authorised the fictitious company (Real Glasses) to sell customers' personal information to third parties. In the scenarios where we wanted to mention a justification, the participants also read that their data was sold to third parties 'so that the users gain from personalised advertising and so that the price of the glasses is kept as low as possible'. In the non-justification scenario, the participants just read that this was 'following industry practice'. All scenarios were pretested to confirm that they indeed measured the indented variables.

Measures

All variables were measured by employing seven-point Likert-type scale. To measure perceived intrusiveness, we followed Sanchez and Kull (2022) and asked participants to indicate on a three-item scale how *intrusive* and how *invasive* they found the way the privacy policy was communicated to them and how much of an *imposition* they considered reading the privacy policy (1 = not at all, 7 = very much; α = 0.89).

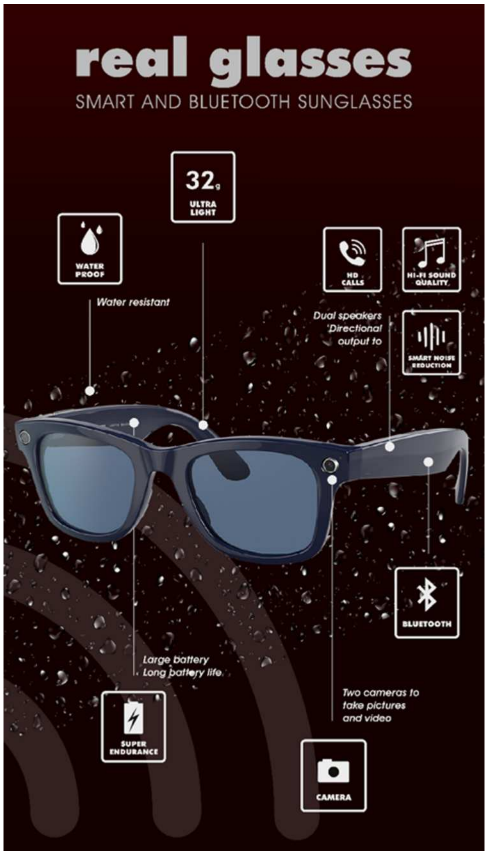

Figure 3. Infographic developed for non-visualisation scenarios.

To measure brand trust, or trust in the company concerning how they would deal with consumers' data, a four-item scale was adopted following Herbst et al. (2012) (1 = strongly disagree, 7 = strongly agree; α = 0.79). Items included: 'I trust this company', 'this company is reliable', 'this company is truthful', 'I can rely in this company'.

Finally, we included two questions regarding the extent to which respondents usually paid attention to privacy policies and to enquire whether the hypothetic scenario was realistic to them.

Table 2 lists the means, standard deviation and intercorrelations of the studied variables.

Results

Two manipulation checks were conducted to verify the effectiveness of our scenarios. The results revealed that participants perceived the communication policy as more visually effective in the visualisation condition (M = 6.37, SD = .60) and felt that the reasons for collected data were better understood in our justification condition (M = 6.44, SD = .55) indicating that our manipulations were successful.

Hypothesis 1 proposed that high visualisation would result in lower perceived intrusiveness of the communication of a privacy policy compared to a non-visualisation text only condition. The results revealed that participants in High Visualisation condition (*M* = 2.14, *SD* = 1.29) reported lower perceived intrusion than those in the Text Only (low visualisation) condition (*M* = 4.29, *SD* = 1.88), *t*(284) = 11.32, *p* < .001, providing support for H1.

To test our remaining hypotheses, Model 7, a moderated mediation model in PROCESS (Bootstrap sample: 5000; Hayes 2013), was performed. Visualisation as the independent variable, Trust as the mediator, Justification for Data Collection as the moderator, and Perceived Intrusiveness as the dependent variable.

Consistent with our first hypothesis, the analysis verified the direct negative effect of Visualisation to

Table 2. Means, standard deviation and intercorrelations of the studied variables.

Variables	Mean	S.D.	1.	2.	3.	4.
1. Visualisation	1.49	.50	1			
2. Trust	4.69	1.79	−.621**	1		
3. Justification	1.5	.50	−.056	.219**	1	
4. Intrusiveness	3.19	1.93	.558**	−.796**	−.241**	1

N = 286.
**p* < .05.
***p* < .01.

