Title

Mastering boundaries: differences in online privacy boundary phenomena across digital devices and years

Journal

Behaviour and Information Technology, ahead-of-print(ahead-of-print)

ISSN

0144-929X

Authors

Wang, Laurent H

Rice, Ronald E

Liu, Xingyu

et al.

Publication Date

2025

DOI

10.1080/0144929x.2024.2448706

Wang, L. H., Rice, R. E., Liu, X., Hagen, I. & Zamanzadeh, N. (2025). **Mastering boundaries: Differences in online privacy boundary issues across digital devices and years**. *Behaviour and Information Technology*. Open access: https://www.tandfonline.com/doi/full/10.1080/0144929X.2024.2448706

Data availability: The data that support the findings of this study are available from the corresponding author, RER, upon reasonable request.

Human subjects: This research was authorized by the UC Santa Barbara Institutional Review Board, Office of Research, protocol 3-05-092, dates 2/23/2006 and 8/27/2016, "Using mobile phones and computers."

Support: The authors gratefully acknowledge the support of the Arthur N. Rupe endowed professorship (Dr. Rice) and the very thoughtful comments by Dr. Miriam Metzger on an earlier version.

Mastering Boundaries: Differences in Online Privacy Boundary Phenomena Across Digital Devices and Years

Abstract

Multiple digital communication devices provide varying capabilities and processes for self-disclosure, surveillance, and privacy management, therefore eliciting a variety of user privacy perceptions and behaviors. Drawing from the media mastery framework and the comparative privacy research framework, this study investigates similarities and differences in online privacy outcomes associated with computer and mobile phone use via content analysis of 12 focus groups conducted with US college students in 2006 and 2016. Findings reveal similarities and differences across device type and time and their combinations among selected privacy-related codes from the media mastery framework. Cluster analysis of the codes reveals several general themes such as *crossing the boundary from private to public*, and *safety and trust*. Contributions include the use of a reliable conceptual foundation for categorizing online privacy boundary phenomena, the generation of discussions about these phenomena from a goal-free evaluation approach, and comparisons across devices and time. The discussion provides theoretical and practical implications.

Keywords: Online privacy, comparative privacy, computers, mobile phones, media mastery, content analysis

Mastering Boundaries: Differences in Online Privacy Boundary Phenomena Across Digital Devices and Years

Digital technologies offer both advantages and disadvantages (Helles, 2013; Jensen, 2010; Rice et al., 2018); therefore, users need to navigate between the benefits and risks associated with these devices. One consequential challenge is balancing users' need for communication and self-disclosure with online privacy management. While users may attempt to manage available privacy control mechanisms, digital devices (and associated apps and platforms) may challenge users' privacy by continuously offering social and material benefits to motivate general use, such as communication, searching, and information sharing (e.g., Dienlin & Metzger, 2016).

Extensive theorizing and research have documented how people hold varying privacy concerns and enact protection behaviors within a given device (e.g., mobile phone, smart devices, algorithms) (Kang & Jung, 2021; Kim & Sung, 2022) and/or a platform (e.g., social media) (Chen, 2018; Dienlin & Metzger, 2016). But privacy perceptions and behavior may differ across multiple devices (mobile phones vs. computers) (e.g., Chin et al., 2012) and over time (e.g., Lee & Yuan, 2020; Pekárek & Pötzsch, 2009) based on factors such as device structural settings (e.g., available robust privacy protection mechanisms, processing speed, and information storage capacity) and users' psychological mechanisms (e.g., privacy mobility heuristics, psychological ownership) (discussed below). On the one hand, the portable nature of mobile phones makes them more susceptible to physical loss and may elicit greater concerns over the security of information stored on the devices (e.g., Silver et al., 2019; Sundar et al., 2020). In addition, mobile phones are often considered a "personal technology" (Vincent, 2013); therefore people may disclose more sensitive information over mobile phones than computers, which heightens privacy risks (Murthy et al., 2015). On the other hand, research demonstrates that people are more likely to notice and click on phishing emails on desktop computers than mobile phones, suggesting less careful privacy protection over computers (Liao et al., 2023). Motivating this study's focus is therefore mixed anecdotal and empirical evidence on users' privacy and security experiences across device types.

Given that different types of personal information may be collected, processed, and shared on mobile phone and computer devices, theoretically and practically important questions remain unanswered as to how do users perceive and manage various privacy issues associated with digital devices, and what are similarities and differences in those across devices and time? Answering these questions theoretically informs communication and self-disclosure behaviors and online privacy management, and practically supports a more informed public education about online privacy and technology designs. We apply the comparative privacy research framework (Masur et al., 2021) to highlight device differences in privacy outcomes, and apply a content analysis using reliable conceptual categories from the media mastery framework (Rice et al., 2018; Rice et al., 2020) to identify context and themes of these phenomena salient to college students in 2006 and 2016.

We start by reviewing conceptual approaches to online privacy, including the comparative privacy research framework (Masur et al., 2021). We then provide an overview of the media mastery framework (Rice et al., 2018; Rice et al., 2020) and discuss how the framework and its boundaries subcomponents inform device comparisons in online privacy phenomena. Finally, we present theoretical arguments and empirical evidence for device and time differences in online privacy-related phenomena.

Conceptualizing Online Privacy

The concept of and actions associated with privacy have a long history (Vincent, 2016). Privacy is traditionally conceptualized as the ownership of or the right to control personal information vis-à-vis interpersonal interactions (Altman, 1975; Petronio, 2002). However, in the digital environment there are various types of (in)visible seekers, monitors, or recipients of personal information, such as scammers, social media platforms, corporations, and government agencies, posing (often unknown) daunting privacy threats to users.[1]

Privacy scholars have therefore started to recognize the multidimensional nature of online privacy, suggesting that people may be more or less concerned about online privacy and enact privacy behaviors differently, depending on the audiences, contexts, and the types of information disclosed (e.g., Dienlin & Trepte, 2015; Masur, 2018; Nissenbaum, 2010; Quinn et al., 2019). For example, Nissenbaum's (2010) theory of privacy as contextual integrity holds that privacy perceptions and behaviors are shaped by the context (the backdrop that informs privacy norms), actors (individuals and entities involved in information disclosure), attributes (types of personal information), and transmission principles (stipulations that shape the information flow in a given context). Bazarova and Masur's (2020) integrated model of online privacy proposes a conceptual distinction of online privacy along two dimensions. On the *horizontal* dimension, people manage their privacy vis-à-vis other users who may have access to their personal information (e.g., family members, friends, employers) (Marwick & boyd, 2014). On the *vertical* dimension, people deal with institutional surveillance posed by government agencies, social media companies, and other institutions that actively collect users' data for commercial, administrative, or even illegal purposes (Baruh & Popescu, 2017; Wu et al., 2019).

More recently, the comparative privacy research (CPR) framework (Masur et al., 2021) argues that privacy is contingent on cultural, social, political, economic, and technological structures, and needs to be understood by investigating such structural similarities and differences. Relevant to the current study is the technological structure that represents the types of technological environments. Although a few studies have investigated privacy differences across social media platforms (e.g., Facebook vs. Instagram, Lee & Yuan, 2020; Pekárek & Pötzsch, 2009), research lacks a comparative perspective on device differences (i.e., mobile phones vs. computers) and associated privacy perceptions and behaviors. As multiple media use becomes normative in people's everyday practices, the CPR framework calls for a comprehensive understanding of how structural similarities and differences in technological settings, affordances, and modalities shape the way people respond to privacy threats.

We adopt the notion of multidimensionality of online privacy and the CPR approach to recognize that people's online privacy perceptions and behaviors may vary across devices and shift across years as technologies, norms, knowledge, and regulations change.

