Computers in Human Behavior Reports 15 (2024) 100443

Contents lists available at ScienceDirect

Computers in Human Behavior Reports

journal homepage: www.sciencedirect.com/journal/computers-in-human-behavior-reports

Understanding contextual expectations for sharing wearables' data: Insights from a vignette study

August Bourgeus [a,*], Laurens Vandercruysse [b], Nanouk Verhulst [a,c]

[a] Imec-SMIT, Vrije Universiteit Brussel. Pleinlaan 9, 1050, Brussels, Belgium
[b] Department of Applied Economics, Vrije Universiteit Brussel. Pleinlaan 5, 1050, Brussels, Belgium
[c] Department of Business, Vrije Universiteit Brussel. Pleinlaan 5, 1050 Brussels, Belgium

ARTICLE INFO

Keywords:
Privacy
Contextual Integrity
Wearables
Agency

ABSTRACT

People are increasingly open to sharing personal data collected by wearables, while concerns have emerged on how companies, governments and organisations process this data. This paper applies Nissenbaum's theory of contextual integrity to explore the perceived appropriateness of information flows linked to wearables. A vignette study was conducted (N = 500) to examine the influence of the type of data shared, its purpose, and the sender, on the appropriateness of different wearables' information flow scenarios. Results revealed a significant impact of information type, sharing purpose, and sender on the perceived appropriateness of data sharing. Notably, data collected for research purposes or to develop new functionalities was deemed most appropriate, while data used for advertising was viewed unfavourably. Further, the user-controlled sharing received higher appropriateness ratings. This research underscores the need for meaningful consent in data sharing and suggests that manufacturers of wearable devices should utilise user agency to supplement information flow automation based on societal and contextual privacy norms.

1. Introduction

The market for wearable devices is seeing significant growth, with a rising number of people using these devices to gather personal data during their everyday activities (IDC, 2023). Wearables, such as smartwatches and smart wristbands, come in different shapes and can already collect over 7500 physiological and behavioural variables (The Economist, 2022). People are willing to share that collected data if the perceived value of sharing is high, but recent years have highlighted the shortcomings of organisations' current approach to processing personal data (Lehtiniemi, 2017; Zuboff, 2019). Instances where reasonable user privacy expectations have been violated, such as the Cambridge Analytica scandal, have sparked public debate, policy interventions and research on personal data protection and privacy (Isaak et al., 2018). Over the last few years, legislation has been enacted, attempting to strengthen users' control over (the use of) their personal data (van Ooijen & Vrabec, 2019). However, increased personal control over data remains largely at odds with market incentives (Lazaro et al., 2015). As a result, in practice, internet users still have little control over organisations' data collection practices and are often overwhelmed navigating excessively long and complex privacy policies (Sloan et al., 2013). Consequently, it is unlikely that people will be able to manage all their privacy choices without encountering fatigue or resignation. Thus, there is a need for communal norms that empower users without overburdening them. Nissenbaum (2004) argues that protecting privacy means ensuring that personal information flows appropriately. It is vital to consider the appropriateness of information flows, especially in contexts where interfacing (for consent) is difficult. This is often the case with wearables - sharing data without a user's active intervention - and thus, it forms an ideal basis for our research, as there are different norms and contexts at play when using these.

This paper applies Nissenbaum's (2004) theory of contextual integrity (CI) to investigate the perceived appropriateness of information flows in the context of wearables. Specifically, a full-factorial vignette study was carried out focusing on the type of information shared, the purpose of the data processing, and the sender of the data. This study aims to understand better users' privacy expectations in the context of wearables. As such, this paper contributes to the existing literature on privacy and data sharing by giving insights into privacy norms in the context of wearables.

The findings of our research suggest that privacy management tools can be further improved by incorporating automatic adaptations to cater

* Corresponding author.
E-mail address: august.bourgeus@vub.be (A. Bourgeus).

https://doi.org/10.1016/j.chbr.2024.100443
Received 15 February 2024; Received in revised form 20 May 2024; Accepted 17 June 2024
Available online 20 June 2024

to the privacy expectations of average users, as suggested by (Sanchez et al., 2020) and (Kurtan et al., 2021). Partial consent automation will arguably be necessary to transition toward a paradigm where meaningful consent and agency for end users can be achieved (Le Métayer & Monteleone, 2009). Moreover, insights into specific configurations of CI parameters deemed appropriate by consumers are crucial to inform organisations' privacy practices proactively. For example, responsible innovation and concurrent data sharing in line with societal expectations arising from our research can help companies avoid backlash from perceived privacy violations (e.g., Hull et al., 2011). Thought leaders from various domains (e.g., management, marketing) have not only extensively called for in-depth investigations on the factors underlying consumers' willingness to share data, but also for more emphasis on privacy concerns (e.g., De Keyser et al., 2021; Schweidel et al., 2022). In contrast with previous research, our study took agency into consideration and highlighted the importance of user-controlled sharing, which garners higher appropriateness ratings. We try to understand the granularity of appropriateness ratings and hence contribute to a deeper understanding of consumer attitudes towards data sharing in wearable technology contexts. In the following section, the literature that supports the research approach is presented. Next, the methodology is discussed. Further, the findings are analysed. Finally, the implications of our findings are evaluated.

2. Literature study

2.1. Personal data sharing

Trust in digital service providers has decreased over the years. In response, a policy push in the European Union (EU) has been centred around improving trust in online services by empowering users (European Commission, 2020). The most evident example of an empowerment measure is that users must be asked whether they would accept that their data is collected and used in certain cases. This 'consent' is a prime legal basis for collecting and processing personal data under the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/579). The entry into applicability of GDPR in 2018 made internet users acutely aware of the existence of the legal basis for consent through, among others, the widespread appearance of cookie banners.

Using consent to legitimise personal data processing is not uncontroversial. It has been argued that the highly complex and largely opaque nature of current digital ecosystems leads to users' inability to make informed decisions about the collection and processing of their data per se (Solove, 2006). Among others, users encounter time constraints, knowledge gaps, cognitive biases, and service dependency when handling privacy choices via consent (Kröger et al., 2021). Such issues form substantial obstacles to informed and rational privacy choices. For example, there is a discrepancy between people's time constraints and the time necessary to exercise meaningful control over privacy choices (Obar, 2015). For example, Gauttier (2019) revealed that the mere act of seeking employees' consent for the implementation of a stress-monitoring wearable device is not adequate. Ebert et al. (2021) found that concise privacy policies can increase user awareness of data practices and lead to more informed decisions. Furthermore, there are widespread misconceptions about data protection law (Solove, 2013).

Users often lack the knowledge to make proper decisions when faced with privacy choices (Weinshel et al., 2019). As a case in point, (Ben--Shahar & Schneider, 2011; Calo, 2011) show that users often ignore information that seems meaningless. Such issues form substantial obstacles to informed and rational privacy choices. The desired level of user empowerment and control is rarely achieved. Besides user constraints, there are data-collecting organisations that nudge users to share a lot of data and restrict their ability to negotiate privacy choices (e.g. by using dark patterns) because of financial incentives (Kröger et al., 2021).

