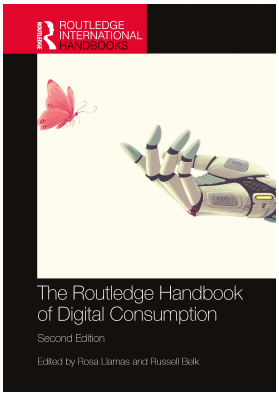

The Routledge Handbook of Digital Consumption

Rosa Llamas, Russell Belk

Online Privacy as Space

Publication details
https://test.routledgehandbooks.com/doi/10.4324/9781003317524-41
Ian Grant, Kathryn Waite
Published online on: 26 Sep 2022

34

ONLINE PRIVACY AS SPACE

Concepts, Issues, and Research Avenues for Digital Consumption

Ian Grant and Kathryn Waite

Introduction

Privacy is commonly cited in legal terms as being the individual's "right to be let alone" (Warren and Brandeis 1890). In this chapter, we discuss how managing privacy is complicated by the different ways in which information about the self is gathered and digitised when participating in virtual and offline spaces. Accordingly, we consider online privacy as space. Indeed Clarke (2016: 79) defines privacy as "the interest that individuals have in sustaining personal space, free from interference by other people and organisations". Our aim in this chapter is to argue for consideration of online space as personal, semi-public, and public spaces that enable the individual to reveal, manage, and protect multiple digital identities (Straub and Nentwich 2013, Kerrigan and Hart 2016).

We begin by identifying how technological developments have enabled a commercial interference within online personal space and the marketisation of personal data. We proceed to examine the concept of privacy concern and the growing spectrum of affective attitudes that include privacy cynicism, fatigue, apathy, and alienation. We explain how the process of information sharing has been conceptualised as an exchange according to Privacy Calculus Theory. We conclude that there are limitations in applying an exchange model as this does not fully account for paradoxical behaviours. In the final section we draw on research that applies concepts from Human Geography studies to propose a bridge between identity performance and privacy behaviour. We argue that online spaces provide a resource within which consumers manage multiple online identities through selective information disclosure. We conclude by prompting digital scholars to take a multi-layered examination of privacy practices, identity performance, and the power dynamics inherent in commercial interference within and across online (and offline) spaces.

The Marketisation of Personal Data

Technological developments in analytical and tracking software coupled with the commercial benefits associated with the use of predictive technology have resulted in the marketisation of individual information (Pomfret *et al.* 2020). The speed, volume, accessibility, and ease of collecting digital information is a phenomenon that has been labelled Big Data. Big

 DOI: 10.4324/9781003317524-41

Data refers to a large amount of data which requires specialised tools and practices for collecting, storing, processing, and analysing (Alharthi *et al.* 2017). Big Data analysis provides organisations with actionable points or micro-moments of truth about millions of consumers that facilitate marketing practices when coupled with predictive analytics (Talón-Ballestero *et al.* 2018, Braun and Eklund 2019). Data mining tools and sophisticated data collection techniques all provide grounds for privacy concern.

Once collected, Big Datasets can be sold or otherwise shared between organisations who are interested in gaining competitive advantage from possessing a 360-degree consumer view. A range of data practices (explicit and implicit sharing, harvesting, aggregation, re-identification) result in personal information being commodified and commercialised. The term "data capitalism" is applied to the systematic commoditisation of data and is closely linked to "surveillance capitalism" which Zuboff (2019: 1) defines as "profits from the unilateral surveillance and modification of human behaviour". Increasingly, online activity is tracked, recorded, and analysed for commercial reasons (Zuboff 2019), although we acknowledge that there are legitimate user-centred design reasons for organisations recording and analysing online activity using (for example, tracking cookies are used to ensure the smooth functioning of web software).

To reflect the pervasiveness of data collection, in Table 34.1 we identify that individual information can be gathered and digitised from the *embodied self* (being, behaviour, and action), the *recorded self* (records of voice, image, and other data), and the *disembodied self* (membership of groups, information exchange, and attribution of thought). Our formulation of self-hood is informed by the eight basic types of privacy in a typology of privacy proposed by Koops *et al.* (2016); however, we provide more detail on the role of digital technology. We link each selfhood dimensions to a privacy focus. The privacy foci are derived from three privacy types formulated by Clarke (2016) (personal behaviour, personal communication, personal data) and four privacy types by Finn *et al.* (2012) (privacy of the person, privacy of thoughts and feelings, privacy of location and space, privacy of association). The final column provides examples of technology or techniques (termed interference technology) that provide a route for the monitoring of personal data. In this format, we can see that selfhood exists as simultaneous and indeed maybe at times competing consumer identities: the *embodied-self*, the *recorded-self*, and the *disembodied-self*.