The Media Mastery Framework and Online Privacy

As more digital devices, with more advanced and diverse features, apps, and formats, become available, some privacy challenges and perceptions may change, while others may persist. So rather than focusing on specific privacy phenomena associated with a particular device at a particular time, a deeper understanding requires a foundational, conceptual approach that can be applied across devices and time: here, the media mastery framework (Rice et al., 2018; Rice et al., 2020).

Media mastery refers to the (im)balance between the degree to which people understand, use, cope with, and "master" or attempt to manage media in their everyday lives, and the degree to which media in turn influence, control, facilitate, constrain, shape, and "master" people's attitudes, behaviors, and relationships (Rice et al., 2018; Rice et al., 2020).[2] The changing

balance of media mastery is influenced by characteristics of digital media and users, and therefore shifts across media, contexts, and time (Rice et al., 2020).

The overall media mastery framework integrates four main components (each with multiple subcomponents) and relationships among them: a) technology (devices, services, sites; affordances; uses), b) social aspects (social relations, social influence, self-presentation), c) individual aspects (problematic use, health, traits, cognition), and d) media mastery contexts (access, boundaries, constraints, managing content, obstacles, and use awareness). This framework helps illuminate how people more or less consciously and successfully navigate the features, uses, implications, and meanings of different types of devices, and act more or less accordingly. Moreover, this perspective emphasizes the multidimensional nature of (new, digital) media use, as well as the potential positive and negative implications of such use. So far, the media mastery framework has been applied to understand media multitasking (Zamanzadeh & Rice, 2021) and strategic cognitive media skill (Hamilton, 2020).

Development

The interest in developing the media mastery framework was initially motivated by noticing how college students in the first few years of the new millennium were trying to figure out how to (more or less successfully) master the increasing availability of multiple digital devices, such as computers, and the growing use of mobile phones (Rice & Hagen, 2010). Multiple digital devices could provide great social, business, and academic benefits, but also pose challenges to users' digital skills, social relationships, privacy, and well-being (Rice et al., 2018). The process of developing, expanding, and refining the framework encompassed different devices (desktop, laptop, tablet computers, and regular and smart mobile phones), and years (2006 and 2016), and a broad and deep literature review. This process developed components and subcomponents of the framework, and relevant content-analytic categories, using a hermeneutic approach (Boell & Cecez-Kecmanovic, 2014), which involves multiple cycles of search, acquisition, analysis, and interpretation of the literature and focus groups data on new media use, especially by college students. The authors first iteratively developed an initial media mastery typology based on an extensive literature review of new media use by college students and an analysis of focus groups conducted with college students in the U.S. in 2006 (see Rice & Hagen, 2010). After a ten-year interval, when use of laptop and tablet computers and smartphones had become more prevalent, the researchers returned to the literature to extend and revise both the components and content categories to analyze another round of focus groups in 2016 (Rice et al., 2018). Those results were used to further extend and revise the framework (see esp. Rice et al., 2020).

Relevance for Online Privacy

Although not designed to study privacy *per se*, the media mastery framework can help to broadly investigate people's online privacy-related perceptions and behaviors in three ways. First, of particular interest to our study are instances of technology use that involve the media mastery subcomponent of *boundaries*. Boundaries-related instances occur when technology is used across personal, social, and system boundaries, and/or when media use is more or less bounded, in more or less known or preferred ways (Rice et al., 2020). The boundary metaphor is also used in the Communication Privacy Management (CPM) theory (Petronio, 2002) to describe how people attempt to manage the extent to which they self-disclose or expose personal information to others. We adapt the notion of boundaries from both theoretical perspectives to conceptualize privacy boundaries as ownership lines of *personal information* between the information owners and other social and institutional actors that define the ability to control.

Therefore, we apply the subcomponents of *boundaries* from the media mastery framework to understand how people perceive and manage privacy boundary issues with multiple devices.

Second, media mastery proposes that people often attempt to manage the challenges and tradeoffs of media use, such as the balance between managing privacy, self-disclosure, identification, and access to online benefits. The privacy calculus model (Dienlin & Metzger, 2016; Laufer & Wolfe, 1977) similarly argues that people self-disclose based on a benefit-risk tradeoff, where online users may strategically self-present for affective, financial, and social benefits at the (often unknown) cost of perceived privacy and potential future risks. For example, some apps offer possibilities for usage benefits but require user information during set-up to install, authorize, or personalize; the device and/or app vendors or third parties typically use or sell that information for marketing and other purposes (Rice & Hoffman, 2018).

Third, Masur et al. (2021) in their comparative privacy research framework critiqued extant privacy research for its limited generalizability as findings are primarily derived from a single cultural, social, and technological context. Very few studies have explicitly compared multiple technologies and implications on privacy, and the existing ones mainly focus on affordances associated with multiple platforms (Lee & Yuan, 2020; Pekárek & Pötzsch, 2009), rather than with different devices (e.g., computers vs. mobile phones). The emphasis on multiple media use and the implications on the associated privacy benefits and risks of the media mastery framework can thus guide a broad accounting of privacy-related perceptions, experiences, and behaviors that span theoretical and socio-technological constraints, through a comparative privacy lens (Masur et al., 2021).

Consequently, from the media mastery perspective, online privacy can be understood as an ongoing (more or less conscious, continuous, and successful) process through which people continue to learn, understand, and cope with information disclosure and privacy protection, within and across boundaries and devices, vis-à-vis other people and institutions, over time. That is, users attempt to learn how to master, while also attempting to learn how to avoid being mastered by, privacy-related aspects of digital devices.

Applying Boundaries Subcomponents to Online Privacy

As noted, the full media mastery framework includes four main components (technology, social, individual, and media mastery). The media mastery component includes five subcomponents, one of which is "boundaries". After iterative discussions, we identified 13 of the 22 boundaries components that were most relevant to, and representative of, privacy boundary phenomena. Table 1 provides their definition, operational examples with both computer and mobile devices, and key references that demonstrate their connection to the privacy literature.

– Table 1 –

To elaborate, *anonymity*, *context collapse*, and *visibility-transparency* address how the networked nature and affordances of digital technology shape the dynamic of information flow and privacy management (Evans et al., 2016; Pearce et al., 2018; Trepte, 2021; Vitak, 2012). *Audience* and *public* highlight the variety of observers, monitors, and receivers of personal information and may include social media friends, strangers, doxxers, governments, law enforcements, and companies (Bazarova & Masur, 2020; Marwick & Boyd, 2014). *Parental access* and *surveillance* may entail monitoring, observing, and obtaining information about other users without conscious awareness and/or permission, and may involve both social and institutional actors as the audiences for personal information (Boerman & Segijn, 2022; Wang & Metzger, 2023). *Self-broadcasting* normally involves publicly disclosing personal information, posing both benefits and risks to privacy (Bazarova & Choi, 2014), whereas *privacy*

management is the use of strategies to protect personal information and ensure data *safety* from social and institutional actors (Dodel & Mesch, 2018; Epstein & Quinn, 2020). *Trust*, *vulnerability*, and *watchfulness* are psychological mechanisms that underlie privacy management and/or self-disclosure (Joinson et al., 2010; van Ooijen et al., 2022; Walker & Hargittai, 2021). We note that in the context of online privacy, these components may not be mutually exclusive and may interact with each other to influence privacy outcomes. For example, parental access may be considered as one form of surveillance; high perceived vulnerability and lack of trust in social media companies may prompt more frequent privacy management behaviors. Nonetheless, to the extent that these components were generated through multiple (re)iterations of the research literature and focus group analyses via a hermeneutic approach (Rice et al., 2020), they each represent a unique aspect of boundary issues that were of interest to researchers and college student users.

Media Mastery Contexts for Comparing Online Privacy

The following sections discuss how the media mastery framework and the CPR framework guide us to understand comparisons of online privacy boundary phenomena across devices (desktop/laptop/tablet computers vs. cell phones/smartphones) and years (2006 vs. 2016).