2.2. Privacy

The concept of privacy is dynamic across cultures and over time (Kasper, 2005). Historically, the focus has often been on the individual. First, privacy has been understood as the ability to restrict access to sensitive information. The perspective was conveyed by either disclosing details or maintaining confidentiality. Sloan and Warner (2013) define privacy as the ability to determine for yourself when and how others may collect and use your information. A sufficiently broad ability to provide or withhold free and informed consent for intended uses is necessary to ensure adequate informational privacy (Sloan & Warner, 2013). Second, Westin (2003) gauges privacy through surveys that classify individuals based on their level of concern about privacy or the importance and strength of maintaining control over access to data from or about themselves. Third, the privacy calculus hypothesis states that privacy is a commodity that can be exchanged for benefits, such as other commodities or free services (Dinev & Hart, 2006). An individual may weigh the pros and cons of utilising technologies based on their value-in-use and level of convenience and effectiveness. This decision is often based on the data type (e.g. often sharing an email address to log in to a service) and considering the specific characteristics and vulnerabilities inherent to the shared data.

Privacy was defined as "an individual's space, which was seen as necessary for meeting the individual's vital interests" (Becker, 2019, p. 307), yet in the last decades, we have seen a shift to a more dynamic and social definition of privacy. Indeed, relying on one dimension, such as the sensitivity of information type or privacy categorisation of the respondent, is too limiting (Hoyle et al., 2020). As digitalization becomes omnipresent, the limitations of considering privacy as a static concept become visible. Dispositional approaches, which presume that people's behaviour remains constant over time and is not influenced by situational and contextual parameters, cannot explain how individuals adapt to changing circumstances, such as the complexity of novel data sources or data management techniques (Ackermann et al., 2022). Some scholars indicated that privacy preferences and sensitivity labels prove to be highly influenced by the context and use of the situation (Cohen, 2013; Hoel et al., 2020; Martin & Nissenbaum, 2016; Nissenbaum, 2010). Recently, Colnago et al. (2023) reaffirmed that privacy preferences should be understood within their context. Ebert et al. (2020) noted that while researchers have studied the factors influencing general concerns, research on factors affecting concerns in specific situations and contexts is still lacking.

2.3. Privacy as contextual integrity

Nissenbaum (2010) presented the theory of CI in her book 'Privacy in Context: Technology, Policy, and the Integrity of Social Life'. Contextual integrity demands appropriate information gathering and dissemination in specific contexts, following governing norms of distribution. She states that privacy protection is not about stopping an information flow or being secretive but simply a matter of appropriate information flow. For example, a doctor receiving a patient's MRI scan to diagnose an illness could generally be considered an appropriate information flow, whereas an e-commerce actor receiving this scan is inappropriate. For almost two decades, the theory of CI has played a significant role in understanding the various, and sometimes conflicting, privacy practices that emerged as technology became more ubiquitous. Since then, CI theory has been applied in different studies and contexts (e.g., Apthorpe et al., 2018; Grodzinsky et al., 2011; Norval et al., 2017; Zhang et al., 2022) and is mainly used to test whether new technologies comply with the consensus on privacy in modern societies.

Generally, an appropriate information flow is determined by adhering to established contextual norms, which can be described using five CI parameters: three actor parameters (sender, recipient, and information subject), a parameter specifying the information type, and the transmission principle parameter dictating the information flow

conditions. The transmission principle covers a wide variety of possible factors (Nissenbaum, 2010). For example, Harborth et al. (2021) manipulated the transmission principle by introducing the permission justification as a way to introduce transparency and provide a valid purpose for collecting. According to CI theory, it is crucial to determine the values of all five parameters to assess the privacy impact of any information flow practice (Nissenbaum, 2004). Societal norms affect these parameters by shaping our privacy expectations and governing the flow of personal information in a specific context. For example, most users will happily share their address and age to get a public transport subscription but not to buy groceries in a supermarket (cf. purpose parameter).

Indeed, privacy norms are formed within a social contract (Culnan, 1995; Dunfee et al., 1999; Martin, 2012). It has been argued that: "these social contracts are the unstated agreements that individuals and groups make in contexts, communities, and relationships" (Martin, 2016, p. 553). In this case, privacy-specific risks and benefits are related to fulfilling contextual norms and goals. Whenever norms are breached, a 'violation of privacy occurs', Nissenbaum (2004) argues. Martin and Nissenbaum (2015) argue that releasing information is not the same as giving up privacy if the flow is appropriate. For example, you do not give up privacy by sharing medical data to get better healthcare because sharing data in this context is morally justifiable and often politically enforced. However, contextual purposes and values may disfavour the user's interests, such as the continuous disclosure of information during the COVID-19 pandemic (Bernes, 2022). The expectations of what is deemed appropriate can vary over time and may differ among different cultures (Oghazi et al., 2020). Barkhuus (2012) advocates using CI in privacy-related user studies, which aim to comprehend the contextual parameters behind people's privacy concerns or lack thereof.

2.4. Contextual integrity theory and wearables

CI has been applied in various studies and different contexts (e.g. Apthorpe et al., 2018; Grodzinsky et al., 2011; Norval et al., 2017; Zhang et al., 2022) such as the context of augmented reality apps (Harborth et al., 2021), photo posting online (Hoyle et al., 2020), smart homes (Apthorpe et al., 2018), covid-19 vaccination certificates (Zhang et al., 2022), and accessing public records (Martin & Nissenbaum, 2016). Apthorpe et al. (2018), who investigated the appropriateness of information flows in smart homes, provided actionable recommendations based on discovered privacy norms for device manufacturers. They found that privacy policies should clearly state transmission principles and that device communications should directly support the device's primary functionality (Apthorpe et al., 2018). Harborth and Pape (2021) derived a new structure of permissions for augmented reality apps, which were more context-dependent. They urge developers to find a good balance between offering transparency to the consumer and privacy fatigue.

The theory of CI is particularly beneficial for grasping the impact of emerging and evolving norms associated with the introduction of new technology. This paper applies CI theory to the context of wearables. A consumer wearable is "a computer with embedded sensors and actuators/output devices developed as a garment, accessory, or device that is worn (or carried) by a person and easily purchased through retailers" (Perez & Zeadally, 2018, p. 47). Recently, wearables (e.g., smartwatches) have gained popularity and been democratised. Motti and Caine (2015), who analysed online reviews of different wearables, showed that users' privacy concerns depend on which wearable they use, which data are collected (cf. information type) and which sensors are included in the wearable, thus supporting CI in the wearable context.

Wiesner et al. (2018) shed light on the motivational and privacy aspects of wearables, used for exercise activities, in Germany. They showed that 35% of runners would not allow vendors to share their data with third parties for commercial purposes. In cases of voluntary data sharing, 52% allowed to share their exercise data. Further, they found a difference in privacy concerns between users, especially for the older age groups. Privacy remains one of the primary hurdles to overcome in wearable computing, just like with ubiquitous and mobile computing. Not only because wearables capture, analyse, and preserve sensitive information about users but also because they can do so seamlessly and constantly without attracting attention (Motti et al., 2015).

In sum, preliminary evidence shows the importance of contextual parameters in privacy expectations and data sharing behaviour. However, an investigation of CI parameters in the context of wearables is currently missing from the literature. Therefore, this study investigates the impact of the type of information shared, how information is shared (e.g., I vs application), and the purpose used on the perceived appropriateness of information flows in the context of wearables.