Table 34.1 Selfhood, Privacy, and Examples of Interference Technology

Selfhood dimensions	*Privacy focus*	*Privacy focus definition*	*Interference technology examples*
Embodied self	Privacy of being	Ability to keep bodily functions and characteristics private	Biometric trackers recording genetic codes and DNA
	Privacy of behaviour and action	Ability to be without surveillance in public, semi-public, and private space	Systematic observation and recording of activity
	Privacy of location and space	Ability to be present in public or semi-public space without being identified or tracked	Identification, tracking, and monitoring i.e., using Cookies and RFID
Recorded self	Privacy of personal data, voice, and image	Ability to control personal records such as voice and image	Sharing of data and image with others, ability to tag and share and be tracked as a result.

(*Continued*)

Selfhood dimensions	*Privacy focus*	*Privacy focus definition*	*Interference technology examples*
Disembodied self	privacy of association (group privacy)	Ability to associate with whoever you wish without being tracked.	Monitoring by and of association with a group or organisation using network analysis.
	Privacy of personal communication	Ability to exchange information without interception of content	Monitoring and recording of communication, analysis for key words, and use in behavioural advertising
	Privacy of thoughts, opinions, and feelings	Ability to express thoughts, opinions or feelings without judgement, or manipulation	Capturing and systematically analysing opinions, expression, and statements to make algorithmic adjustments to news feed items (filter bubbles).

Source: Adapted from Clarke (2016), Finn *et al.* (2012).

We use the term "interference technology" to acknowledge the increased commercial interference in online activity that is driven by Big Data. Our choice of "interference" is informed by the definition of Privacy interference referred to in the United Nations (1948) Declaration of Human Rights (UDHR) Article 12 which states that:

> no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

We argue that the ontology of surveillance capitalism, amplified by the rhetoric about the organisational benefits of Big Data, promotes the idea that commercial interference with personal privacy is not only desirable but essential to remaining competitive (Buhalis *et al.* 2020).

Examples of marketing techniques that "interfere" with online activity include the personalising and customising online advertisements, the automated sending of personalised email messages, the selection and ordering of online content, the setting prices for goods and services based on online patterns of behaviour, and the use of artificial intelligence (recommender agents) to promote products and services for consumption. We consider such practices arbitrary interference in consumption for three reasons. First, there is forced exposure to commercial content which results in customised advertising being viewed as an attack that elicits consumer feelings of fear and distrust (Samuel *et al.* 2021). Second, the predictive models are biased which discriminate against certain groups (Giest and Samuels 2020). For example, Ali *et al.* (2019) demonstrate how advertisement delivery is skewed in Facebook. Third, that due to stereotyping bias individuals are presented with commercial messages that conform to gender and life stage norms that are personally offensive, interacting with this content will register as a positive response and thus the content will continue to be presented (Ali *et al.* 2019).

Overall, the marketisation of individual data means that records of individual online activity are not owned or controlled by the user. Waite and Perez-Vega (forthcoming) explain how Big Data generated during online consumption can be transactional or non-transactional. Transactional data is generated actively by consumers when a product or service is sold. Non-transactional data is generated passively by consumers through non-sales activity from general customer online behaviour or sensor readings from interactions with smart devices. Whereas consumers are aware of active collection they may be unaware of the data collected passively. Survey research reports that 91% of consumers agree that they have lost control of their personal information and 70% of consumers are more concerned about their privacy than previously (Rainie, 2016, IDC 2017 cited by Hong *et al.* 2021). We now explain privacy concern and its related responses.

Privacy Concern

Yun *et al.* (2019: 570) define privacy concern as "the concern that individuals have with the information privacy practices of organizations, which could comprise the individuals' ability to control personal information". Although research in this area is mature, the debate about the causes, behaviours, and consequences of online privacy concern continues (see Ginosar and Ariel 2017). Consumer concern over information marketisation has expanded to include related responses of privacy cynicism, fatigue, fatalism, and alienation (Hoffman *et al.* 2016, Choi *et al.* 2018). We now consider how each of these emotions shapes and hinders consumer privacy choice.