Perceived Intrusiveness (β = -.397, SE = .176, $p < .05$). More importantly, our analysis provided support for a significant partial mediating impact of Perceived Trust to the effect (β = −1.753, SE = .206, 95% CI [−2.174, – 1.137]) supporting Hypothesis 2.

Hypothesis 3 predicted that Justification for Data Collection will moderate the indirect relationship between Visualisation and Perceived Intrusiveness such that the mediated effect of perceived Trust will be stronger for those who receive Justification for the data collection. The index of the moderated mediation, which provides an appropriate test of moderated mediation (Hayes 2013), was significant (index = .813, 95% CI = [.309, 1.316]). Specifically, the indirect effect was significantly larger when respondents read the scenario which justified data collection (effect = 12.129, 95% CI = [−2.654, – 1.649]) than when they didn't (effect = −1.316, 95% CI = −1.870, – .910,]). Thus, Hypothesis 3 was supported.

Discussion and conclusion

Smart wearable devices are revolutionising how users communicate with each other and how they interact with the physical world around them. acquire information. However, the benefits of smart wearables largely depend on the devices' ability to collect and analyse a large amount of user data, shaping the smart wearables-privacy paradox (Kang and Jung 2021) where privacy risks and user benefits are combined. In this context, we wanted to explore the effect of various variables, most notably the visualisation of privacy policies. Most users don't bother to understand or even read privacy policies and suggestions have been made that using images in combination with text, will increase their readability, user attention and acceptance. Our findings highlight diverse beneficial outcomes resulting from the visualisation of privacy policies. In accordance with recent studies, this study confirms that providing a visualised alternative of privacy policies increases perceived clarity of how a company administers consumers' data (Kitkowska et al. 2020; Soumelidou and Tsohou 2020).

More importantly, this study goes beyond prior literature by determining further effects of the enhanced transparency caused by this visualisation. Specifically, consumers who were shown the visualised version of the privacy policies compared to those who saw the text-only one demonstrated higher brand trust to our fictitious company and perceived the collection of personal information as less intrusive. Importantly, our analysis suggests that brand trust mediated the link between visualisation and perceived intrusiveness, suggesting that visualisation in its own might not be enough to reduce perceived intrusiveness but companies need to ensure that they have gained consumers' trust as well.

Finally, consistent with the study's hypotheses we find evidence for the moderating role of justification for the collection of data. Employing the theoretical lens of the privacy calculus theory (PCT) which suggests that individuals will weigh the risk of information disclosure against their benefits (Gutierrez et al. 2019) enabled us to formulate a hypothesis for a moderated mediation: Providing justification for the collection of user's data increased the mediating role of trust between visualisation and perceived intrusiveness. In other words, in high justification scenarios, the positive effect of visualisation to brand trust increased, suggesting that the overall mediation effect is stronger.

The above-mentioned findings offer implication for theory and practice alike. IoT literature is extended in various ways. Firstly, we add to the limited literature confirming the positive effects of the inclusion of explanatory images in privacy policies in a different context, that of IoT devices, which often involve complex and extensive data collection. These findings confirm the applicability of dual coding theory which asserts that the combination of text and images improves comprehension and retention highlighting its importance in the context of modern privacy communication for IoT technology.

The study also makes a novel contribution by identifying trust as a mediating factor in the relationship between privacy policy visualisation and perceived intrusiveness. Previous work focused on other variables such as increased accuracy, enjoyment, awareness and effort, of users and placed little emphasis on trust (see Table 1). When trust was examined, it was always treated as a dependent variable while the mediating role of trust remained underexplored. By addressing this gap, the study underscores the importance of trust as a key mechanism that can alleviate negative perceptions and enhance consumers' receptivity to privacy practices.

We finally add two novel (in this literature) concepts, those of perceived *intrusiveness*, which is a key obstacle in consumers' willingness to allow collection of private data and *justification* for the collection of data, to moderate the effect of visualisation on trust. Both of these play a key role in our understanding of the user – IoT interaction. While not explicitly examined in this study, perceived intrusiveness is well linked with personalised advertising and increasing transparency on data collection methods can lead to a more positive attitude towards personalised adverts (Brinson, Eastin, and Bright 2019; Dogruel 2019; Jiang, Xiao, and Wang

2020). Marketing colleagues, therefore, may be interested to explore these interactions further. Consumers' *decision-making* process related to wearables' use is influenced by 'the duality between the benefits of the devices and the threat to privacy not only of those who use them but also of others around them' (Ferreira et al. 2021, 7) so reducing the concern for privacy might increase trust and perceived adoption of these devices.