Research Questions.

RQ 1: How do the type of information shared, the sender of information, and the purpose impact the appropriateness of certain information flows in the context of wearables?
RQ 2: How do individual privacy preferences influence the appropriateness of certain information flows in the context of wearables?

3. Methodology

This paper employs a full factorial vignette experiment to assess the appropriateness of 18 selected information flows concerning wearables. The study focuses on the influence of CI parameters, such as information type, sender, and purpose, as well as the impact of privacy profiles. This section outlines the study design and procedure, after which the vignette compilation is explained.

3.1. Design & procedure

A sample of 500 Flemish respondents, representative on age and gender (Mean age 46 years; 54.6 % women), participated in a full factorial 3 × 2 × 3 vignette experiment. Participants were recruited through the ISO-20252-certified recruitment panel company Bilendi and paid in credits that respondents could exchange for products or cash.

Before the start of the experiment, respondents read a short introduction and filled out the informed consent. Next, respondents filled out two demographic questions and the commonly used 3-item Privacy Segmentation Index (Kumaraguru et al., 2005) based on (Westin, 2003). This scale uses a 4-point Likert scale ranging from strongly disagree to strongly agree. This index classifies users into three privacy types, namely fundamentalists (very privacy-protective), pragmatists (privacy neutral), and unconcerned (least privacy-protective).[1] 66.2% of our respondents are classified as privacy pragmatists, 23.8% as fundamentalists and 10% as Unconcerned. This aligns with prior studies using this index (Motti et al., 2015). Subsequently, the respondents got a brief explanation of what to expect in the following part of the study, a brief explanation of what wearables entail, and were asked to indicate if they have used a wearable already. Finally, each respondent was presented with 18 vignettes on wearable data sharing in a randomised order and was then asked to score each vignette on its appropriateness by way of a 7-point Likert scale (Cf. Table 1). Respondents went through the 18 vignettes at their own pace but were not allowed to return to previous responses. The participants filled out an attention check after rating nine vignettes.

3.2. Vignettes

A vignette is a short, constructed description of a person, object, or situation (i.e., a scenario). A vignette-based methodology is ideal for

[1] PSI was obtained before showing the vignettes in order not to prime respondents.

Table 1
Vignette example (Original in Dutch, freely translated to English).

While using a wearable device, you decide to share information about yourself, including your risk of developing heart disease. This information is used so that you receive customised, targeted advertisements.
How comfortable are you with the above information sharing when using a wearable? Very inappropriate Inappropriate Mostly inappropriate Not appropriate nor inappropriate Mostly appropriate Appropriate Very appropriate

investigating human judgment and attitudes (Atzmüller et al., 2010; Korir et al., 2023). We created 18 vignettes on sharing wearable data, in which three parameters varied: information type, sender, and purpose. All vignettes were adapted based on the following template: "*While using a wearable, **the sender** shares information about you, including **information type,** in order to **purpose**"*, and respondents were asked to rate how appropriate they find this information-sharing scenario when using a wearable on a 7-point Likert scale (1 = highly inappropriate; 7 = highly appropriate; see Table 1 for example).

Information type factor. We used the adapted taxonomy of personal data categories of Abrams (Abrams, 2014; OECD, 2019), which distinguishes between three categories of data: provided, observed, and inferred data. We chose three information types that were relevant within this context of wearables: location data (observed), weight (provided), and health profile (inferred).

Sender factor. This factor has two levels: either 'the application' automatically shares the data, or you decide to share the data yourself. We operationalised the sender factor by distinguishing between scenarios where the user actively decides to share data and those where the application autonomously shares data on behalf of the user. This distinction aimed to capture differences in user perception and behaviour regarding voluntary versus automatic data sharing, which are pivotal in the context of wearable technologies. The relative size of the effects remains consistent, as our comparison involves 'the system decides to share' and not 'the system is given the option to share,' focusing on actual information flows rather than potential ones. It is essential that the respondent clearly understands the difference between these two levels. We are particularly interested in whether the amount of agency over sharing personal data influences the respondent's appropriateness ratings.

Purpose factor. This factor provides a reason under which an information flow occurs (i.e. when data can be shared). Transmission principles in CI refer to the constraints on the flow of information, which can be defined broadly or narrowly. For this study, we decided to consider a purpose factor, following (Gilbert et al., 2021; Harborth et al., 2021). The purposes were related to the secondary use of the collected data. This implies that the vignettes will provide an explanation of the additional purposes for which the data will be used other than the basic functionality of wearables. We have identified three such purposes: developing new functionalities, conducting scientific research, and receiving customised and targeted advertisements.

In line with Martin and Nissenbaum (2016) and Apthorpe et al. (2018), keeping some parameters fixed or having a relatively small number of options reduces cognitive fatigue for participants. Varying the three parameters (type, sender, purpose) covers a variety of purposes for processing information in the context of wearables. The subject was fixed to be the data subject across the 18 vignettes. We fixed the recipient to be the application, which improved the relevance of information flows and produced clearer results by controlling variables in this way.

4. Results

The data was analysed using a cumulative link mixed effects model (CLMM) and was grouped by respondent and vignette, including interaction effects between CI factors.[2] The model summary can be found in Table 2. Concretely, the data were analysed on two levels: variation in privacy ratings attributable to the contextual parameters and variation in privacy judgments attributable to the respondent-level variables (i.e., the Westin profiles and socio-demographic variables). The data are balanced because each vignette is equally often measured, meaning that every respondent rated 18 vignettes. A CLMM is most appropriate because the rating variable is an ordinal Likert scale, and respondents rated multiple vignettes, so there is a chance these ratings are correlated (Gilbert et al., 2021; Taylor et al., 2023). For example, some respondents might have a general tendency to rate higher or lower than others, regardless of the vignette. By grouping the data per respondent, we acknowledge this possibility and estimate a random intercept for each respondent. The random intercepts capture individual-level variations in the ratings that are not explained by the fixed effects (Taylor et al., 2023). A CLMM model with random intercepts for each respondent allows us to model the within-respondent correlation in ratings, which can lead to more accurate estimates of the fixed effects. Additionally, more precise estimates of the random effect variances are obtained, which

Table 2
Regression of Appropriateness of Information flow on Vignette and Respondent Factors.

Coefficients:	Estimate	Std. Error	z value	p-value
SenderUser	0.29998	0.12100	2.479	<0.05
TypeLocation	−0.56031	0.12069	−4.643	<0.01
TypeWeight	−0.38937	0.11988	−3.248	<0.01
PurposeFunctionalities	1.82975	0.11920	15.350	<0.01
PurposeResearch	2.63302	0.12318	21.375	<0.01
SenderUser:TypeLocation	0.16689	0.16995	0.982	0.32610
SenderUser:TypeWeight	−0.03023	0.16950	−0.178	0.85847
SenderUser: PurposeFunctionalities	0.07005	0.16609	0.422	0.67319
SenderUser: PurposeResearch	−0.03603	0.16927	−0.213	0.83143
TypeLocation: PurposeFunctionalities	−0.52451	0.16606	−3.159	<0.01
TypeWeight: TransmissionFunctionalities	−0.20024	0.16461	−1.216	0.22383
TypeLocation: PurposeResearch	−0.79184	0.16887	−4.689	<0.01
TypeWeight: PurposeResearch	−0.27526	0.16826	−1.636	0.10185
SenderUser:TypeLocation: PurposeFunctionalities	−0.01564	0.23403	−0.067	0.94673
SenderUser:TypeWeight: PurposeFunctionalities	0.19330	0.23283	0.830	0.40643
SenderUser:TypeLocation: PurposeResearch	0.01161	0.23746	0.049	0.96102
SenderUser:TypeWeight: PurposeResearch	0.25920	0.23727	1.092	0.27464

[2] As a robustness test, we included the Westin privacy profiles as additional variables in another CLMM. The results and effects remained generally consistent with our primary analysis, suggesting that the inclusion of these variables did not significantly alter the overall findings.

helps to understand the variability in the ratings due to unobserved respondent-level factors. These insights can be found in Table 3.