Privacy cynicism was originally conceptualised as a coping mechanism in the context of growing levels of commercial privacy threats (see Hoffman *et al.* 2016, Lutz *et al.* 2020). Rather than actively protecting their personal information, consumers increasingly ignore or dismiss privacy concerns, driven by feelings of powerlessness and resignation. Privacy cynicism reflects rising levels of mistrust and/or antagonism towards the online actions of commercial organisations, despite the corporate "rhetoric" (Hoffman *et al.* 2016).

Privacy fatigue is the psychological strain and eventually exhaustion generated over time when considering threats to online privacy (Choi *et al.* 2018). The longitudinal component of privacy fatigue is linked to individual feelings of loss of control. For individuals experiencing privacy fatigue, sustaining personal privacy becomes burdensome due to the growing ease with which personal information can be collected, stored, and shared result. Privacy fatigue can manifest itself in indecision about updating privacy preferences or simply (mis) understanding the processes to maintain an optimum level of privacy. Psychologists argue that consumer privacy concern is better understood through the construct of *rational fatalism*. Fatalism in this context ranges from a passive denying of personal control to outright resignation (see Xie *et al.* 2019). Privacy fatigue and fatalisms are characterised by feelings of resignation, inevitability, helplessness, and pessimism.

Consumer alienation is linked to the commercial storage, manipulation, and release of personal information through social network sites (Ortiz *et al.* 2018). Alienated consumers experience a sense of individual powerlessness and societal normlessness in relation to online privacy (Schwaig *et al.* 2013). This tallies a lack of identification with the corporate institutions, their marketing practices, and consequential privacy-related policies. Boyd and Hargittai (2010) point out that individuals are far more likely to react to the threats posed by other social users than institutional threats, where their reactions are more indifferent and apathetic.

Consumer Response to Privacy Concern

Historically, researchers have identified three key areas of behavioural responses adopted to counter privacy concern. First, informational non-disclosure (Nam *et al.* 2006), as an avoidance tactic in response to heightened risks. Second, information falsification (Dinev and Hart 2006) is used to counter security risks when actively inputting information, whereas non-disclosure relates to measures that are taken to prevent passive collection taking place. Falsification is a more pervasive tactic used by consumers to deliberately conceal and disguise their identity with past studies suggesting between 30% and 40% of consumers admitting to this, using fake or multiple passwords for example. For example, Ortiz *et al.* (2018) detail how privacy alienation manifests itself in both consumer "lurking" and "concealment" behaviours within social networks. Consumers with higher levels of alienation were found less likely to disclose information and more likely to simply lurk in the background. This was due to a lack of institutional trust and an inability to influence the practices of organisational privacy policies, leading to concealment of personal information. Third, the non-adoption of the technology (Dinev and Hart 2006).

Profiling by Privacy Concern and Online Behaviour

Customer segmentation has been used to deepen understanding of how privacy concern and online behaviour varied within the wider population, according to individual characteristics such as gender, life stage, values, and personality traits (see Schomakers *et al.* 2019). Gender differences have been recorded, primarily within the context of social network research. Several studies have reported higher levels of privacy concern amongst females (e.g., Litt and Hargittai 2014, Shepherd 2016, Thelwall and Vis 2017, Tifferet 2019). Examples of heightened protective behaviour include increased untagging of photographs and activation of privacy settings. Researchers have explained female privacy concern as a reflection of personality traits such as neuroticism (Lehmann *et al.* 2012) and anxiety (Kajonius and Johnson 2018) and there is limited exploration of alternative explanations. The link between privacy concern and gender is strongly contested (see Tifferet 2019: 2). Hoffman and Lutz (2021) argue that focusing on socio-demographic variables in isolation is over simplistic since the influence is culturally and structurally mediated.

Personality traits research sought psychological determinants of differences in privacy concern and behaviours. Early work by Smith *et al.* (1996) proposes that different personality traits are linked to differences in user privacy behaviour. For example, the trait of "*agreeableness*" was closely correlated with a "*willingness to believe others*", "*comply with orders*", and "*pay attention to deviant behaviour*", and correspondingly individuals with this trait displayed cared more about privacy issues (see Korzaan and Boswell 2008; Osatuyi 2015). Similarly, Tang *et al.* (2020) argue that an "easy-going" personality trait reduces privacy fatigue and heightens privacy concerns during use of mobile apps. They conclude that individuals possessing strong traits of "*neuroticism, agreeableness*", and "*conscientiousness*" pay greater attention to the privacy risks they face. Such approaches provide limited insight however into what Nissenbaum (2011) argues is the context-dependent nature of privacy concern and the norms and consequences that surround these, providing only a narrow understanding based on individual motivations and traits.