From a more practical standpoint, policymakers can employ these findings to advocate for more transparency in data collection and privacy policies. Similarly to the food industry where such guidelines exist, we add to calls for the inclusion of visual representations in privacy policies. This would ensure that privacy communications are more comprehensible and accessible, empowering consumers to make informed decisions about their data. This is particularly salient as information collected by wearable devices is increasing extensively (De Arriba-Pérez, Caeiro-Rodríguez, and Santos-Gago 2016) but privacy policies are remaining stable with policymakers failing to protect consumers in such a developing interconnected world (Rossi and Lenzini 2020). Our study highlights how the visualisation of privacy policies would primarily benefit society at large, empowering consumers by offering them the possibility to conduct more informed choices.

Lastly, marketers should leverage visually supported privacy policies and justification for data collected to increase user's trust reduce consumer resistance to personalised advertising. Enhanced transparency achieved through visual elements can help consumers feel more informed and in control, fostering positive attitudes towards targeted marketing such as personalised advertising. This strategy can mitigate the 'backlash effect' often seen with highly personalised advertisements perceived as intrusive. It can also help reduce the privacy-paradox (Kang and Jung 2021) since when consumers are faced between a decision to choose between their privacy and a better user experience, they often adopt a risk-benefit analysis and increasingly ignore privacy policies based on the perception of future gains (Sun, Willemsen, and Knijnenburg 2020). By balancing the need for data-driven personalisation with respect for consumer privacy, companies can improve ad effectiveness and click-through rates, ultimately driving better marketing outcomes.

Our study is not without limitations, which however suggest opportunities for future researchers. The first limitation originates from the context in which we test our hypotheses. Our participants were surveyed about their attitude towards the privacy policy of smart glasses however their attitudes might differ in a non-wearable device context. Future researchers can test similar hypotheses in different contexts. Another limitation finally comes from the methods employed. We acknowledge that our infographics' design is a crucial part of the study since the provision of different data visualisation could have led to different results (Wang et al. 2019). While this is arguably the case for all similar studies, our suggestion for future research practice alike would be that for visualisation to become an established standard, specific guidelines need to be adopted, ideally approved by an independent organisation.

Author contributions

CRediT: **Michael Christofi:** Writing – review & editing.

Disclosure statement

No potential conflict of interest was reported by the author(s).

References

Aiolfi, S., S. Bellini, and D. Pellegrini. 2021. "Data-driven Digital Advertising: Benefits and Risks of Online Behavioral Advertising." *International Journal of Retail & Distribution Management* 49:1089–1110. https://doi.org/10.1108/IJRDM-10-2020-0410

Aktypi, A., J. R. Nurse, and M. Goldsmith. 2017. "Unwinding Ariadne's Identity Thread: Privacy Risks with Fitness Trackers and Online Social Networks." In *Proceedings of the 2017 on Multimedia Privacy and Security*, edited by R. A. Hallman, K. Rohloff, and V. Chang, 1–11. New York, NY: Association for Computing Machinery.

Albalawi, T., and K. Ghazinour. 2016. "A Usability Study on The Privacy Policy Visualization Model." *IEEE 14th Intl Conf on Dependable, Autonomic and Secure Computing, 14th Intl Conf on Pervasive Intelligence and Computing, 2nd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech)*: 578–585.

Aleixo, P. A., and K. Sumner. 2017. "Memory for Biopsychology Material Presented in Comic Book Format." *Journal of graphic novels & comics* 8 (1): 79–88. https://doi.org/10.1080/21504857.2016.1219957

Badii, C., P. Bellini, A. Difino, and P. Nesi. 2020. "Smart City IoT Platform Respecting GDPR Privacy and Security Aspects." *IEEE Access* 8: 23601–23623. https://doi.org/10.1109/ACCESS.2020.2968741

Barrett, C. 2020. "Emerging Trends from the First Year of EU GDPR Enforcement", American Bar Association, Chicago. *The SciTech Lawyer* 16 (3).