Device Comparisons

As part of the media mastery process, media *convergence* represents the ability for users to navigate through the content, capacities, and functionalities of multiple devices, while media *comparisons* refer to how users more or less strategically select different devices for different purposes based on their motivations and the devices' distinct capabilities and affordances (Evans et al., 2016; Rice et al., 2018). Extending to online privacy, users may leverage multiple devices or selectively use different devices and their functionalities to achieve different goals (e.g., computer for storing and analyzing content, or connecting to email; mobile phone for location sharing, or texting). Similarly, the CPR framework advocates for comparisons of technological structures as device-specific affordances may foster different privacy outcomes. Both the media mastery and the CPR perspectives suggest privacy concerns and behaviors may differ based on several reasons. Below, we review evidence for device differences based on (a) device structural settings and privacy protection capacities and (b) users' psychological mechanisms, which inform our comparisons.

Device Structural Settings and Privacy Protection Capacities

Mobile phones and computers differ in general structural settings (Napoli & Obar, 2014; Sundar et al., 2018; Rice et al., 2022), which may have privacy implications. For example, *technological capacities* may include memory and processing speed that facilitate information storage and sharing over the device. *Capacity for content viewing and creation* allows users to engage with and contribute to the media environment, which may include sharing personal information online. *Hardware* such as camera, screen size, keyboard, microphone, may facilitate and/or constrain the type and amount of information shared. *Portability* as a defining affordance of mobile devices allows real-time and nearly effortless information sharing. *Location awareness and sharing* makes it especially easy for personalized and interactive information sharing on mobile phones. These structural settings, of course, evolve over time.

At least in the early years, structural constraints of mobile phones (e.g., slower internet speed, smaller screen size) manifested in their less sophisticated privacy protection mechanisms, such as less secure password-based authentication and network connectivity (Botha et al., 2009; Suh & Hargittai, 2015; Thompson et al., 2017). Indeed, mobile phones were three times more

susceptible to phishing attacks than desktop computers due to the limitations in system architectures (Goel & Jain, 2018), and have stimulated privacy and security concerns regarding identity theft, information security (Silver et al., 2019), physical loss and tracking (Botha et al., 2009; Chin et al., 2012). Perhaps due to these reasons, mobile phone users reported lower confidence in their own ability to protect their privacy and showed suspicions about the effectiveness of existing privacy protection mechanisms on mobile phones (McGill & Thompson, 2017; Thompson et al., 2017). They were also less inclined to enter social security numbers, make purchases, access health and medical records, and log into bank accounts on mobile phones than computers (Chin et al., 2012).

Users' Psychological Mechanisms

Another stream of research shows that users develop unique psychological mechanisms that underlie their privacy and self-disclosure behaviors on different devices. For example, research drawing from the heuristics perspective argues that people use mental shortcuts or cognitive rules of thumb to help make quick privacy judgments (e.g., Sundar et al., 2020). Particularly related to device differences is the mobility heuristic, which says that mobile devices are considered inherently less secure than desktop devices in protecting personal information due to mobile phones' higher risks of being stolen or lost, smaller size, and portability (Sundar et al., 2020). Thus users' belief in the mobility heuristic may make them more concerned about privacy and disclose less information over mobile phones than over computers.

Alternatively, research shows that as mobile phones are deeply embedded in people's everyday lives, users develop intimate emotional experiences with their mobile phones, and consider them to be a "personal technology" (Vincent, 2013). Such strong feelings of psychological ownership may cultivate a sense of trust towards mobile phones, thus habituating users to click through privacy prompts without scrutinizing them (Anderson et al., 2017) and prompting more intimate self-disclosure on mobile phones (such as through social media) (Quinn & Oldmeadow, 2013; Walsh et al., 2009). Consequences include lower levels of privacy awareness, lower levels of perceived severity of data breaches, and less secure privacy management behaviors on mobile devices than on computers (Kelley et al., 2012; McGill & Thompson, 2017; Mylonas et al., 2013; Thompson et al., 2017).

Indeed, Murthy and colleagues (2015) found that compared to web tweets, mobile tweets contained more references to the self, as manifested by the use of first-person pronouns. The authors suggested that the inherently personal nature of mobile phones facilitate more egocentric self-disclosure, whereas web devices encourage more careful articulations, reflections of thoughts, and references to others, implying greater privacy risks associated with mobile phones. Similarly, Groshek and Cutino (2016) reported that mobile tweets included more uncivil and impolite content, attributing this finding to mobile-specific features (e.g., ready accessibility) that allow users to record their immediate feelings with less contemplation. One study, however, found that people were more likely to notice and click on phishing emails on desktop computers than mobile phones, which suggests more privacy incursions over computers (Liao et al., 2023)

In sum, though finding mixed evidence, the research above shows that users have varying levels of privacy concerns, and engage in protective behaviors differently, over mobile phones and computers due to a) technological structures (e.g., device capacities for information processing and security) and b) users' psychological mechanisms (e.g., privacy heuristics associated with devices, psychological ownership).

Year Comparisons

Media mastery is a process, as people's media use patterns constantly involve negotiations, challenges, self-regulation, learning, social influence, and changes in technologies (Rice et al., 2018). Online privacy is also a process, in which people continuously (re)evaluate their attitudes and motivations, and adjust privacy behaviors accordingly over time (Meier & Krämer, 2023). There is thus a need to focus on temporary changes in people's privacy perceptions and behaviors (see also Dienlin et al., 2023; Masur & Trepte, 2021). Here, we discuss two prominent reasons for a temporal comparison in online privacy—one hinging upon technological shifts and one accounting for broader changes in privacy awareness, attitudes, efficacies, and literacies.

The review above on device differences suggests that changes in privacy outcomes over time may be influenced by *technological advances in privacy-related functionalities*. For example, in recent years many desktop privacy functions have been integrated into mobile phones, especially as smartphones become powerful. Indeed, in a replication of Chin et al. (2012), Schessler et al. (2021) found no significant difference in willingness to perform privacy-related tasks on either device. They argued that the privacy ecosystem matured on mobile phones, so it has become more accessible and convenient for users to protect privacy. Rice et al. (2022) also broadly found that the digital device divide (i.e., socioeconomic and demographic differences in uses and activities associated with desktop computers and mobile phones) has been withering over the years, thus rejecting an earlier presumption of desktop computer superiority. As a result, privacy concerns and behavior with both devices have likely changed over time due to evolutions in privacy-related structural settings.

At the same time, the range of digital devices changed considerably between 2006 and 2016 (see Table 2). Nearly three-quarters of US adults had accessed the Internet, had a computer or laptop, or used a mobile phone by 2006. However, in 2006, tablet and smartphone use were both below 3%. By 2016 those figures had jumped to 51% and around 80%, respectively. As the functionality of mobile phones expanded and devices became more affordable, mobile phones were now integrated into many aspects of everyday lives and offered a wide variety of applications. For example, social media have become a primary aspect of mobile phone use given its mobility, camera, audio recording, and immediate sharing affordances. Because of the increasing use of smartphones and social media in the years after 2006, it is likely that people's early privacy experiences that were primarily reflected in their desktop use had gradually shifted into mobile phone use.

– Table 2 –

In addition, longitudinal studies that track users' general privacy perceptions and behaviors suggest some interesting differences in *privacy awareness and attitudes* over time. Goldfarb and Tucker (2012) found that people increasingly refused to reveal personal information between 2001 and 2008, suggesting an increase in privacy awareness and management behaviors. Tracking a cohort of teenagers, Kelly et al. (2017) found their autonomy, connectedness, and competence shifted across 8 years. In particular, participants evolved from a mindset of *experimenters* who had nothing to lose in 2007, to *accepters* who weighed social benefits over privacy concerns in 2011, to *managers* who strategically protected their privacy in 2015, suggesting an increase in privacy concerns, awareness, and skills. Antón et al. (2010) found that people felt more uncomfortable with institutional data collection and personalization in 2008 than in 2002. Finally, Tsay-Vogel et al. (2018) reported an increase in various privacy-related perceptions from 2010 through 2015, including perceived threat to general privacy and

online privacy, support for governmental privacy protection, and a decrease in online and offline self-disclosure.