Life stage has been used to understand that privacy attitudes and behaviours vary by generational cohort and online experience (see Walgrave *et al.* 2018). There is a stream of research that focuses on teenagers, as adolescence is recognised as a transitional period

where a broadening of social relationships becomes more important. The pursuit of social relationships results in higher utilisation of social networks, more time spent updating social profiles and expanding social circles (Stutzman *et al.* 2013). Young adults (particularly those aged 10–17) actively disclose personal information, images, opinions, and hobbies online, which leads to the sharing of such details with third parties (Turow and Nir 2000). Combining life stage with gender shows that younger females have an enhanced desire for socialisation through social networks. The concept of disclosure leading to a reward (in this case a wide social circle and related social reward through influence and exchange) provides an alternative explanation for the causality of personality traits (Kokolakis 2017). To reflect this exchange-driven view of disclosure, the Privacy Calculus model was proposed as an explanation for evidence that showed that, despite privacy concerns, private information is disclosed in a knowing exchange for benefits (Laufer and Wolfe 1977, Wang *et al.* 2016).

The Privacy Calculus Model

The Privacy Calculus model assumes that consumers act rationally and have full agency. The model seeks to explain the process and conditions of exchanging the right to privacy for a range of other benefits. Experiments provide evidence of Privacy Calculus taking place by demonstrating the willingness to disclose personal information such as photos, and personal information (age, address, and economic status) for small financial gains (see Acquisti and Grossklags 2005, Norberg *et al.* 2007, Beresford *et al.* 2012). Survey evidence shows that participants report a willingness to trade location information to gain benefits from mobile phone applications (Zafeiropoulou *et al.* 2013). However, questions remain about the extent to which an exchange model reflects consumer behaviour and there are warnings about the dangers of oversimplification when researching privacy concern (Yun *et al.* 2019).

There is persistent evidence of a "dichotomy between privacy attitude and privacy behaviour" (Kokolakis 2017: 123). Consumers report concerns about the volume of personal information being collected whilst, at the same time, expressing willingness to continue to buy online or receive small loyalty card-based cost savings (Sayre and Horne 2000). One suggestion is that consumers are not always rational and calculating in their approach to online privacy. In attempt to account for the gap between attitude and behaviour, the term *privacy paradox* was coined (Norberg *et al.* 2007). Persisting in the view that consumers would choose to act rationally, early studies of the *privacy paradox* characterised consumers as either uninformed about how their personal information was collected or more actively involved when their perceptions of the rewards (of disclosure) outweighed the risks (see Westin 2000, Draper 2017). Acquisti (2004) concludes that consumers can act as rational agents except when they are influenced by three factors: *incomplete information, bounded rationality*, and *psychological biases*.

However, the privacy paradox proposition has been subject to several challenges for not providing a sufficient explanation for online privacy behaviour. A major criticism is the complexity of theoretical explanations for the paradox, each with their own set of assumptions and methodologies. For example, a literature review by Gerber *et al.* (2018) expands the initial explanations of *privacy calculus*, *bounded rationality and decision bias*, *lack of personal experience and protection knowledge* to include *social influence*, *risk and trust*, *illusion and control*, and *quantum theory*.

From the preceding discussion we conclude that research using the Privacy Calculus model is limited by the focus on economic rationality and neglects psychological orientations such as individual and identity-related motivations (Kokolakis 2017, Bandara *et al.* 2020). In

addition, privacy concern responses are considered in terms of action, inaction, or paradoxical behaviours. Existing approaches tend to characterise the consumers as being knowing and active in managing their privacy. However, development of Big Data techniques gathers data passively as well as actively and can track and aggregate information within and across online and offline boundaries and erodes the degree of individual control of data. Lutz *et al.* (2020: 1169) argue that the new era of "data capitalism" results in a (new) form of social reality in which users continue to share their personal information irrespective of the known risks, fearful of being excluded from the dominant means of socialisation.

Moreover, there is a tendency to assume that individuals are trading information of a single identity or unified notion of self. Privacy is linked to an individual, monolithic identity rather than to multiple dimensions of the self within consumption spaces. However, research points to multiple digital identities each knowingly crafted for a particular audience (Kerrigan and Hart, 2016). We conclude that the focus on an economic/rational exchange model has resulted in a neglect of alternative approaches.