Barth, S., and M. D. T. de Jong. 2017. "The Privacy Paradox – Investigating Discrepancies between Expressed Privacy Concerns and Actual Online Behavior – a Systematic Literature Review." *Telematics and Informatics* 34 (7): 1038–1058. https://doi.org/10.1016/j.tele.2017.04.013

Barth, S., D. Ionita, M. de Jong, P. Hartel, and M. Junger. 2021. "Privacy Rating: A User-Centered Approach for Visualizing Data Handling Practices of Online Services."

IEEE Transactions on Professional Communication 64 (4): 354–373. https://doi.org/10.1109/TPC.2021.3110617

Belk, R. W. 2013. “Extended Self in a Digital World.” *Journal of Consumer Research* 40 (3): 477–500. https://doi.org/10.1086/671052

Boerman, S. C., S. Kruikemeier, and F. J. Zuiderveen Borgesius. 2021. “Exploring Motivations for Online Privacy Protection Behavior: Insights from Panel Data.” *Communication Research* 48 (7): 953–977. https://doi.org/10.1177/0093650218800915

Bol, N., T. Dienlin, S. Kruikemeier, M. Sax, S. C. Boerman, J. Strycharz, N. Helberger, and C. H. de Vreese. 2018. “Understanding the Effects of Personalization as a Privacy Calculus: Analyzing Self-disclosure across Health, News, and Commerce Contexts.” *Journal of Computer-Mediated Communication* 23 (6): 370–388. https://doi.org/10.1093/jcmc/zmy020

Brinson, N. H., M. S. Eastin, and L. F. Bright. 2019. “Advertising in a Quantified World: A Proposed Model of Consumer Trust, Attitude toward Personalized Advertising and Outcome Expectancies.” *Journal of current issues and research in advertising* 40 (1): 54–72. https://doi.org/10.1080/10641734.2018.1503108

Broeck, E. V. D., K. Poels, and M. Walrave. 2017. “A Factorial Survey Study on the Influence of Advertising Place and the Use of Personal Data on User Acceptance of Facebook Ads.” *The American behavioral scientist (Beverly Hills)* 61 (7): 653–671. https://doi.org/10.1177/0002764217717560

Chang, C., H. Li, Y. Zhang, S. Du, H. Cao, and H. Zhu. 2019. *Automated and Personalized Privacy Policy Extraction Under GDPR Consideration*. Cham: Springer International Publishing, 43–54.

Chassidim, H., C. Perentis, E. Toh, and B. Lepri. 2021. “Between Privacy and Security: The Factors That Drive Intentions to use Cyber-Security Applications.” *Behaviour & Information Technology* 40 (16): 1769–1783. https://doi.org/10.1080/0144929X.2020.1781259

Cheng, L., F. Liu, and D. D. Yao. 2017. “Enterprise Data Breach: Causes, Challenges, Prevention, and Future Directions: Enterprise Data Breach.” *Wiley Interdisciplinary Reviews. Data Mining and Knowledge Discovery* 7 (5): e1211. https://doi.org/10.1002/widm.1211

Cheng, X., L. Qiao, B. Yang, and X. Zhang. 2024. “Investigation on Users’ Resistance Intention to Facial Recognition Payment: A Perspective of Privacy.” *Electronic Commerce Research* 24 (1): 275–301. https://doi.org/10.1007/s10660-022-09588-y

Chow, R. 2017. “The Last Mile for IoT Privacy.” *IEEE Security & Privacy* 15 (6): 73–76. https://doi.org/10.1109/MSP.2017.4251118

Creswell, J. W. 2017. *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. 5th (international student). edn. London: SAGE Publications.

Cui, L., G. Xie, Y. Qu, L. Gao, and Y. Yang. 2018. “Security and Privacy in Smart Cities: Challenges and Opportunities.” *IEEE Access* 6: 46134–46145. https://doi.org/10.1109/ACCESS.2018.2853985

De Arriba-Pérez, F., M. Caeiro-Rodríguez, and J. M. Santos-Gago. 2016. “Collection and Processing of Data from Wrist Wearable Devices in Heterogeneous and Multiple-User Scenarios.” *Sensors (Basel, Switzerland)* 16 (9): 1538. https://doi.org/10.3390/s16091538

De Cremer, D., B. Nguyen, and L. Simkin. 2017. “The Integrity Challenge of the Internet-of-Things (IoT): On Understanding Its Dark Side.” *Journal of marketing management* 33 (1-2): 145–158. https://doi.org/10.1080/0267257X.2016.1247517

De Keyzer, F., N. Dens, and P. De Pelsmacker. 2021. “How and When Personalized Advertising Leads to Brand Attitude, Click, and WOM Intention.” *Journal of Advertising* 51 (1): 39–56.