Table 3 describes the random effects of our model. The low variance for vignettes in the random effects component indicates that the variation in ratings across vignettes is relatively small compared to the variation in ratings due to other factors in the model, such as the fixed effects (Sender, Type, Purpose) and the random effect of the respondent. Thus, there is a low likelihood of unmeasured characteristics or factors inherent to the vignettes influencing the ratings.

For the sake of completeness, we also report the results of the various individual vignettes with respect to appropriateness. Table 4 describes the mean appropriateness ratings and the mean Likert result for the different vignettes.

To respond to Research Question 1, as can be gleaned from Table 2, we show that all the contextual parameters significantly impact the appropriateness of information flows. Information type and purpose are the most important contextual parameters that impacted respondents' appropriateness scores. Vignettes in which data is collected to either 'Develop new functionalities' or to use in 'Research' had the highest positive impact on appropriateness rating. In contrast, the utilisation of data for advertising purposes is deemed inappropriate. Notably, the information type 'Location' and 'Weight' exhibit a negative coefficient, suggesting that individuals find disclosing information pertaining to the risk of heart disease more appropriate across different purpose and sender combinations. In addition, two significant interaction effects were observed (see Table 2). The use of location data slightly diminished the perceived appropriateness of sharing information to enhance wearable functionalities and sharing location data for scientific research purposes was rated as less appropriate compared to other types of data for the same research purposes. The other interactions between sender, type, and purpose were not significant, indicating that these combinations do not have a strong impact on the appropriateness ratings.

Fig. 1 displays the mean appropriateness ratings per information type and purpose level. It can be discerned that differences in ratings between the three purposes remain consistent across all information type levels. Although information on the risk of a heart disease was generally rated highly, there was notable variability in the ratings. This suggests differing views among respondents on its appropriateness, even for research purposes. For Location information, there is a considerable spread in the ratings, particularly when shared for ads, indicating diverse opinions about the appropriateness of sharing location data. For Weight information, the ratings exhibit a moderate range, especially for ads and functionalities, suggesting mixed feelings among respondents regarding the appropriateness of sharing weight information. Whether a respondent had or used a wearable had no significant influence on respondents' ratings.

The sender parameter is also of significant importance across all vignettes. Fig. 2 displays the average appropriateness rating for various contexts. The dashed line represents average ratings of vignettes where the user was the sender, while the full line represents contexts where the sender was the device. Vignettes where the sender is the user generally have a higher appropriateness rating than vignettes where the sender is the device itself. The difference in appropriateness is significant over 7 of the 9 context combinations (information type x purpose). As shown in Fig. 2, vignettes where weight information and risk of heart disease information were collected for research purposes were deemed most appropriate, regardless of whether the sender was the user or the device itself. User agency (i.e., sender) was not a statistically significant parameter for appropriateness in two instances, namely those concerning sharing weight information and heart disease risk for the purpose of receiving tailored advertisements.

Table 3
Random effects.

Random effects:	Variance	Std.Dev.
Respondent (Intercept)	3.511	1.874
Vignette (Intercept)	0.0000	0.000

Table 4
Appropriateness of Information flow per vignette.

Nr.	Sender	Type	Purpose	Mean	Appropriateness
1	Device	Weight	Functionalities	3,90	Nor Appropriate, Nor Inappropriate
2	Device	Weight	Ads	2,84	Quite Inappropriate
3	Device	Weight	Research	4,34	Nor Appropriate, Nor Inappropriate
4	Device	Location	Functionalities	3,58	Nor Appropriate, Nor Inappropriate
5	Device	Location	Ads	2,77	Quite Inappropriate
6	Device	Location	Research	3,93	Nor Appropriate, Nor Inappropriate
7	Device	Disease	Functionalities	4,29	Nor Appropriate, Nor Inappropriate
8	Device	Disease	Ads	3,10	Quite Inappropriate
9	Device	Disease	Research	4,73	Nor Appropriate, Nor Inappropriate
10	User	Weight	Functionalities	4,27	Nor Appropriate, Nor Inappropriate
11	User	Weight	Ads	3,03	Quite Inappropriate
12	User	Weight	Research	4,66	Quite Appropriate
13	User	Location	Functionalities	3,93	Nor Appropriate, Nor Inappropriate
14	User	Location	Ads	3,05	Quite Inappropriate
15	User	Location	Research	4,22	Nor Appropriate, Nor Inappropriate
16	User	Disease	Functionalities	4,55	Quite Appropriate
17	User	Disease	Ads	3,28	Quite Inappropriate
18	User	Disease	Research	4,93	Quite Appropriate

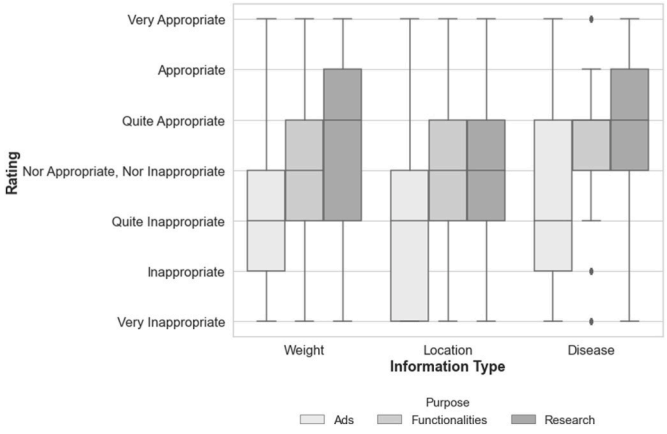

Fig. 1. Mean appropriateness ratings over Type and Purpose.

To investigate the impact of Westin's privacy profiles on the appropriateness of information flows in the context of wearables (cf. RQ2), we plotted mean rating scores by profile, and several one-way ANOVAs were carried out. The profiles significantly affected the appropriateness of information flows. A post-hoc Tukey's HSD test showed a significant difference between the ratings of the three privacy profiles (see Table 5). More specifically, the "privacy unconcerned"-participants found vignettes, in general, more appropriate than the "privacy pragmatists" or "privacy fundamentalists".