Online Privacy as Space

We propose that research would benefit by considering privacy as space and moving away from the confines of the exchange-based model of privacy, as exemplified by Privacy Calculus Theory. We are inspired by the theorisation of consumer spatial practices by Maciel and Wallendorf (2021), who propose that space is "resource that people deliberately employ and transform to represent their identities, negotiate social relations, and express cultural desires". In their paper, Maciel and Wallendorf (2021) categorise spaces as private, public, and semi-public and draw on the work of McDowell (1999) to argue that consumption spaces are subject to variations in hierarchy according to specific locations, properties, and social relations. They demonstrate how activities in each space interconnect and shape identity work at individual, community, and public levels. Specifically, Maciel and Wallendorf (2021: 2) examine how the craft of knitting is enacted within private, semi-public, and public space through individual and communal actions to develop and politicise how individuals identify as being a knitter.

In Table 34.2 we apply the concepts of Maciel and Wallendorf (2021) to online platforms and provide examples of different spaces for online privacy (as per Koops *et al.* 2016 we use personal rather than private to avoid confusion). Classifying online spaces as personal, semi-public, and public spaces connects online privacy enquiry with the established stream of research that demonstrates that individuals reveal, manage, and protect multiple digital identities (Zwick and Deeegri Knott 2009, Straub and Nentwich 2013, Kerrigan and Hart 2016). As such we concur with Koops and Galič (2021: 5) who define privacy as:

> having spaces in which you can be yourselves. In other words, having spaces in which you can be yourselves gives you privacy, and privacy requires having some spaces in which you can be yourselves.

A spatial approach enables digital consumption researchers to link identity work with privacy concern and behaviour. There are hints that this link exists within privacy-paradox research, but the implications are underdeveloped. For example, it is assumed that individuals "trade" their personal information in order to "pay" for the benefits of building a social network (Lutz *et al.* 2020). However, these formulations fail to account for the complex interactions and fluidity associated with identity performance and strategic identity disclosure

Table 34.2 Spaces for Online Privacy

Space	*Personal*	*Semi-public*	*Public*
Definition	Bounded space that is shared with intimate others i.e., family, close friends	Semi-bounded space shared with peers that have a common interest or bond.	Unbounded spaces that are shared with strangers
Offline example	The home	Sports clubs, hobby shops, or the workplace	Highways, public parks, general stores
Online example	An individual's digital account	Community accounts, brand community account, online gaming platforms	Networking platforms i.e., Twitter, TikTok

Source: Adapted from Maciel and Wallendorf (2021).

across and within online spaces as evidenced by Maciel and Wallendorf (2021). Furthermore, a spatial approach enables research to draw on Human Geography domain to evaluate the role of commercial actors within digital spaces. Indeed, geographers would argue that the "common (legal) division of the social world into public and private is not a natural division; rather, it is an expression of power" (Koops and Galič 2017: 19). Therefore, an important extension to privacy research would be an examination of how commercial entities such as brands and platform owners perform or hide power within the digital places and the impact on privacy/identity management.

Privacy research has encouraged us to view technological systems, devices, and behaviours as being "embedded in larger material and social networks and webs of meaning" (Nissenbaum 2010: 6). Researchers in the past have been critical of a dearth of research into the types of information collected, variations in different markets (e.g., healthcare, marketing, finance), the political context, and the intersectionality of social-economic and cultural backgrounds of those disclosing information (Smith *et al.* 1996). The work of Maciel and Wallendorf (2021) demonstrates how space can be both an environment for enthusiastic engagement with surrounding market practices or a site for avoidance and escapism from forces that seek to destabilise, exert oppressive influence, or interference. There is scope for privacy research to build on this foundation by examining specific contexts where privacy behaviours, power dynamics, and norms may be distinct or fluid.

Conclusion

In this chapter we have provided an overview of privacy concern and have argued that the complexities of online privacy concerns are not fully captured by existing explanations. For instance, the existence of paradox in technology use persists after it was first highlighted by Mick and Fournier (1998). A spatial approach provides consumer agency and provides insight into the paradox of evincing privacy concern whilst sharing personal information. We suggest that, rather than assuming a transactional trade-off between individual reward and risk, it would be more productive to consider privacy being performed across online spaces with blurred boundaries between personal, semi-public, and public spaces with liminal practices by which consumers enact multiple selves. If we consider privacy as spatial practice, then we can explore how space can be used as a resource for privacy protection or identity sharing. If we frame *space* as an "environment" where consumer use to act, and interact, with the world around them, this allows us to consider how environmental affordances are used in privacy

practice. The idea of privacy practices as spanning both online and offline spaces enables us to consider how the forms of selfhood and privacy foci contained in Table 34.1 interact and shape privacy responses. Discourse on Big Data identifies that online consumption takes place in contested space, that is negotiated, and sometimes compromised, by a range of competing parties, each with vested interests and power bases. Our starting point as considering Clarke's (2016) as privacy as sustaining personal space free from interference has enabled us to view privacy concern afresh.