Research Questions

Based on the preceding evidence and arguments, we ask two guiding research questions about privacy boundary phenomena as operationalized by the 13 boundary subcomponents: What are the similarities and differences in the nature, relative frequency, and combinations of online privacy boundary phenomena comparing the following?

RQ1: Devices: Computers (desktop, laptop, tablets) vs. mobile phones (cell phone, smartphone)

RQ2: Years: 2006 vs. 2016

Method

Analyses

Content Analysis

We conducted a content analysis of two different sets of six college student focus groups on computer and mobile phone use (RQ1) a decade apart (RQ2). A content analytic approach, rather than an inductive qualitative analysis of the focus groups (as, for example, Best & Tozer, 2013), is appropriate for our study because first, it is informed *a priori* by the comparative privacy research and the media mastery frameworks (rather than relying on *emergent* codes and themes), and second, it allows us to investigate and compare the relative frequency of the selected boundaries codes being discussed across digital devices and years. We conducted an *a priori* coding of the focus group comments using the 13 privacy-related boundaries subcomponents of the media mastery framework. We applied a descriptive content analysis approach, described by Neuendorf (2017) as one "in which all variables analyzed are measures from within the content analysis, without attempts to infer or predict to source variables or receiver variables" (p. 73). We also provide selected quotes from both the focus groups to illustrate our findings (see Table 1). And because the content analysis aligns with the nomothetic approach, of which the goal is to create general patterns rather than interpretations of individual cases (Neuendorf, 2017), our findings can contribute to a broader accounting of similarities and differences in various online privacy phenomena across these comparisons.

Cluster Analysis

Co-occurrences and relationships among the privacy-related codes can portray some of the complexities and interdependencies among privacy phenomena over mobile phone and computer use. Clustering of code co-occurrence is a common approach to identifying underlying themes in content analysis (Neuendorf, 2017). A cluster is a set of codes that co-occur frequently (here, within a given focus group), at each increasingly distant level of clustering. Co-occurrence frequency is conceptually and empirically distinct from overall frequency; two codes might be mentioned frequently across analysis units, but rarely within the same analysis unit.

Data Sources

Focus groups were used as the data-collection method because the interactive discussion within groups facilitates participants to recall, elaborate, and generate diverse opinions and meanings (Krueger & Casey, 2015). Six focus groups of 6-8 U.S. college Communication students at a southwestern university were conducted each in 2006 and in 2016. Conradson (2013) noted that the inclusion of same- and mixed-gender focus group discussions controls for possible gender bias in participation and openness, providing both group homogeneity and heterogeneity. Thus our sample included, for 2006, 35 participants in total (32 females, 3 males),

with 4 groups all female, and 2 groups mixed; for 2016, 42 participants in total (21 females, 21 males), with 2 groups all male, 2 all female, and 2 groups mixed.

Both studies were approved by the university's Institutional Review Board. College students were chosen because they are usually exposed to diverse new media, and therefore have more experiences with online self-disclosure and privacy management. They are also savvy and heavy digital media users, experiencing a set of positive and negative outcomes (Pew Research Center, 2021a; 2021b), though also experience digital divides and technology inadequacies (Jaggars et al., 2021).

As noted above, the focus groups were not conducted to specifically discuss online privacy phenomena; they were part of a sequential, hermeneutic approach to develop and validate the media mastery framework. When designing and conducting the focus groups, neither the researcher, moderator, the research assistant, nor the participants were explicitly or intentionally focusing on privacy phenomena. The online privacy frame was only applied after all the data were collected. To some extent, then, we may consider the analysis process as a form of *goal-free evaluation* (primarily used in educational settings; Youker et al., 2016) with respect to privacy phenomena (but not with respect to developing the media mastery framework). The argument for goal-free evaluation is that the approach removes issues such as response or researcher bias, pre-specified goals, leading questions, side effects, or unexpected material. Thus, to the extent that participants mentioned issues related to online privacy, those were unprompted, and presumably salient to the participants. However, such comments were also likely far less frequent than if the focus groups were conducted specifically about privacy boundary phenomena associated with computers and mobile phones.

Based on the literature reviewed up to 2006 about college students' use of digital media (discussed above), seven questions were developed and pretested (see Table 3). In each focus group, the moderator asked each of the seven questions separately about the use of computers (desktops and laptops in 2006; tablet computers were included in 2016) and mobile phones.[3] Discussions were recorded and then transcribed. Thus, we analyze transcripts from six college student focus groups for each year (2006 and 2016), discussing the questions for each set of devices (computers and mobile phones), for a total of 12 focus groups, generating four combinations of device and year, allowing for aggregations across, and interactions between, devices and years.

– Table 3 –

Coding Procedure

The Codebook, Codes, and Coding Units

The codebook was adapted from 13 codes in the boundaries component of the media mastery typology (Rice et al., 2020). Because our focal variable of interest is any privacy issue represented in the boundaries codes, which may include privacy perceptions, behaviors, audience of personal information, and technological affordances that may influence privacy decisions, we consider the focus group responses as latent content, which is defined as unobservable concepts that "cannot be measured directly but can be represented or measured by one or more… indicators" (Hair et al., 2010, p. 614). The unit of analysis was each individual's separate verbal response to each question, regardless of the number of sentences within the same response or the number of responses from the same participant, as long as they were separated by other participants' comments. We coded 1 for each specific boundaries subcomponent indicated in a unit of analysis, and 0 if not, regardless of the total number of times the same subcomponent was mentioned in the same unit.

Content Analysis Training and Reliabilities

Following the procedure outlined in Neuendorf (2017), our training included three rounds of coding together and independently, discussing and resolving disagreements between the two coders, and revising the codes. In the first round, the coders first discussed the operationalizations of all codes and coded a small set of content together as a consensus-building process, and then independently coded responses to two questions in both 2006 and 2016 focus groups, and made small revisions to the codebook based on discussions. The second round consisted of each coder independently coding all six focus groups in 2016. Inspection of the crosstabulation confusion matrix showed that a few differences occurred in the cross-coding of audience, privacy, and visibility. Each disagreement was discussed and resolved, with respective slight clarifications added to the codebook operationalizations. In the final round of coding, all 2006 focus groups were independently coded. Overall, reliability analyses of all 2006 and 2016 data combined revealed high scores for Cohen's Kappa (from .90 for context collapse, to 1.00 for parental access, and trust) (see Table 4). To prepare the final coded data for analysis, the two coders had another discussion to resolve the few remaining disagreements.

– Table 4 –

Results

Descriptives

Table 5 reports the descriptive statistics for each code. The most frequently occurring boundary components across devices and years were audience (3.55%), visibility-transparency (3.50%), self-broadcasting (1.36%), privacy management (1.27%), and safety (1.1%), while parental access (.03%) and trust (.06%) occurred the least frequently.

– Table 5 –

Comparisons of Privacy Boundary Phenomena Across Devices and Years

To answer RQ1 and RQ2, a multivariate analysis of variance was conducted to compare the proportions of each boundary code across sets of devices (computer, mobile phone) and years (2006, 2016) (see Table 6). Overall, results showed some statistically significant differences (though small effect sizes) in boundary codes for device, year, and their interaction. We elaborate on the findings and discuss their implications below.