De Keyzer, F., N. Dens, and P. De Pelsmacker. 2022. “Let’s Get Personal: Which Elements Elicit Perceived Personalization in Social Media Advertising?.” *Electronic Commerce Research and Applications* 55: 101183. https://doi.org/10.1016/j.elerap.2022.101183

Dogruel, L. 2019. “Too Much Information!? Examining the Impact of Different Levels of Transparency on Consumers’ Evaluations of Targeted Advertising.” *Communication Research Reports* 36 (5): 383–392. https://doi.org/10.1080/08824096.2019.1684253

Donner, H., and M. Steep. 2021. “’Monetizing the IoT Revolution’.” *Sustainability* 13 (4): 1–15. https://doi.org/10.3390/su13042195

Esmaeilzadeh, P. 2019. “The Impacts of the Perceived Transparency of Privacy Policies and Trust in Providers for Building Trust in Health Information Exchange: Empirical Study.” *JMIR Medical Informatics* 7 (4): e14050–e14050. https://doi.org/10.2196/14050

EU General Data Protection Regulation (GDPR). 2016. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation).” *Official Journal L* 119/1.

Ferreira, J. J., C. I. Fernandes, H. G. Rammal, and P. M. Veiga. 2021. “Wearable Technology and Consumer Interaction: A Systematic Review and Research Agenda.” *Computers in Human Behavior* 118: 106710. https://doi.org/10.1016/j.chb.2021.106710

Fox, G., T. Lynn, and P. Rosati. 2022. “Enhancing Consumer Perceptions of Privacy and Trust: A GDPR Label Perspective.” *Information Technology & People* 35 (8): 181–204. https://doi.org/10.1108/ITP-09-2021-0706

Gabriele, S., and S. Chiasson. 2020. “Understanding Fitness Tracker Users’ Security and Privacy Knowledge, Attitudes and Behaviours.” In *2020 CHI Conference on Human Factors in Computing Systems*, 1–12.

Garg, P., and C. R. Murthy. 2019. “A Study of Current State of Privacy Policies in Social Networks.” *Indian Journal of Science and Technology* 12 (29): 1–7. https://doi.org/10.17485/ijst/2019/v12i29/146980

Geradin, D., T. Karanikioti, and D. Katsifis. 2021. “GDPR Myopia: How a Well-Intended Regulation Ended up Favouring Large Online Platforms - the Case of ad Tech.” *European competition journal* 17 (1): 47–92. https://doi.org/10.1080/17441056.2020.1848059

Gill, J. M., T. J. Chico, A. Doherty, J. Dunn, U. Ekelund, P. T. Katzmarzyk, and E. Stamatakis. 2023. “Potential Impact of Wearables on Physical Activity Guidelines and Interventions: Opportunities and Challenges.” *British*

Journal of Sports Medicine 57 (19): 1223–1225. https://doi.org/10.1136/bjsports-2023-106822

Gironda, J. T., and P. K. Korgaonkar. 2018. “iSpy? Tailored versus Invasive Ads and Consumers’ Perceptions of Personalized Advertising.” *Electronic Commerce Research and Applications* 29: 64–77. https://doi.org/10.1016/j.elerap.2018.03.007

Guo, Y., F. Liu, T. Zhou, Z. Cai, and N. Xiao. 2023. “Seeing Is Believing: Towards Interactive Visual Exploration of Data Privacy in Federated Learning.” *Information Processing & Management* 60 (2): 103162. https://doi.org/10.1016/j.ipm.2022.103162

Guo, W., J. Rodolitz, and E. Birrell. 2020. “Poli-see: An Interactive Tool for Visualizing Privacy Policies.” In *Proceedings of the 19th Workshop on Privacy in the Electronic Society*, 57–71.

Gutierrez, A., S. O’Leary, N. P. Rana, Y. K. Dwivedi, and T. Calle. 2019. “Using Privacy Calculus Theory to Explore Entrepreneurial Directions in Mobile Location-Based Advertising: Identifying Intrusiveness as the Critical Risk Factor.” *Computers in Human Behavior* 95: 295–306. https://doi.org/10.1016/j.chb.2018.09.015

Hayes, A. F. 2013. *Introduction to Mediation, Moderation, and Conditional Process Analysis: A Regression-Based Approach*, 34–40. London & New York: Guilford Press.