Furthermore, we show that there is a visible difference in appropriateness ratings between the privacy profiles over the three purpose levels. See Fig. 3 for mean appropriateness ratings visualised by privacy profile per purpose level. Privacy unconcerned respondents are most comfortable with information flows for different purposes, consistently giving higher appropriateness ratings across Ads, Functionalities, and Research. Privacy pragmatists show moderate comfort levels, while privacy fundamentalists rate the appropriateness lower across all

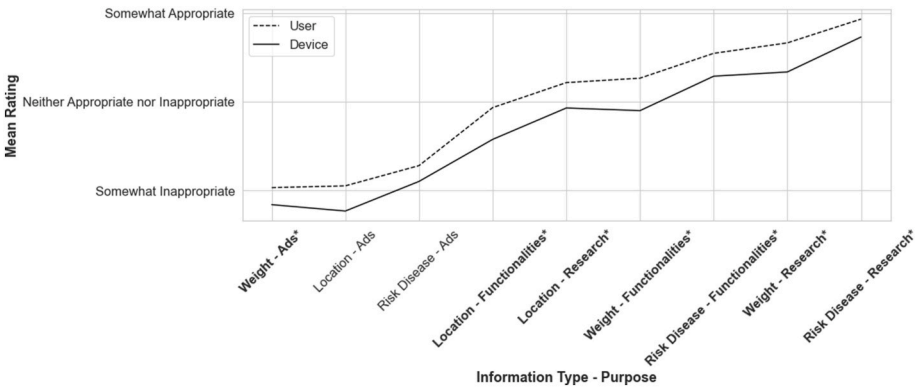

Fig. 2. Mean ratings Sender by Information type, Purpose.

Table 5
Post-hoc Tukey's HSD test.

group1	group2	meandiff	p-adj	lower	upper	reject
Fund	Prag	0.672	0.0	0.4091	0.9349	True
Fund	Uncon	1.2034	0.0	0.7889	1.6179	True
Prag	Uncon	0.5314	0.0025	0.1583	0.9046	True

purposes, reflecting their cautious stance on information sharing.

5. Discussion

Our study clearly indicates that the appropriateness of information flows while using wearables depends on contextual parameters. All three CI parameters had a significant impact on the appropriateness of data sharing. Unsurprisingly, information flows for advertising purposes are deemed the least appropriate. However, we uncovered surprising interactions between sender agency and contextual integrity parameters, shedding light on when users prefer control over data sharing and when they may relinquish it.

We showed that the purpose of an information flow (e.g., developing new functionalities) is the key parameter influencing the appropriateness of wearable data sharing. Placing restrictions on why the information is shared (such as limiting data processing purpose or use) increases the overall appropriateness of the flow of information, which is in line with the purpose limitation principle in GDPR. Besides, as users are overwhelmed with privacy choices, they might be unaware that particular information flows exist and, when revealed, can cause serious consternation.

One remarkable insight was that people deemed it less appropriate to share their weight and location compared to data on heart disease risk. One potential explanation is that the risk of having a heart disease is something unsure (i.e., it could or could not manifest in the future). In contrast, weight and location data are an objective given (i.e., certain at present). This could indicate that future uncertain harms are discounted more heavily (Mcnally, 2021). Respondents could also feel that the utility/value of discovering a heart disease exceeds that of having privacy. This aligns with the rationale of offering privacy in the quest for improved public health, as in (Kokkoris & Kamleitner, 2020).

There is a significant difference between appropriateness ratings for users with versus without agency for seven out of nine situations. This finding is in line with, among others, Urbonavicius et al. (2021), who found that user agency over personal data processing boosts trust levels and information disclosure. For the scenarios on sharing weight information and the risk of heart disease for personalised ads, no differences were found. This suggests that users feel very strongly about not wanting personalised ads, therefore, agency might not be necessary as we know that people already install broad spectrum adblockers to counter these (Miroglio et al., 2018). However, agency does enhance the appropriateness rating of location-based advertisements. This adds empirical evidence to claims by Lambillotte et al. (2022), who have recently shown that the negative impact of personalisation on privacy concerns may be mediated by 'perceived control.' Our contribution shows that while that might be the case for some types of ads, these claims cannot be generalised to all types of ads in every context.

Individual agency and control do not constitute the be-all and end-all when it comes to facilitating effective data protection. EU regulation seeks to shift the locus of agency and control towards the user in an effort to transform the user from a passive into an active participant in the processing of personal data (European Commission, 2020). Interestingly, merely providing control over data collection has paradoxically little effect due to low awareness of what data users generate and

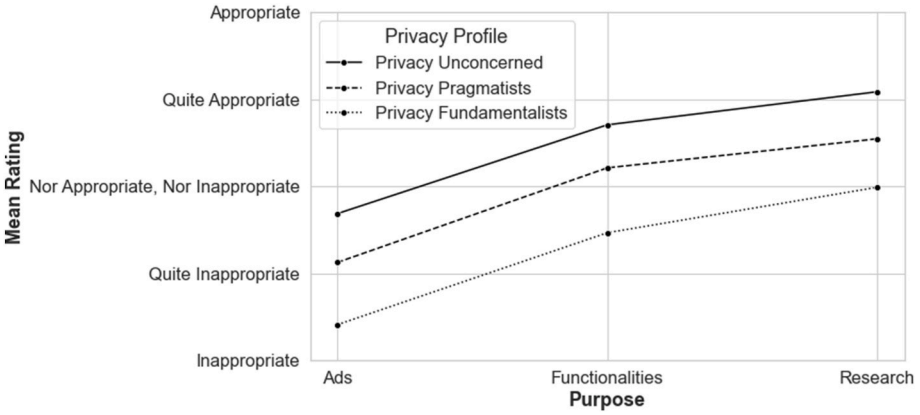

Fig. 3. Mean ratings by Purpose and Privacy Profile.

confusion about what choices they have (Johnson et al., 2020). In contemporary society, the management of privacy is a multifaceted issue negotiated not only at an individual level but also at a group or community level, encompassing the involvement of various entities such as companies and third parties. In this hyperconnected world, personal information can be easily shared or posted on various online channels, necessitating greater awareness of group privacy and connected security concerns (Floridi et al., 2017).

This research is the first step in uncovering how people perceive different information flows in the context of wearables, hence deriving contextual norms. For example, this study illustrates that sharing information for research is generally deemed appropriate. As Nissenbaum rightly states, appropriate information flow is determined by adhering to established contextual norms. Defining these established norms is vital in understanding how people perceive information flows. These norms can be leveraged to define generally accepted consents. These are consents that users generally accept as they adhere to contextual norms. In practice, users will not have to interact with a system for these consents as this could be an automated process, unburdening the user. Taking out or automating the obvious consents can lead to meaningful consent, as users must only consider consents that could be more complex. More individually oriented or preference-specific consents can be prioritised. Our empirical research contributes to the ongoing evolution of CI theory, enhancing its applicability and relevance in understanding privacy in contemporary technological contexts. While CI is a well-established privacy theory, operationalising it can be challenging in practical settings. In our study, we address this challenge by focusing on operationalising the sender parameter, particularly by examining the role of user agency over information flows. By doing so, this paper provides empirical insights that enrich the theoretical understanding of CI and its application in real-world contexts.

Expressing individual consent is vital for advancing interests, but privacy is crucial in limiting data flows to maintain societal and contextual norms. To proceed towards meaningful consent, we need to make sure that users are actively interacting with a service when they need to. For example, for research purposes, Norval and Henderson (2017) argue that giving the ability to consent to projects and alter consent preferences easily can enable more engaged participants, streamlined recruitment, improved public trust, and the knowledge that their research conforms to high legal standards. To ensure genuine empowerment by meaningful consent, it is imperative to have a comprehensive understanding of privacy norms and the user's need for agency.