Further reading

Finn, R.L., Wright, D. and Friedewald, M. (2012) "Seven types of privacy" in S. Gutwirth *et al.* (eds.), *European Data Protection: Coming of Age*, Springer, Dordrecht, pp. 3–32.

Kerrigan, F. and Hart, A. (2016) "Theorising digital personhood: A dramaturgical approach," *Journal of Marketing Management*, 32, 17–18.

Kokolakis, S. (2017) "Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon," *Computer Security*, 64, 122–134.

Koops, B.J. and Galič, M. (2021) "Unity in privacy diversity: A Kaleidoscopic view of privacy definitions. *South Carolina Law Review*, 73(2).

Lutz, C., Hoffmann, C. P. and Ranzini, G. (2020) "Data capitalism and the user: An exploration of privacy cynicism in Germany," *New Media & Society,* 22(7), 1168–1187.

Maciel, A.F. and Wallendorf, M. (2021) "Space as a resource in the politics of consumer identity," *Journal of Consumer Research*, January 23, Advance Access.

References

Acquisti, A. (2004) "Privacy in electronic commerce and the economics of immediate gratification," *Proceedings of the 5th ACM Conference on Electronic Commerce*, May 21–29.

Acquisti, A. and Grossklags, J. (2005) "Privacy and rationality in individual decision making," *IEEE Security & Privacy,* 3(1), 26–33.

Alharthi, A., Krotov, V. and Bowman, M. (2017) "Addressing barriers to big data," *Business Horizons*, 60(3), 285–292.

Ali, M., Sapiezynski, P., Bogen, M., Korolova, A., Mislove, A. and Rieke, A. (2019), "Discrimination through Optimization", *Proceedings of the ACM on Human-Computer Interaction*, 3(No. CSCW), 1–30.

Bandara, R., Fernando, M. and Akter, S. (2020) "Explicating the privacy paradox: A qualitative inquiry of online shopping consumers," *Journal of Retailing and Consumer Services,* 52, 1–8.

Beresford, A. R., Kubler, D. and Preibusch, S. (2012) "Unwillingness to pay for privacy: A field experiment," *Economic Letters,* 117(1), 25–27.

Boyd, D. and Hargittai, E. (2010) "Facebook privacy settings: Who Cares? *First Monday*, 15(8). https://doi.org/10.5210/fm.v15i8.3086.

Braun, J. A. and Eklund, J. L. (2019) "Fake news, real money: Ad tech platforms, profit-driven hoaxes, and the business of journalism," *Digital Journalism*, 7(1), 1–21.

Buhalis, D., Andreu, L. and Gnoth, J. (2020) "The dark side of the sharing economy: Balancing value co-creation and value co-destruction," *Psychology & Marketing*, 37(5), 689–704.

Choi, H., Park, J. and Jung, Y. (2018) "The role of privacy fatigue in online privacy behaviour," *Computers in Human Behavior*, 81, 42–51.

Clarke, R. (2016), "A framework for analysing technology's negative and positive impacts on freedom and privacy," *Datenschutz Und Datensicherheit - DuD*, 40(2), 79–83.

Dinev, T and Hart, P. (2006) "Internet privacy concerns and social awareness as determinants of intention to transact," *International Journal of Electronic Commerce*, 10(2), 7–29.

Draper, N. A. (2017) "From privacy pragmatist to privacy resigned: Challenging narratives of rational choice in digital privacy debates," *Policy & Internet*, 9(2), 232–251.

Finn, R. L., Wright, D. and Friedewald, M. (2012) "Seven Types of Privacy." In *European Data Protection: Coming of Age*, S. Gutwirth *et al.* (eds.), 3–32. Springer, Dordrecht.

Gerber, N., Gerber, P. and Volmaker, M. (2018) "Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior," *Computer Security*, 77, 226–227.