Herbst, K. C., E. J. Finkel, D. Allan, and G. M. Fitzsimons. 2012. “On the Dangers of Pulling a Fast One: Advertisement Disclaimer Speed, Brand Trust, and Purchase Intention.” *Journal of Consumer Research* 38 (5): 909–919. https://doi.org/10.1086/660854

Jiang, Y., J. Xiao, and J. Wang. 2020. “’Understanding Consumers’ Avoidance of Personalized Advertising in Social Commerce: The Leveraging Effect of Information Transparency and Information Dissemination Scenes.” *WHICEB 2020 Proceedings.*

John, L. K., T. Kim, and K. Barasz. 2019. “Why Am I Seeing This Ad? The Effect of Ad Transparency on Ad Effectiveness.” *The Journal of Consumer Research* 45 (5): 906–932. https://doi.org/10.1093/jcr/ucy039

Kang, H, and E. H. Jung. 2021. “The Smart Wearables-Privacy Paradox: A Cluster Analysis of Smartwatch Users.” *Behaviour and Information Technology* 40 (16): 1755–1768.

Kelley, P. G., L. Cesca, J. Bresee, and L. F. Cranor. 2010. “Standardizing Privacy Notices: An Online Study of the Nutrition Label Approach.” In *Proceedings of the SIGCHI Conference on Human factors in Computing Systems*, 1573–1582. ISO 690.

Kim, T., K. Barasz, and L. K. John. 2021. “Consumer disclosure.” *Consumer Psychology Review* 4 (1): 59–69. https://doi.org/10.1002/arcp.1065.

Kim, S. B., and D. Y. Kim. 2017. “’Antecedents of Corporate Reputation in the Hotel Industry: The Moderating Role of Transparency’.” *Sustainability* 9 (6): 951. https://doi.org/10.3390/su9060951

Kitkowska, A., M. Warner, Y. Shulman, E. Wästlund, and L. A. Martucci. 2020. “’Enhancing Privacy through the Visual Design of Privacy Notices: Exploring the Interplay of Curiosity, Control and Affect’.” In *Sixteenth Symposium on Usable Privacy and Security (SOUPS)*, 437–456.

Kreuter, F., G. Haas, F. Keusch, S. Bähr, and M. Trappmann. 2020. “Collecting Survey and Smartphone Sensor Data with an App: Opportunities and Challenges around Privacy and Informed Consent.” *Social Science Computer Review* 38 (5): 533–549. https://doi.org/10.1177/0894439318816389

Lamprinakos, G., S. Magrizos, I. Kostopoulos, D. Drossos, and D. Santos. 2022. “Overt and Covert Customer Data Collection in Online Personalized Advertising: The Role of User Emotions.” *Journal of Business Research* 141: 308–320. https://doi.org/10.1016/j.jbusres.2021.12.025

Lăzăroiu, G., O. Neguriţă, I. Grecu, G. Grecu, and P. C. Mitran. 2020. “Consumers’ Decision-Making Process on Social Commerce Platforms: Online Trust, Perceived Risk, and Purchase Intentions.” *Frontiers in Psychology* 11: 890–890. https://doi.org/10.3389/fpsyg.2020.00890

Lee, Y., W. Yang, and T. Kwon. 2018. “Data Transfusion: Pairing Wearable Devices and Its Implication on Security for Internet of Things.” *IEEE Access* 6: 48994–49006. https://doi.org/10.1109/ACCESS.2018.2859046

Liu, R., J. Yang, and J. Yao. 2022. “How Smartwatch use Drives User Reciprocity: The Mediating Effects of Self-expansion and Self-extension.” *Frontiers in Psychology* 13: 1041527. https://doi.org/10.3389/fpsyg.2022.1041527

Ly, V., K. S. Wang, J. Bhanji, and M. R. Delgado. 2019. “A Reward-Based Framework of Perceived Control.” *Frontiers in Neuroscience* 13: 65. https://doi.org/10.3389/fnins.2019.00065.

Magrizos, S. 2020. “Teaching Business Ethics in a Digital World.” *Journal of Global Responsibility* 11 (4): 377–386. https://doi.org/10.1108/JGR-02-2020-0026.