Manufacturers of wearable devices may benefit from our findings, which indicate that the variations in appropriateness ratings of information exchanges are particularly significant given the pervasive nature of data sharing in such devices. These devices share data on numerous occasions without active user participation. Wearables could offer control to users where users actually value this control or agency. Our findings suggest that wearable device manufacturers should consider user preferences for data control more deeply. For example, enhancing user control settings to allow more granular preferences regarding data sharing based on the type of data and its intended use. Whereas previous studies have mostly focused on contextual privacy in broader digital interactions, our study provides timely empirical evidence on how contextual factors are perceived in the domain of wearables. The increasing use of wearables for healthcare purposes makes the need to have appropriate information flows and best practices even more vital.

6. Limitations and future research

Our study shows that context is crucial to determine data sharing appropriateness, yet this is based on a single country sample at a specific moment. Although the quality of the professionally recruited sample instils confidence in the sample and measurements, it is important to recognise that the ability to generalise the findings may be constrained. Indeed, cultural norms (Oghazi et al., 2020) and temporal societal changes (Zhang et al., 2022) (e.g., COVID-19 pandemic, economic crisis) can impact users' privacy attitudes and concerns.

We administered the Privacy Segmentation Index questions before the experiment to establish a baseline of participants' privacy attitudes. By assessing respondents' privacy attitudes upfront, we sought to capture their predispositions towards privacy concerns before exposing them to specific wearable-related scenarios. While we acknowledge potential priming effects, our study did not allow us to make direct statements about such effects. Additionally, vignettes have some limitations in investigating user attitudes and behaviours. The social dynamics and structures that shape how people rate information flows are complex. Within CI, it is possible to characterise each information flow by deriving five distinct parameters. In accordance with prior research rooted in CI-based surveys, our investigation is constrained to the realm of information flows defined by the specific values of CI parameters. Following Martin & Nissenbaum, we chose to manipulate three parameters and keep the subject and recipient parameters fixed. Concerning the purpose principle, we focused on specific secondary use (i.e. purposes beyond the basic functionality of a wearable). This implies that the data will only be used for the purpose described in the specific vignettes. However, we cannot guarantee that individuals will not imagine the data types presented in the examples would be used for other, unintended purposes. Further, the scenario text '*you decide to share information about yourself*' in the Sender variable emphasised user agency and differentiated it from automated data sharing. However, it might have induced a bias toward higher appropriateness ratings, as participants could perceive their hypothetical decisions as inherently justified.

In future work, researchers could expand the work by investigating norms in different contexts or by scaling the vignette method. Researchers should also consider focusing on actual data sharing behaviour. As discussed in the literature, there could be a mismatch between people's ratings of appropriateness and what they would do in real-life situations (cf. Attitude-behaviour gap). To gain a more profound insight, it is necessary to assess participants' reasoning and the right equilibrium between individual values (e.g., trust) and societal values (e.g., national security, safety) and objectives such as enhancing system efficiency or user productivity that play a role in shaping the development of these norms. To provide deeper insights into the effects of user choice on the perceived appropriateness of information sharing, the appropriateness of the reception of various consent requests, rather than the actual information flows, could be investigated. Lastly, it is essential to acknowledge the limitations of Westin's profiles and consider more nuanced and contextually sensitive approaches when analysing privacy concerns in today's digital environment. We are realistic about its reliable fundamentals and limits. However, Westin's scale was used as a secondary measure within our research.

7. Conclusion

Our research underscores the influence of contextual parameters on people's assessments of the appropriateness of information flows in the context of wearable technology. We found that the purpose of information sharing, particularly for advertising, significantly affects appropriateness ratings, and restricting the purpose of data transmission enhances overall appropriateness. Notably, we observed that sharing weight and location data was considered less appropriate than sharing data on heart disease risk, possibly due to the perceived utility of health-related information. Our study also revealed differences in appropriateness ratings between situations where users had agency and those where they had less agency, suggesting the need for a nuanced approach to user control in data sharing.

This research underscores the potential for automated, context-based consent mechanisms to streamline user interactions with wearable technologies. These mechanisms could operate by pre-configuring consent preferences, automatically adjusting privacy settings, and consent

requirements that depend not only on the sharing context but also on established norms and user-specific preferences. To illustrate, typical uses of data that align with widely accepted norms (such as sharing anonymised health data for public health research) could be processed with minimal user interaction, while uses that deviate from these norms (such as using sensitive location data for targeted advertising) would potentially automatically lead to not sharing this information in this context or prompt for explicit consent.

These norms could, in later stages, be used as the backbone for sector-specific privacy legislation and/or technical system requirements, to get the practice of data processing more in line with societal expectations. Balancing individual consent with societal and contextual norms is crucial for meaningful consent, and understanding privacy norms and the need for user agency is central to achieving this goal.

CRediT authorship contribution statement

August Bourgeus: Writing – review & editing, Writing – original draft, Visualization, Methodology, Investigation, Formal analysis, Conceptualization. **Laurens Vandercruysse:** Writing – review & editing, Supervision, Methodology, Conceptualization. **Nanouk Verhulst:** Writing – review & editing, Conceptualization.

8. Declaration of AI and AI-assisted technologies in the writing process

During the preparation of this work, the author(s) used Grammarly in order to improve the phrasing, spelling and flow of the text. After using this tool, the author(s) reviewed and edited the content as needed and take(s) full responsibility for the content of the publication.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

The authors do not have permission to share data.

Acknowledgements

The research is supported by SolidLab Vlaanderen (Flemish Government, EWI and RRF project VV023/10). The research design was approved by the ethical committee of the Vrije Universiteit Brussel.

Appendix A. Supplementary data

Supplementary data to this article can be found online at https://doi.org/10.1016/j.chbr.2024.100443.

References

Abrams, M. (2014). The Origins of personal data and its implications for governance. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2510927

Ackermann, K. A., Burkhalter, L., Mildenberger, T., Frey, M., & Bearth, A. (2022). Willingness to share data: Contextual determinants of consumers' decisions to share private data with companies. *Journal of Consumer Behaviour, 21*, 375–386. https://doi.org/10.1002/cb.2012

Apthorpe, N., Shvartzshnaider, Y., Mathur, A., Reisman, D., & Feamster, N. (2018). Discovering smart home internet of Things privacy norms using contextual integrity. *Proc ACM Interact Mob Wearable Ubiquitous Technol., 2*, 1–23. https://doi.org/10.1145/3214262

Atzmüller, C., & Steiner, P. M. (2010). Experimental vignette studies n survey research. *Methodology, 6*, 128–138. https://doi.org/10.1027/1614-2241/a000014

Barkhuus, L. (2012). The mismeasurement of privacy: Using contextual integrity to reconsider privacy in HCI. *Conference on Human Factors in Computing Systems - Proceedings*, 367–376. https://doi.org/10.1145/2207676.2207727

Becker, M. (2019). Privacy in the digital age: Comparing and contrasting individual versus social approaches towards privacy. *Ethics and Information Technology, 21*, 307–317. https://doi.org/10.1007/s10676-019-09508-z

Ben-Shahar, O., & Schneider, C. E. (2011). *The FAILURE of mandated disclosure*. https://www.jstor.org/stable/41149884.