– Table 6 –

Audience was referred to more for computers than for mobile phones, with an interaction with year, as the highest value was for computers in 2006. One possible explanation is that, compared to mobile phones, the diverse ways that computer devices were utilized (e.g., work, education, entertainment), particularly in 2006 before smartphones, encompass a wider range of audiences, such as friends, family, but also coworkers, employers, institutions and organizations. This makes intuitive sense given our speculation that people's privacy experiences may be primarily reflected in their desktop experiences in the earlier time frame (i.e., 2006), while they would be reflected in both computer and mobile use in later years (i.e., 2016). Our data suggest that while participants in 2006 were generally interested in the capability of the internet (accessed through computer devices) to widely share aspects of their personal lives with different audiences, by 2016 participants showed some awareness of the collection and processing of personal data by institutional and organizational actors, such as third-party marketing companies, consistent with previous research (e.g., Bazarova & Masur, 2020; Rice & Hoffmann, 2018).

Public exhibited significant differences by year (higher in 2006), device (higher for computers) and the interaction (highest for computers in 2006). Similar to the audience subcomponent, participants in 2006 were more likely than in 2016 to discuss experiences of

disclosing personal information to the public with computer devices. Beyond evidence for early fascination for computer devices, such decreasing salience of "public" may indicate a growing awareness of privacy risks of making personal information available to the public.

Privacy management showed only an interaction effect, with the highest mention for mobile devices in 2016. We conceptualized this term as "the desire and the (in)ability for a person to seclude their personal information from other actors" to reflect the paradox that regardless of their privacy concerns, people may not always have the ability to protect their privacy online given the limited mechanisms offered by technology designers (Hoffmann et al., 2016; Taddei & Contena, 2013), or may see that the benefits outweigh the possible risks (Dienlin & Metzger, 2016). Instances in which participants described the lack of self-efficacy in privacy management were frequently brought up in 2016, given the burgeoning capacities of mobile devices and platforms to collect user data and metadata. For example, participants noted their (in)ability to protect privacy in terms of location sharing and content curation.

Safety references were higher in 2006 than 2016. Participants in 2006 noted safety concerns regarding each device, though not statistically differently. Consistent with previous studies (Chin et al., 2012; O'Neil, 2001), our results confirmed that people felt their mobile devices were more susceptible to physical loss than computers, which created privacy risks because mobile phones store a variety of private information (e.g., text messages, photos, and contact information). Computer devices were more likely to arouse concerns such as viruses and online identity theft in 2006. Such decreasing safety concerns over time perhaps show evidence for the maturing safety protection mechanisms on both devices (e.g., dual-factor authentication, biometrics, find-my-iPhone).

Self-broadcasting was indicated significantly more in 2016, and via an interaction of mobile phones in 2016. This finding shows the prevalence and variety of social media platforms on smartphones in recent years. Combined with the salience of *privacy management* for mobile phones in 2016, however, it is interesting to note that while participants expressed the attempt to protect privacy online, and sometimes noted a lack of ability to do so, they continued to self-broadcast and share personal information online. Even though self-broadcasting is a voluntary behavior per se, motivations for self-broadcasting can be social, material, and psychological benefits enabled by a digital medium. This manifests the central tenet of the media mastery framework that while users attempt to master multiple media, media may also be mastering the users.

Surveillance showed only an interaction, with the highest percentage for mobile phones in 2016. Our conceptualization of surveillance encompasses privacy instances on both interpersonal and institutional levels. Consistent with *audience*, while in 2006 participants occasionally brought up online stalking instances, in 2016 participants showed strong awareness of how manifestations of personal information may also be tracked and leveraged for commercial purposes. But again, they may engage in a privacy calculus favoring perceived benefits over risks.

Finally, *visibility-transparency* was mentioned proportionally more for computers, especially in 2016. This code refers to the "capacity for aspects and/or manifestations of personal information to be visible to others, either intentionally or unintentionally." As suggested above, there may be more diverse audiences via computer devices in 2016, including other online users but also organizations and institutions, to whom personal information may be accessible. And these audiences may be more salient to people on computers, as such devices may facilitate greater self-reflection and rational thinking, and the content may be more work-related (Murthy

et al., 2015). However, it is a bit surprising that visibility-transparency was not more mentioned in the 2016 mobile phone comments, given the by-then pervasiveness of both mobile phones and social media, and indeed the increasing emphasis on social and cultural visibility through social media.

No significant differences in mean percentages for device or year were found for *anonymity*, *context collapse*, *parental access*, *trust*, *vulnerability*, and *watchfulness*. These were also among the least frequently mentioned codes, which suggests that these aspects of privacy were of less general interest to our participants regardless of device or year.

Overall, computer devices gathered more attention in aspects of *audience* and *public*, while discussions of mobile phones revolved more around *privacy management*, *self-broadcasting*, and *surveillance*, with interactions of the year (i.e., highest for 2016). In addition, while focus group participants showed a more nuanced understanding of online privacy in 2016, they might still engage in potentially privacy-threatening practices, such as *self-broadcasting*, perhaps as a result of a risk-benefit calculus. Nonetheless, we see a positive picture where people transitioned from passively accepting and thus being mastered by the privacy boundaries set by technological affordances to (at least somewhat) taking agency and trying to master their privacy boundaries (see Kelly et al., 2017), though sometimes favoring benefits while perhaps discounting, or not being aware of, risks.

Themes of Privacy Boundary Phenomena from Cluster Analysis

Figure 1 presents the dendrogram from a hierarchical cluster analysis of the co-occurrences of the 13 codes within each focus group, aggregated across all the focus groups. The dendrogram indicates the most frequently co-occurring codes as the most specific clusters (here, codes connected near the left; that is, the furthest from other terms), and the less frequently co-occurring codes cluster at greater distance levels (here, near the right). The top left theme may be considered to represent *crossing the boundary from private to public*, where one actively engages in providing visibility and self-broadcasting about oneself to an audience or the public, often relating to *context collapse.* The second theme represents the typical connotation of *privacy intrusion*, crossing from public (or unknown others) into the private via surveillance, associated with the feeling of vulnerability and watchfulness. The third theme underscores how a sense of privacy involves both *safety and trust*. The fourth theme seems to indicate concern about *managing one's anonymity,* often with respect to *parents*, or perhaps more generally to authority figures. These two issues are not specifically aligned with any of the other clusters.

– Figure 1 –

Contributions, Limitations, and Future Directions

Our study makes several theoretical contributions. Perhaps the most important contribution is an empirical analysis of device differences across a decade concerning a wide array of online privacy phenomena. In particular, our study applies the concept of technological structures (through differentiating devices) as an important yet understudied comparison unit proposed by the comparative privacy research framework (Masur et al., 2021). As we argue, device differences in privacy may occur as a result of (a) device structural settings and physical characteristics (e.g., keyboard, screen size), privacy protection capacities (e.g., hardware, portability, location awareness) and (b) users' psychological mechanisms (e.g., mobility heuristic, psychological ownership). As such, we echo Masur and colleagues' (2021) argument and previous privacy theorizing (e.g., contextual integrity; Nissenbaum, 2010) that a holistic understanding of privacy behaviors must account for context that informs the privacy norms,

actors involved in the disclosure, attributes of information being disclosed, and transmission principles that govern information flow.

As most privacy research has focused on a single technological device or platform, our comparisons add an important piece of knowledge to the literature by drawing attention to the influences of structural settings of technologies on privacy, and reinforce the need to study privacy across situations, contexts, and time. We therefore argue that future theorizing and operationalization of online privacy should consider structural differences in technology design that may be at play during privacy decision-making. For example, future research should specify the technological context of privacy research in the measurement (e.g., privacy concerns on social media on mobile phones). We believe our results can inspire a fruitful line of research that aims to further disentangle the interplay between the structural settings of digital technology (e.g., affordances) and users' privacy experience.