Giest, S. and Samuels, A. (2020) "'For good measure': Data gaps in a big data world," *Policy Sciences*, 53(3), 559–569.
Ginosar, A. and Ariel, Y. (2017) "An analytical framework for online privacy research: What is missing?" *Information and Management*, 54(7), 948–957.
Hoffmann, C.P. and Lutz, C. (2021) "Digital divides in political participation: The mediating role of social media self-efficacy and privacy concerns," *Policy & Internet*, 13(1), 6–29.
Hoffmann, C. P., Lutz, C. and Ranzini, G. (2016) "Privacy cynicism: A new approach to the privacy paradox," *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, 10(4), 7.
Hong, W., Chan, F. K. and Thong, J. Y. (2021) "Drivers and inhibitors of internet privacy concern: A multidimensional development theory perspective," *Journal of Business Ethics*, 168, 539–564.
Kajonius, P. J. and Johnson, J. (2018) "Sex differences in 30 facets of the five-factor model of personality in the large public," *Personality and Individual Differences*, 129, 126–130.
Kerrigan, F. and Hart, A. (2016) "Theorising digital personhood: A dramaturgical approach," *Journal of Marketing Management*, 32, 17–18.
Kokolakis, S. (2017) "Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon," *Computer Security*, 64, 122–134.
Koops, B. J. and Galič, M. (2017) "Conceptualizing space and place: Lessons from geography for the debate on privacy in public." in: *Privacy in Public Space*. Edward Elgar Publishing, Cheltenham.
Koops, B. J. and Galič, M. (2021) "Unity in privacy diversity: A kaleidoscopic view of privacy definitions," *South Carolina Law Review*, 73(2), 1–36.
Koops, B. J., Newell, B. C., Timan, T., Skorvanek, I., Chokrevski, T. and Galič, M., (2016) "A typology of privacy," *University of Pennsylvania Journal of International Law*, 38(2), 483–575.
Korzaan, M. L., and Boswell, K. T. (2008) "The influence of personality traits and information privacy concerns on behavioural intentions," *Journal of Computer Information Systems,* 48(4), 15–24.
Laufer, R.S. and Wolfe, M. (1977) "Privacy as a concept and a social issue: A multidimensional developmental theory", *Journal of Social Issues*, 33(3), 22–42.
Lehmann, R., Denissen, J. J., Allemand, M. and Penke, L. (2012) "Age and gender differences in motivational manifestations of the Big Five from age 16 to 60," *Developmental Psychology*, 49(2), 365–383.
Litt, E. and Hargittai, E. (2014) Smile, snap and share? A nuanced approach to privacy and online photo-sharing, *Poetics*, 42(1), 1–21.
Lutz, C., Hoffmann, C. P. and Ranzini, G. (2020) "Data capitalism and the user: An exploration of privacy cynicism in Germany," *New Media & Society*, 22(7), 1168–1187.
Maciel, A.F. and Wallendorf, M. (2021) "Space as a resource in the politics of consumer identity," *Journal of Consumer Research*, forthcoming.
McDowell, L. (1999). *Gender, Identity and Place: Understanding Feminist Geographies*. Polity Press, Minneapolis, MN.
Mick, D. G and Fournier, S. (1998) "Paradoxes of technology: Consumer cognizance, emotions, and coping strategies," *Journal of Consumer Research,* 25(2), 123–143.
Nam, C., Song, C., Park, E. L. and Ik. C. (2006) "Consumers' privacy concerns and willingness to provide marketing-related personal information online," *Advances in Consumer Research*, 33, 212–217.
Nissenbaum, H. (2010). *Privacy in Context: Technology, Policy and the Integrity of Social Life*. Stanford University Press, Stanford, CA.
Nissenbaum, H. (2011), "A contextual approach to privacy online," *Daedalus*, 140(4), 32–48.
Norberg, P. A., Horne, D. R. and Horne, D. A. (2007) "The privacy paradox: Personal information disclosure intentions versus behaviors," *Journal of Consumer Affairs*, 41(1), 100–126.
Ortiz, J., Chih, W-H. and Tsai, F.-S. (2018) "Information privacy, consumer alienation, and lurking behavior in social network sites," *Computers in Human Behavior*, 80, 143–157.
Osatuyi, B. (2015) "Personality traits and information privacy concern on social media platforms," *Journal of Computer Information Systems, 55*(4), 11–19.
Pomfret, L., Previte, J. and Coote, L. (2020) "Beyond concern: Socio-demographic and attitudinal influences on privacy and disclosure choices," *Journal of Marketing Management*, 36(5/6), 519–549.
Samuel, A., White, G.R., Thomas, R. and Jones, P., (2021) "Programmatic advertising: An exegesis of consumer concerns," *Computers in Human Behavior*, 116, 106657.
Sayre, S. and Horne, D. (2000) "Trading secrets for savings: How concerned are consumers about club cards as a privacy threat," *Advances in Consumer Research*, 27(1), 151–155.
Schomakers, E. M., Lidynia, C. and Ziefle, M. (2019) "A typology of online privacy personalities," *Journal of Grid Computing*, 17(4), 727–747.