Bernes, A. (2022). *Enhancing transparency of data processing and data subject's rights through technical tools: The PIMS and PDS solution*. https://doi.org/10.1007/978-981-16-3049-1_17

Calo, M. R. (2011). The boundaries of privacy harm. *Indiana Law Journal, 86*, 1131–1162. https://www.repository.law.indiana.edu/ilj/vol86/iss3/8.

Cohen, J. E. (2013). *What privacy is for, 126* pp. 1904–1933).

Colnago, J., Cranor, L., & Acquisti, A. (2023). Is there a reverse privacy paradox? An exploratory analysis of gaps between privacy perspectives and privacy-seeking behaviors. *Proceedings on Privacy Enhancing Technologies*, 455–476. https://doi.org/10.56553/popets-2023-0027, 2023.

Culnan, M. J. (1995). Consumer awareness of name removal procedures: Implications for direct marketing. *Journal of Direct Marketing, 9*, 10–19. https://doi.org/10.1002/dir.4000090204

De Keyser, A., Bart, Y., Gu, X., Liu, S. Q., Robinson, S. G., & Kannan, P. K. (2021). Opportunities and challenges of using biometrics for business: Developing a research agenda. *Journal of Business Research, 136*, 52–62. https://doi.org/10.1016/j.jbusres.2021.07.028

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for E-commerce transactions. *Information Systems Research, 17*, 61–80. https://doi.org/10.1287/isre.1060.0080

Dunfee, T. W., Smith, N. C., & Ross, W. T. (1999). Social contracts and marketing ethics. *J Mark, 63*, 14–32. https://doi.org/10.1177/002224299906300302

Ebert, N., Ackermann, K. A., & Heinrich, P. (2020). *Does context in privacy communication really matter? A- A survey on consumer concerns and preferences. Conference on human factors in computing systems - proceedings*. https://doi.org/10.1145/3313831.3376575

Ebert, N., Ackermann, K. A., & Scheppler, B. (2021). *Bolder is beter: Raising user awareness through salient and concise privacy notices. Conference on Human Factors in Computing Systems - proceedings*. https://doi.org/10.1145/3411764.3445516

European Commission. (2020). Commission report : EU data protection rules empower citizens and are fit for the digital age. https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1163.

European Parliament and of the Council: Regulation (EU) 2016/679. (2016). *Official Journal of the European Union, L119*, 1–88.

Floridi, L. (2017). Group privacy: A defence and an interpretation. In L. Taylor, L. Floridi, & B. van der Sloot (Eds.), *Group privacy* (pp. 83–100). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-46608-8_5.

Gauttier, S. (2019). *Modifying consent procedures to collect better data: The case of stress-monitoring wearables in the workplace. Presented at the*. https://doi.org/10.1007/978-3-030-20485-3_27

Gilbert, S., Vitak, J., & Shilton, K. (2021). Measuring Americans' comfort with research uses of their social media data. *Social Media and Society, 7*. https://doi.org/10.1177/20563051211033824

Grodzinsky, F. S., & Tavani, H. T. (2011). Privacy in the cloud: Applying Nissenbaum's theory of contextual integrity. *ACM SIGCAS - Computers and Society, 41*, 38–47. https://doi.org/10.1145/2095266.2095270

Harborth, D., & Pape, S. (2021). Investigating privacy concerns related to mobile augmented reality Apps – a vignette based online experiment. *Comput Human Behav, 122*, 17. https://doi.org/10.1016/j.chb.2021.106833

Hoel, T., Chen, W., & Pawlowski, J. M. (2020). Making context the central concept in privacy engineering. *Research and Practice in Technology Enhanced Learning, 15*. https://doi.org/10.1186/s41039-020-00141-9

Hoyle, R., Stark, L., Ismail, Q., Crandall, D., Kapadia, A., & Anthony, D. (2020). Privacy norms and preferences for photos posted online. *ACM Transactions on Computer-Human Interaction, 27*. https://doi.org/10.1145/3380960

Hull, G., Lipford, H. R., & Latulipe, C. (2011). Contextual gaps: Privacy issues on facebook. *Ethics and Information Technology, 13*, 289–302. https://doi.org/10.1007/s10676-010-9224-8

IDC. Worldwide quarterly wearable device tracker. https://www.idc.com/promo/wearablevendor. (Accessed 22 July 2023).

Isaak, J., & Hanna, M. J. (2018). User data privacy: Facebook, Cambridge Analytica, and privacy protection. *IEEE Computer Society, 51*, 56–59. https://doi.org/10.1109/MC.2018.3191268

Johnson, G. A., Shriver, S. K., & Du, S. (2020). Consumer privacy choice in online advertising: Who opts out and at what cost to industry? *Marketing Science, 39*, 33–51. https://doi.org/10.1287/mksc.2019.1198

Kasper, D. V. S. (2005). The evolution (or devolution) of privacy. *Sociological Forum, 20*, 69–92. https://doi.org/10.1007/s11206-005-1898-z

Kokkoris, M. D., & Kamleitner, B. (2020). Would you sacrifice your privacy to protect public health? Prosocial responsibility in a pandemic paves the way for digital surveillance. *Frontiers in Psychology, 11*, 1–8. https://doi.org/10.3389/fpsyg.2020.578618

Korir, M., Slade, S., Holmes, W., Héliot, Y., & Rienties, B. (2023). Investigating the dimensions of students' privacy concern in the collection, use and sharing of data for learning analytics. *Computers in Human Behavior Reports, 9*, Article 100262. https://doi.org/10.1016/j.chbr.2022.100262

Kröger, J. L., Lutz, O. H.-M., & Ullrich, S. (2021). The myth of individual control: Mapping the limitations of privacy self-management. *SSRN Electronic Journal.* , Article 106705. https://doi.org/10.2139/ssrn.3881776

Kumaraguru, P., & Cranor, L. F. (2005). *Privacy indexes: A survey of Westin's studies*. https://doi.org/10.1184/R1/6625406.v1

Kurtan, A. C., & Yolum, P. (2021). *Assisting humans in privacy management: An agent-based approach.* Springer US. https://doi.org/10.1007/s10458-020-09488-1

Lambillotte, L., Bart, Y., & Poncin, I. (2022). When does information transparency reduce downside of personalization? Role of need for cognition and perceived control. *Journal of Interactive Marketing, 57*, 393–420. https://doi.org/10.1177/10949968221095557

Lazaro, C., & Le Métayer, D. (2015). Control over personal data: True remedy or fairytale? *SCRIPT-ed, 12*. https://doi.org/10.2966/scrip.120115.3

Le Métayer, D., & Monteleone, S. (2009). Automated consent through privacy agents: Legal requirements and technical architecture. *Computer Law and Security Review, 25*, 136–144. https://doi.org/10.1016/j.clsr.2009.02.010

Lehtiniemi, T. (2017). Personal data spaces: An intervention in surveillance capitalism? *Surveillance and Society, 15*, 626–639. https://doi.org/10.24908/ss.v15i5.6424

Martin, K. E. (2012). Diminished or just different? A factorial vignette study of privacy as a social contract. *Journal of Business Ethics, 111*, 519–539. https://doi.org/10.1007/s10551-012-1215-8

Martin, K. (2016). Understanding privacy online: Development of a social contract approach to privacy. *Journal of Business Ethics, 137*, 551–569. https://doi.org/10.1007/s10551-015-2565-9

Martin, K. E., & Nissenbaum, H. (2015). Measuring privacy: Using context to expose confounding variables. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2709584

Martin, K. E., & Nissenbaum, H. (2016). Privacy interests in public records: An empirical investigation. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2875720

Mcnally, K. (2021). Accept all '. How hyperbolic discounting renders privacy self-management a faulty foundation for privacy protection. *Studies in Philosophy, Politics and Economics*, 38–43.