Another highlight of this study is its scope. Recent privacy scholarship suggests that privacy should be understood as a multidimensional decision process (Quinn et al., 2019). Our content analytical approach that quantitatively compares the boundaries subcomponents adapted from the media mastery framework allowed us to empirically test 13 theoretically-informed "dimensions" of privacy that would otherwise be more challenging to achieve in a single survey or qualitative study. Therefore, this study advances the multidimensional nature of privacy, and these dimensions provide a theoretically motivated starting point for future comparative studies on, for example, media coverage about privacy across nations or cultures (see Masur et al., 2021). Doing so also demonstrates the utility of the media mastery framework in guiding research on how people understand, cope with, and master multiple media vis à vis online privacy (Rice et al., 2018; Rice et al., 2020). We further advance the framework by addressing how these structures may further change over time. Results confirmed differences in privacy phenomena across devices and years, and their interactions, thereby further highlighting the contextual and processual nature of privacy management (Masur, 2018; Nissenbaum, 2010).

Practically, our study adapts a taxonomy of 13 boundaries topics that can serve as an explicit guide for privacy educators and stakeholders. Interventions such as the social media testdrive (DiFranzo et al., 2019; https://socialmediatestdrive.org/) can implement this taxonomy for privacy education. For instance, based on the high co-occurrence of *audience, visibility-transparency* and *self-broadcasting* in our data, privacy educators may note that when publicly sharing (self-broadcasting) one's life online, such information may be visible or transparent to different types of audiences, including not only other people online, but also institutions and organizations. Practitioners may also emphasize the aspects of *privacy* that may be neglected by users, such as *vulnerability*. They may also wish to discuss privacy concerns specifically involving parents.

Both a somewhat innovative approach and limitation of the current study is that our focus groups were not specifically designed to study online privacy, and therefore participants' responses cannot fully capture a wide range of privacy-related experiences. Nonetheless, to the extent that these privacy instances were mentioned without prompting, our data provide compelling evidence that these were salient aspects of privacy across devices and years for users (in line with goal-free evaluation, Youker et al., 2016).

Further, the two sets of focus groups, while consistent in format across the decade, are extremely limited in size and representation, thus only providing initial, exploratory insights. Viewpoints of other groups who may have different privacy experiences than college students should be considered in future research. For example, research should compare such perspectives

with those from more elite groups, who tend to address privacy from the legal, institutional, and legislative perspectives. Extant research has addressed privacy discussions of various elite actors, such as mass media (Fornaciari, 2014, 2018), congresspeople (Epstein & Medzini, 2022), government representatives (Epstein et al., 2014), and technology designers (Ribak, 2019). For instance, Epstein and Medzini (2022) content-analyzed transcripts of two Congressional hearings and found that congresspeople's framing of privacy was primarily oriented toward the relationships between users and platform providers. Other studies showed that security was a primary privacy theme of technology designers (Ribak, 2019) and government representatives, while vulnerability was heavily discussed by civil society stakeholders (Epstein et al., 2014).

It is also important to acknowledge that, although we proposed mechanisms that may explain differences across device and year comparisons (based on prior research and survey reports), the descriptive nature of the content analysis does not allow us to test them. As noted earlier, these content analyses can make no claims about influences or outcomes (Neuendorf, 2017). These mechanisms could be more empirically tested in future research.

Additional samples and years would also help assess the relevance of these specific results. Those could include literature review and focus group questions specifically oriented toward privacy boundary phenomena. Quantitative studies, such as through surveys, perhaps with specific measures about privacy calculus or media features and uses, applying the boundaries privacy subcomponents, are also needed to yield more generalizable results about differences in online privacy boundary phenomena. In addition, nuances in the literature and focus groups could be coded, such as the positive and negative valence of privacy-related issues, and the horizontal and vertical conceptual distinction of online privacy (see Bazarova & Masur, 2020), to further contribute to our understanding. Future research should also build on other components of media mastery, such as the technology, social and individual aspects, to further explore people's online privacy experiences. Finally, though the age of data limits its informative value for the current time, arguably 2016 began to mark a new era of artificially intelligent technologies such as conversational agents, home or work virtual assistants, social robots, and artificial intelligence chatbots (Lutz et al., 2019; Ravacizadeh et al., 2019; Sannon et al., 2020; Wu et al., 2024), which may create unique privacy challenges that future research may address. Such research and implications may help users understand and manage the balance between mastering privacy issues in digital media, and being mastered by them.

Of particular interest for future research is therefore how artificial intelligence embedded in the applications and platforms on both devices may complicate user privacy perceptions and behaviors. For example, conversational agents and mobile APPs (e.g., Apple Health) may collect sensitive personal information through numerous sensors on mobile phones, often without user awareness, such as users' physical activity, emotional state, images of users' bedrooms and their floor plans, in order to make predictions and recommendations (e.g., health risks) (Sannon et al., 2020). Products that leverage generative artificial intelligence (GenAI), such as ChatGPT, that is widely used on desktop computers, while bringing opportunities for productivity and efficiency, pose privacy challenges for knowledge sharing, content creation, and design, as the way personal information is collected and processed remains unclear to users (Lund & Agbaji, 2023). Nevertheless, while the current study documents broad trends in users' privacy experience across two sets of devices, results should inform rich conversations around privacy implications on various policy arenas.

Conclusion

Drawing from the media mastery framework and the comparative privacy research framework, this study set out to investigate how discussions of online privacy boundary phenomena compare across devices (computers vs. mobile phones), and years (2006 vs. 2016). By applying the comparative privacy research framework, and extending the media mastery boundaries subcomponents to privacy, we uncovered similarities and differences in ways computer and mobile phone users attempt to master available privacy protection mechanisms, in some cases through tradeoffs of benefits and risks posed by communication, self-disclosure and information sharing, while in turn, becoming mastered by device capabilities and structural settings in terms of privacy concerns, risks, or surveillance. Specifically, results of our content analysis showed significant differences in some phenomena across devices and years, and interactions for a number of privacy-related boundary codes, including *audience*, *privacy management*, *public*, *safety*, self-*broadcasting*, *surveillance*, and *visibility-transparency*.

Disclosure of interest: The authors report there are no competing interests to declare.

References

Altman, I. (1975). *The environment and social behavior: Privacy, personal space, territory, crowding*. Brooks/Cole Publishing Company.

Anderson, B. B., Vance, A., Jenkins, J. L., Kirwan, C. B., & Bjornn, D. (2017). It all blurs together: How the effects of habituation generalize across system notifications and security warnings. In F. D. Davis, R. Riedl, J. vom Brocke, A. B. Randolph, P-M. Léger, & G. Müller-Putz (Eds.), *Information systems and neuroscience* (pp. 43-49). Springer, Cham.

Antón, A. I., Earp, J. B., & Young, J. D. (2010). How internet users' privacy concerns have evolved since 2002. *IEEE Security & Privacy*, *8*(1), 21-27.

Baruh, L., & Popescu, M. (2017). Big data analytics and the limits of privacy self-management. *New Media & Society*, *19*(4), 579-596.

Bazarova, N. N., & Choi, Y. H. (2014). Self-disclosure in social media: Extending the functional approach to disclosure motivations and characteristics on social network sites. *Journal of Communication*, *64*(4), 635-657.

Bazarova, N. N., & Masur, P. K. (2020). Towards an integration of individualistic, networked, and institutional approaches to online disclosure and privacy in a networked ecology. *Current Opinion in Psychology*, *36*, 118-123.

Best, K., & Tozer, N. (2013). Scaling digital walls: Everyday practices of consent and adaptation to digital architectural control. *International Journal of Cultural Studies, 16*(4), 401-417.

Bishop, S. (2018). Anxiety, panic and self-optimization: Inequalities and the YouTube algorithm. *Convergence*, *24*(1), 69-84.

Boell, S. K., & Cecez-Kecmanovic, D. (2014). A hermeneutic approach for conducting literature reviews and literature searches. *Communications of the Association for Information Systems*, *34*(1), 257-286.