Menard, P., and G. J. Bott. 2020. “Analyzing IOT Users’ Mobile Device Privacy Concerns: Extracting Privacy Permissions Using a Disclosure Experiment.” *Computers & Security* 95: 101856. https://doi.org/10.1016/j.cose.2020.101856

Moorman, C., G. Zaltman, and R. Deshpande. 1992. “Relationships between Providers and Users of Market Research: The Dynamics of Trust within and between Organizations.” *Journal of Marketing Research* 29 (3): 314–328. https://doi.org/10.1177/002224379202900303

Onu, E., M. Mireku Kwakye, and K. Barker. 2020. “Contextual Privacy Policy Modeling in IoT,” IEEE Intl Conf on Dependable, Autonomic and Secure Computing, *Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress), Calgary*, AB, Canada, 2020 94-102.

Orazi, D. C., and G. Nyilasy. 2019. “Straight to the Heart of Your Target Audience: Personalized Advertising Systems Based on Wearable Technology and Heart-Rate Variability.” *Journal of Advertising Research* 59 (2): 137–141. https://doi.org/10.2501/JAR-2019-020

Paivio, A. 1971. *Imagery and Verbal Processes*. Holt, NY: Rinehart, and Winston.

Paivio, A. 1975. “Coding Distinctions and Repetition Effects in Memory.” In *The Psychology of Learning and Motivation*, Vol. 9, edited by G. H. Bower, 179–214. New York: Academic Press.

Palmirani, M., G. Bincoletto, V. Leone, S. Sapienza, and F. Sovrano. 2020. “Hybrid Refining Approach of Pronto Ontology.” In *International Conference on Electronic Government and the Information Systems Perspective*, 3–17. Cham: Springer International Publishing.

Pappachan, P., M. Degeling, R. Yus, A. Das, S. Bhagavatula, W. Melicher, P. E. Naeini, et al. 2017. “Towards Privacy-Aware Smart Buildings: Capturing, Communicating, and Enforcing Privacy Policies and Preferences”, *IEEE*, pp. 193.

Paul, N., W. B. Tesfay, D. K. Kipker, M. Stelter, and S. Pape. 2018. “Assessing Privacy Policies of Internet of Things Services.” In *IFIP International Conference on ICT Systems Security and Privacy Protection*, 156–169. Cham: Springer.

Perdana, A., A. Robb, and F. Rohde. 2019. “Interactive Data Visualisation for Accounting Information: A Three-fit Perspective.” *Behaviour & Information Technology* 38 (1): 85–100. https://doi.org/10.1080/0144929X.2018.1514424

Perez, A. J., S. Zeadally, and J. Cochran. 2018. “A Review and an Empirical Analysis of Privacy Policy and Notices for Consumer Internet of Things.” *Security and privacy* 1 (3): 1–15. https://doi.org/10.1002/spy2.15

Perez, A. J., S. Zeadally, and S. Griffith. 2017. “Bystanders’ Privacy.” *IT Professional* 19 (3): 61–65. https://doi.org/10.1109/MITP.2017.42

Portal, S., R. Abratt, and M. Bendixen. 2019. “The Role of Brand Authenticity in Developing Brand Trust.” *Journal of strategic marketing* 27 (8): 714–729. https://doi.org/10.1080/0965254X.2018.1466828

Rapp, A. 2023. “Wearable Technologies as Extensions: A Postphenomenological Framework and Its Design Implications.” *Human–Computer Interaction* 38 (2): 79–117. https://doi.org/10.1080/07370024.2021.1927039

Reich, J. W., and F. J. Infurna. 2016. *Perceived Control: Theory, Research, and Practice in the First 50 Years*. New York: Oxford University Press.

Riva, F., S. Magrizos, I. Rizomyliotis, and M. R. Uddin. 2024. “Beyond the Hype: Deciphering Brand Trust amid Sustainability Skepticism.” *Business Strategy and the Environment* 33 (7): 6491–6506.

Rossi, A., and G. Lenzini. 2020. “Transparency by Design in Data-Informed Research: A Collection of Information Design Patterns.” *The computer law and security report* 37: 105402. https://doi.org/10.1016/j.clsr.2020.105402

Rudolph, M., D. Feth, and S. Polst. 2018. *Why Users Ignore Privacy Policies – a Survey and Intention Model for Explaining User Privacy Behavior*, 587–598. Cham: Springer International Publishing.