Miroglio, B., Zeber, D., Kaye, J., & Weiss, R. (2018). The effect of ad blocking on user engagement with the web. *The Web Conference 2018 - Proceedings of the World Wide Web Conference*, 813–821. https://doi.org/10.1145/3178876.3186162. WWW 2018.

Motti, V. G., & Caine, K. (2015). Users' privacy concerns about wearables: Impact of form factor, sensors and type of data collected. *Lecture Notes in Computer Science, 8976*, 231–244. https://doi.org/10.1007/978-3-662-48051-9_17

Nissenbaum, H. (2004). Privacy as contextual integrity. *Washington Law Review, 79*, 119–157.

Nissenbaum, H. (2010). *Privacy in context: Technology, policy, and the integrity of social life. Stanford law books*. https://doi.org/10.1080/15536548.2011.10855919

Norval, C., & Henderson, T. (2017). *Contextual consent: Ethical mining of social media for health research*.

Obar, J. A. (2015). Big data and the phantom public: Walter lippmann and the fallacy of data privacy self-management. *Big Data Soc, 2*, 1–16. https://doi.org/10.1177/2053951715608876

OECD. (2019). *Enhancing access to and sharing of data*. OECD. https://doi.org/10.1787/276aaca8-en

Oghazi, P., Schultheiss, R., Chirumalla, K., Kalmer, N. P., & Rad, F. F. (2020). User self-disclosure on social network sites: A cross-cultural study on facebook's privacy concepts. *Journal of Business Research, 112*, 531–540. https://doi.org/10.1016/j.jbusres.2019.12.006

Perez, A. J., & Zeadally, S. (2018). Privacy issues and solutions for consumer wearables. *IT Prof, 20*, 46–56. https://doi.org/10.1109/MITP.2017.265105905

Sanchez, O. R., Torre, I., & Knijnenburg, B. P. (2020). Semantic-based privacy settings negotiation and management. *Future Generation Computer Systems, 111*, 879–898. https://doi.org/10.1016/j.future.2019.10.024

Schweidel, D. A., Bart, Y., Inman, J. J., Stephen, A. T., Libai, B., Andrews, M., Rosario, A. B., Chae, I., Chen, Z., Kupor, D., Longoni, C., & Thomaz, F. (2022). How consumer digital signals are reshaping the customer journey. *J Acad Mark Sci, 50*, 1257–1276. https://doi.org/10.1007/s11747-022-00839-w

Sloan, R. H., & Warner, R. (2013). Beyond notice and choice: Privacy, norms, and consent. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2239099

Solove, D. J. (2006). A taxonomy of privacy. *Univ PA Law Rev., 154*, 477. https://doi.org/10.2307/40041279

Solove, D. J. (2013). Introduction: Privacy self-management and the consent dilemma. *Harvard Law Review, 126*, 1880–1903. https://ssrn.com/abstract=2171018.

Taylor, J. E., Rousselet, G. A., Scheepers, C., & Sereno, S. C. (2023). Rating norms should be calculated from cumulative link mixed effects models. *Behavior Research Methods, 55*, 2175–2196. https://doi.org/10.3758/s13428-022-01814-7

The Economist. Wearable technology promises to revolutionise health care. https://www.economist.com/leaders/2022/05/05/wearable-technology-promises-to-revolutionise-health-care. (Accessed 9 June 2023).

Urbonavicius, S., Degutis, M., Zimaitis, I., Kaduskeviciute, V., & Skare, V. (2021). From social networking to willingness to disclose personal data when shopping online: Modelling in the context of social exchange theory. *Journal of Business Research, 136*, 76–85. https://doi.org/10.1016/j.jbusres.2021.07.031

van Ooijen, I., & Vrabec, H. U. (2019). Does the GDPR enhance consumers' control over personal data? An analysis from a behavioural perspective. *J Consum Policy (Dordr)., 42*, 91–107. https://doi.org/10.1007/s10603-018-9399-7

Weinshel, B., Wei, M., Mondal, M., Choi, E., Shan, S., Dolin, C., Mazurek, M. L., & Ur, B. (2019). Oh, the places you've been! User reactions to longitudinal transparency about third-party web tracking and inferencing. *Proceedings of the ACM Conference on Computer and Communications Security*, 149–166. https://doi.org/10.1145/3319535.3363200

Westin, A. F. (2003). Social and political dimensions of privacy. *Journal of Social Issues, 59*, 431–453. https://doi.org/10.1111/1540-4560.00072

Wiesner, M., Zowalla, R., Suleder, J., Westers, M., & Pobiruchin, M. (2018). Technology adoption, motivational aspects, and privacy concerns of wearables in the German running community: Field study. *JMIR Mhealth Uhealth, 6*, 1–16. https://doi.org/10.2196/mhealth.9623

Zhang, S., Shvartzshnaider, Y., Feng, Y., Nissenbaum, H., & Sadeh, N. (2022). *Stop the spread: A contextual integrity perspective on the appropriateness of COVID-19 vaccination certificates*. Association for Computing Machinery. https://doi.org/10.1145/3531146.3533222

Zuboff, S. (2019). *The age of surveillance capitalism.* New York.

August Bourgeus is a researcher at imec-SMIT, VUB, specialising in data governance, transparency, and citizen empowerment. He holds an MSc in Business Engineering: Data Analytics from Ghent University (2020), where his thesis examined decentralised identity and citizen data vaults using Solid technology. At imec-SMIT-VUB, he investigates how citizens perceive personal data vaults and advancing transparent data handling practices. As a member of imec-SMIT, VUB's Data, Governance and Communities Unit, Bourgeus' research explores reimagining citizen-government relationships through innovative data stewardship models.

Laurens Vandercruysse is a FEDtWIN-researcher at the Applied Economics department of VUB and the Royal Museums for Fine Art Belgium, working on digitalization and sustainability of public service organisations. Previously, he worked on socio-economic aspects in the context of the SolidLab Vlaanderen research project. His PhD dissertation concentrated on the economic impact of data protection regulation in the context of smart cities, and the economics of data protection impact assessments (DPIAs).

Nanouk Verhulst graduated as an Organizational Psychologist in 2010. Furthermore, she holds a Ph.D. in Business Economics (UGent) and a Master's degree in Management (2011). She is currently Professor ad interim at Business department the Vrije Universiteit Brussel (VUB) and senior researcher at imec-SMIT,VUB. Her current research primarily deals with the impact of innovative technologies on customers and employees in service settings. She focuses on interdisciplinary research and relies on theories and methods from a variety of disciplines (e.g., psychology, neuroscience, computer science, consumer behaviour).