Boerman, S. C., & Segijn, C. M. (2022). Awareness and perceived appropriateness of synched advertising in Dutch adults. *Journal of Interactive Advertising*, *22*(2), 187-194.

Botha, R. A., Furnell, S. M., & Clarke, N. L. (2009). From desktop to mobile: Examining the security experience. *Computers & Security*, *28*(3-4), 130-137.

Büchi, M., Festic, N., Just, N., & Latzer, M. (2021). Digital inequalities in online privacy protection: Effects of age, education and gender. In E. Hargittai (Ed.), *Handbook of digital inequality* (pp. 296-310). Edward Elgar Publishing.

Chen, H. T. (2018). Revisiting the privacy paradox on social media with an extended privacy calculus model: The effect of privacy concerns, privacy self-efficacy, and social capital on privacy management. *American Behavioral Scientist*, *62*(10), 1392-1412.

Chin, E., Felt, A. P., Sekar, V., & Wagner, D. (2012, July). Measuring user confidence in smartphone security and privacy. In *Proceedings of the eighth symposium on usable privacy and security* (pp. 1-16). ACM.

Conradson, D. (2013). Focus groups. In R. Flowerdew & D. M. Martin (Eds.), *Methods in human geography* (pp. 128-143). Routledge.

David, P., Kim, J-H., Brickman, J. S., Ran, W. & Curtis, C. M. (2015). Mobile phone distraction while studying. *New Media & Society, 17*(10), 661-1679.

DeSanctis, G., & Poole, M. S. (1994). Capturing the complexity in advanced technology use: Adaptive structuration theory. *Organization Science, 5*(2), 121-147.

DeVito, M. A. (2017). From editors to algorithms: A values-based approach to understanding story selection in the Facebook news feed. *Digital Journalism*, *5*(6), 753-773.

Dienlin, T., Masur, P. K., & Trepte, S. (2023). A longitudinal analysis of the privacy paradox. *New Media & Society*, *25*(5), 1043-1064.

Dienlin, T., & Metzger, M. J. (2016). An extended privacy calculus model for SNSs: Analyzing self-disclosure and self-withdrawal in a representative US sample. *Journal of Computer-Mediated Communication, 21*(5), 368-383.

Dienlin, T., & Trepte, S. (2015). Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. *European Journal of Social Psychology, 45(*3), 285-297.

DiFranzo, D., Choi, Y. H., Purington, A., Taft, J. G., Whitlock, J., & Bazarova, N. N. (2019, May). Social media testdrive: Real-world social media education for the next generation. In *Proceedings of the 2019 CHI conference on human factors in computing systems* (pp. 1-11).

Dodel, M., & Mesch, G. (2018). Inequality in digital skills and the adoption of online safety behaviors. *Information, Communication & Society*, *21*(5), 712-728.

Durnell, E., Okabe-Miyamoto, K., Howell, R. T., & Zizi, M. (2020). Online privacy breaches, offline consequences: Construction and validation of the concerns with the protection of informational privacy scale. *International Journal of Human–Computer Interaction, 36*(19), 1834-1848.

Epstein, D., & Medzini, R. (2022). Conversations with fellow leaders: Privacy framing in congressional hearings after Cambridge Analytica. *Telecommunications Policy*, *46*(10), 102427.

Epstein, D., & Quinn, K. (2020). Markers of online privacy marginalization: Empirical examination of socioeconomic disparities in social media privacy attitudes, literacy, and behavior. *Social Media+ Society*, *6*(2), 2056305120916853.

Epstein, D., Roth, M. C., & Baumer, E. P. (2014). It's the definition, stupid! Framing of online privacy in the internet governance forum debates. *Journal of Information Policy*, *4*(1), 144-172.

Evans, S. K., Pearce, K. E., Vitak, J., & Treem, J. W. (2016). Explicating affordances: A conceptual framework for understanding affordances in communication research. *Journal of Computer-Mediated Communication*, *22*(1), 35-52.

Fornaciari, F. (2014). Pricey privacy: Framing the economy of information in the digital age. *First Monday*, *19*(12).

Fornaciari, F. (2018). What is privacy anyway? A longitudinal study of media frames of privacy. *Journal of Intellectual Freedom and Privacy, 3*(1), 8-20.

Goel, D., & Jain, A. K. (2018). Mobile phishing attacks and defense mechanisms: State of art and open research challenges. *Computers & Security*, *73*, 519-544.

Goldfarb, A., & Tucker, C. (2012). Shifts in privacy concerns. *American Economic Review*, *102*(3), 349-353.

Groshek, J., & Cutino, C. (2016, July). Meaner on mobile: Incivility and impoliteness in communicating online. In *Proceedings of the 7th 2016 International conference on social media & society* (pp. 1-7).

Hair, J. F., Jr., Black, W. C., Babin, B. J., & Anderson, R. E. (2010). *Multivariate data analysis* (7th ed.). Prentice Hall.

Hamilton, K. A. (2020). *The extended organism: A framework for examining strategic media skill in a digital ecology*. Unpublished Doctoral dissertation, University of Illinois at Urbana-Champaign.

Hawi, N. S., & Samaha, M. (2017). The relations among social media addiction, self-esteem, and life satisfaction in university students. *Social Science Computer Review*, *35*(5), 576-586.

Helles, R. (2013). Mobile communication and intermediality. *Mobile Media & Communication, 1*(1), 14-19.

Hoffmann, C. P., Lutz, C., & Ranzini, G. (2016). Privacy cynicism: A new approach to the privacy paradox. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 10*(4), 7.

Hussain, Z., Griffiths, M. D., & Sheffield, D. (2017). An investigation into problematic smartphone use: The role of narcissism, anxiety, and personality factors. *Journal of Behavioral Addictions, 6*(3), 378-386. [Citing Lookout Mobile Security. (2012). Mobile Mindset Study. https:/www.mylookout.com/resources/reports/mobile-mindset]

IAB, ABI Research. (2012, July). *Mobile's role in a consumer's media day: Smartphones and tablets enable seamless digital lives.* IAB Mobile Center of Excellence Research Program.

Jaggars, S. S., Motz, B. A., Rivera, M. D., Heckler, A., Quick, J. D., Hance, E. A., & Karwisch, C. (2021). The digital divide among college students: Lessons learned from the COVID-19 emergency transition. Policy Report. *Midwestern Higher Education Compact*. https://www.mhec.org/sites/default/files/resources/2021The_Digital_Divide_among_College_Students_1.pdf

Jensen, K. B. (2010). *Media convergence: The three degrees of network, mass, and interpersonal communication.* Routledge.

Ji, P., & Lieber, P. S. (2010). Am I safe? Exploring relationships between primary territories and online privacy. *Journal of Internet Commerce, 9*(1), 3-22.

Joinson, A. N., Reips, U. D., Buchanan, T., & Schofield, C. B. P. (2010). Privacy, trust, and self-disclosure online. *Human–Computer Interaction, 25*(1), 1-24.

Jones, M. R., & Karsten, H. (2008). Giddens's structuration theory and information systems research. *MIS Quarterly, 32*(1), 127-157.

Kang, H., & Jung, E. H. (2021). The smart wearables-privacy paradox: A cluster analysis of smartwatch users. *Behavior & Information Technology*, *40*(16), 1755-1768.

Kanter, M., Afifi, T., & Robbins, S. (2012). The impact of parents "friending" their young adult child on Facebook on perceptions of parental privacy invasions and parent–child relationship quality. *Journal of Communication, 62*(5), 900-917.

Katz, J. E. & Rice, R. E. (2002). *Social consequences of Internet use: Access, involvement and interaction*. The MIT Press.

Kelly, L., Kerr, G., & Drennan, J. (2017). Privacy concerns on social networking sites: A longitudinal study. *Journal of Marketing Management, 33*(17-18), 1465-1489.