Sadeghian, A. H., and A. Otarkhani. 2023. “Data-driven Digital Nudging: A Systematic Literature Review and Future Agenda.” *Behaviour & Information Technology* 43 (15): 3834–3862.

Sanchez, A., and A. J. Kull. 2022. “Don’t put Me on the Spot: The Role of Perceived Intrusiveness in Public Donation Solicitations.” *Psychology & Marketing* 39 (12): 2401–2412. https://doi.org/10.1002/mar.21741

Schaub, F., R. Balebako, and L. F. Cranor. 2017. “Designing Effective Privacy Notices and Controls.” *IEEE Internet Computing* 21 (3): 70–77. https://doi.org/10.1109/MIC.2017.75

Soumelidou, A., and A. Tsohou. 2020. “Effects of Privacy Policy Visualization on Users’ Information Privacy Awareness Level: The Case of Instagram.” *Information technology & people (West Linn, Or.)* 33 (2): 502–534. https://doi.org/10.1108/ITP-08-2017-0241

Statista. 2024a. “Number of Internet of Things (IoT) Connections Worldwide From 2022 to 2023, with Forecasts from 2024 to 2033”. Accessed [01.11.2024] here: https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/.

Statista. 2024b. “Wearables - Statistics & Facts”, Accessed [01.11.2024] here:https://www.statista.com/topics/1556/wearable-technology/#topicOverview.

Sun, Q., M. C. Willemsen, and B. P. Knijnenburg. 2020. “Unpacking the Intention-Behavior gap in Privacy Decision Making for the Internet of Things (IoT) Using Aspect Listing.” *Computers & Security* 97: 101924. https://doi.org/10.1016/j.cose.2020.101924

Surucu, L., F. Yesilada, A. Maslakci, and Faculty of Business Management, European Leadership University. 2020. “Purchasing Intention: A Research on Mobile Phone Usage by Young Adults.” *The Journal of Asian Finance, Economics, and Business* 7 (8): 353–360. https://doi.org/10.13106/jafeb.2020.vol7.no8.353

Tabassum, M., A. Alqhatani, M. Aldossari, and H. Richter Lipford. 2018. “Increasing User Attention with a Comic-Based Policy.” *In Proceedings of the 2018 chi conference on human factors in computing systems*: 1–6.

Tawalbeh, L., F. Muheidat, M. Tawalbeh, and M. Quwaider. 2020. “IoT Privacy and Security: Challenges and Solutions.” *Applied Sciences* 10 (12): 4102. https://doi.org/10.3390/app10124102

Tudoran, A. A. 2024. *Rethinking Privacy in the Internet of Things: A Comprehensive Review of Consumer Studies and Theories*. Internet Research.

Udoh, E. S., and A. Alkharashi. 2016. “’Privacy Risk Awareness and the Behavior of Smartwatch Users: A Case Study of Indiana University Students’.” In *IEEE 2016 Future Technologies Conference (FTC)*, 926–931. https://doi.org/10.1109/FTC.2016.7821714.

Waldman, A. E. 2018. *Privacy, Notice, and Design*. Stanford: Stanford University.

Wang, Y., and C. Herrando. 2019. “Does Privacy Assurance on Social Commerce Sites Matter to Millennials?” *International Journal of Information Management* 44: 164–177. https://doi.org/10.1016/j.ijinfomgt.2018.10.016

Wang, Z., S. Wang, M. Farinella, D. H. Murray-Rust, N. Riche, and B. Bach. 2019. “Comparing Effectiveness and Engagement of Data Comics and Infographics.” In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, 1–12. https://doi.org/10.1145/3290605.3300483

Wottrich, V. M., P. W. J. Verlegh, and E. G. Smit. 2017. “The Role of Customization, Brand Trust, and Privacy Concerns in Advergaming.” *International journal of advertising* 36 (1): 60–81. https://doi.org/10.1080/02650487.2016.1186951

Xue, Y. 2019. “A Review on Intelligent Wearables: Uses and Risks.” *Human Behavior and Emerging Technologies* 1 (4): 287–294. https://doi.org/10.1002/hbe2.173

Zheng, S., N. Apthorpe, M. Chetty, and N. Feamster. 2018. “User Perceptions of Smart Home IoT Privacy.” *Proceedings of the ACM on human-computer interaction* 2 (CSCW): 1–20.