Schwaig, K. S., Segars, A. H., Grover, V. and Fiedler, K. D. (2013) "A model of consumers' perceptions of the invasion of information privacy," *Information & Management*, 50(1), 1–12.

Shepherd, R. P. (2016) "Men, women, and Web 2.0 writing: Gender differences in Facebook composing," *Computers and Composition*, 39, 14–26.

Smith, H. J., Milberg, S. J. and Burke, S. J. (1996) "Information privacy research: Measuring individuals' concerns about organizational practices," *MIS Quarterly*, 20(2), 167–196.

Straub, S. and Nentwich, M. (2013) "Social network sites, privacy and the blurring of boundaries between public and private spaces," *Science and Public Policy*, 40(6), 724–732.

Stutzman, F., Gross, R. and Acquisti, A. (2013) "Silent listeners: The evolution of privacy and disclosure on Facebook," *Journal of Privacy and Confidentiality*, 4(2), 2.

Talón-Ballestero, P., González-Serrano, L., Soguero-Ruiz, C., Muñoz-Romero, S. and Rojo-Álvarez, J. L. (2018) "Using big data from customer relationship management information systems to determine the client profile in the hotel sector," *Tourism Management*, 68(5), 187–197.

Tang, J., Akram, U. and Shi, W. (2020) "Why people need privacy? The role of privacy fatigue in app users' intention to disclose privacy: Based on personality traits," *Journal of Enterprise Information Management,* 34(4), 1097–1120.

Thelwall, M. and Vis, F. (2017) "Gender and image sharing on Facebook, Twitter, Instagram, Snapchat and WhatsApp in the UK," *Aslib Journal of Information Management*, 69(6), 702–720.

Tifferet, S. (2019) Gender differences in privacy tendencies on social network sites: A meta-analysis," *Computers in Human Behavior*, 93, 1–12.

Turow, J. and Nir, L. (2000). *The Internet and the Family 2000: The View from Parents, the View from Kids*. The Annenberg Public Policy Center, Philadelphia, PA.

United Nations (1948) "The Universal Declaration of Human Rights (UDHR)," 10 Dec.: United Nations, Paris. Available at https://www.un.org/en/about-us/universal-declaration-of-human-rights. Accessed 10th August, 2021.

Waite, K and Perez-Vega, R. (forthcoming) "Big data and digital marketing" in *The Sharing Economy: Perspectives, Opportunities and Challenges*, Taheri, B., Rahimi, R. and Buhalis, D. (eds.). Goodfellow Publishing, Oxford.

Walgrave, M., Poels. K., Antheunis, M. L., Van den Broek, E. and van Noort, G. (2018) "Like or dislike? Adolescents' responses to personalized social network site advertising," *Journal of Marketing Communications*, 24(6), 599–616.

Wang, T., Duong, T. D. and Chen, C. C. (2016), "Intention to disclose personal information via mobile applications: A privacy calculus perspective", *International Journal of Information Management*, 36(4), 531–542.

Warren, S. D. and Brandeis, L. (1890) "The right to be left alone," *Harvard Law Review*, 4(5), 193–220.

Westin, A. F. (2000) "Intrusions," *Public Perspective*, 11(6), 8–11.

Xie, W., Fowler-Dawson, A. and Tvauri, A. (2019) "Revealing the relationship between rational fatalism and the online privacy paradox," *Behaviour & Information Technology*, 38(7), 742–759.

Yun, H., Lee, G. and Kim. D. J. (2019) "A chronological review of empirical research on personal information privacy concerns: An analysis of contexts and research constructs," *Information & Management*, 56, 570–601.

Zafeiropoulou, A. M., Millard, D. E., Webber, C. and O'Hara, K. (2013) "Unpicking the privacy paradox: Can structuralisation theory help to explain location-based privacy decisions?" *Proceedings of the 5th Annual ACM Web Science Conference*, May, 463–472.

Zuboff, S. (2019). "*The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*". Profile Books, London.

Zwick, D. and Deegri Knott, J. (2009) "Manufacturing customers: The database as new means of production," *Journal of Consumer Culture*, 9(2), 221–247.