Kelley, T., Camp, L. J., Lien, S., & Stebila, D. (2012, July). Self-identified experts lost on the interwebs: The importance of treating all results as learning experiences. In *Proceedings of the 2012 workshop on learning from authoritative security experiment results* (pp. 47-54). ACM.

Kim, J., & Sung, Y. (2022). Artificial intelligence is safer for my privacy: Interplay between types of personal information and agents on perceived privacy risk and concerns. *Cyberpsychology, Behavior, and Social Networking*, *25*(2), 118-123.

King, D. L., & Delfabbro, P. H. (2020). Video game addiction. In C. A. Essau & P. H. Delfabbro (Eds.), *Adolescent addiction: Epidemiology, assessment, and treatment* (pp. 185-213). Academic Press.

Krasnova, H., Günther, O., Spiekermann, S., & Koroleva, K. (2009). Privacy concerns and identity in online social networks. I*dentity in the Information Society*, *2*(1), 39-63.

Krueger, R. A., & Casey, M. A. (2015). *Focus groups: A practical guide for applied research* (5th ed.). Sage.

Latour, B. (2007). *Reassembling the social: An introduction to actor-network-theory*. Oxford University Press.

Laufer, R. S., & Wolfe, M. (1977). Privacy as a concept and a social issue: A multidimensional developmental theory. *Journal of Social Issues*, *33*(3), 22-42.

Lee, Y. H. & Yuan, C. W. (2020). The privacy calculus of "friending" across multiple social media platforms. *Social Media + Society*, *6*(2), 1-10.

Li, X., Chen, W., & Straubhaar, J. D. (2018). Privacy at the margins| concerns, skills, and activities: Multilayered privacy issues in disadvantaged urban communities. *International Journal of Communication*, *12*, 22.

Liao, M., Wang, J., Chen, C., & Sundar, S. S. (2023). Less vigilant in the mobile era? A comparison of information processing on mobile phones and personal computers. *New Media & Society*, 14614448231209475.

Lum, A. J. (2004). Don't smile, your image has just been recorded on a camera-phone: The need for privacy in the public sphere. *University of Hawai'i Law Review*, *27*, 377-416.

Lund, B., & Agbaji, D. (2023). Information literacy, data literacy, privacy literacy, and ChatGPT: Technology literacies align with perspectives on emerging technology adoption within communities. (January 14, 2023). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4324580

Lutz, C., Schöttler, M., & Hoffmann, C. P. (2019). The privacy implications of social robots: Scoping review and expert interviews. *Mobile Media & Communication*, *7*(3), 412-434.

Marwick, A. E., & Boyd, D. (2014). Networked privacy: How teenagers negotiate context in social media. *New Media & Society*, *16*(7), 1051-1067.

Masur, P. K. (2018). *Situational privacy and self-disclosure: Communication processes in online environments*. Springer.

Masur, P. K., Epstein, D., Quinn, K., Wilhelm, C., Baruh, L., & Lutz, C. (2021). A comparative privacy research framework. *SocArXiv*. https://osf.io/preprints/socarxiv/fjqhs/

Masur, P. K., & Trepte, S. (2021). Transformative or not? How privacy violation experiences influence online privacy concerns and online information disclosure. *Human Communication Research*, *47*(1), 49-74.

Meier, Y., & Krämer, N. C. (2024). A longitudinal examination of Internet users' privacy protection behaviors in relation to their perceived collective value of privacy and individual privacy concerns. *New Media & Society*, *26*(10), 5942-5961.

McGill, T., & Thompson, N. (2017). Old risks, new challenges: Exploring differences in security between home computer and mobile device use. *Behavior & Information Technology*, *36*(11), 1111-1124.

Miller, R. A. (2017). "My voice is definitely strongest in online communities": Students using social media for queer and disability identity-making. *Journal of College Student Development*, *58*(4), 509-525.

Miller, R., & Melton, J. (2015). College students and risk-taking behaviour on Twitter versus Facebook. *Behaviour & Information Technology*, *34*(7), 678-684.

Müller, H., Gove, J. L., Webb, J. S., & Cheang, A. (2015, December). Understanding and comparing smartphone and tablet use: Insights from a large-scale diary study. In *Proceedings of the annual meeting of the Australian special interest group for computer human interaction* (pp. 427-436). ACM.

Murthy, D., Bowman, S., Gross, A. J., & McGarry, M. (2015). Do we tweet differently from our mobile devices? A study of language differences on mobile and web-based twitter platforms. *Journal of Communication*, *65*(5), 816-837.

Mylonas, A., Kastania, A., & Gritzalis, D. (2013). Delegate the smartphone user? Security awareness in smartphone platforms. *Computers & Security*, *34*, 47-66.

Napoli, P. M., & Obar, J. A. (2014). The emerging mobile Internet underclass: A critique of mobile Internet access. *The Information Society*, *30*(5), 323-334.

Neuendorf, K. A. (2017). *The content analysis guidebook* (2nd ed.). Sage.

Nissenbaum, H. F. (2010). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford Law Books.

O'Neil, D. (2001). Analysis of Internet users' level of online privacy concerns. *Social Science Computer Review*, *19*(1), 17-31.

Papacharissi, Z. (2010). *A private sphere: Democracy in a digital age.* Polity Press.

Pearce, K. E., Vitak, J., & Barta, K. (2018). Privacy at the margins| socially mediated visibility: Friendship and dissent in authoritarian Azerbaijan. *International Journal of Communication*, *12*, 22.

Pekárek, M., & Pötzsch, S. (2009). A comparison of privacy issues in collaborative workspaces and social networks. *Identity in the Information Society*, *2*, 81-93.

Petronio, S. (2002). *Boundaries of privacy: Dialectics of disclosure*. State University of New York Press.

Pew Research Center. (2021a, April 7). Mobile fact sheet. https://www.pewresearch.org/internet/fact-sheet/mobile/

Pew Research Center. (2021b, April 7). Social media fact sheet. https://www.pewresearch.org/internet/fact-sheet/social-media/

Pinch, T. & Bijker, W. (1987). The social construction of facts and artifacts: Or how the sociology of science and the sociology of technology might benefit each other. In, W. Bijker, T. Hughes, & T. Pinch (Eds.), *The social construction of technological systems: New directions in the sociology and history of technology* (pp. 17-50). The MIT Press.

Postman, N. (1996). *The end of education: Redefining the value of school*. Vintage.

Primault, V., Boutet, A., Mokhtar, S. B., & Brunie, L. (2018). The long road to computational location privacy: A survey. *IEEE Communications Surveys & Tutorials*, *21*(3), 2772-2793.

Quinn, K., Epstein, D., & Moon, B. (2019). We care about different things: Non-elite conceptualizations of social media privacy. *Social Media + Society*, *5*(3), 2056305119866008.

Quinn, S., & Oldmeadow, J. (2013). The martini effect and social networking sites: Early adolescents, mobile social networking and connectedness to friends. *Mobile Media & Communication*, *1*(2), 237-247.

Ravacizadeh, R., Sen, T., Kim, S. J., Meurisch, C., Keshavarz, H., Mühlhäuser, M., & Pazzani, M. (2019). Manifestation of virtual assistants and robots into daily life: Vision and

challenges. *CCF Transactions on pervasive computing and interaction*, *1*(3), 163-174. Springer.

Ribak, R. (2019). Translating privacy: Developer cultures in the global world of practice. *Information, Communication & Society*, *22*(6), 838-853.

Rice, R. E., & Hagen, I. (2010). Young adults' perpetual contact, social connectivity, and social control through the Internet and mobile phones. In C. Salmon (Ed.), *Communication yearbook, 34* (pp. 2-39). Routledge.

Rice, R. E., Hagen, I., & Zamanzadeh, N. (2018). Media mastery: Paradoxes in college students' use of computers and mobile phones. *American Behavioral Scientist*, *62*(9), 1229-1250.

Rice, R. E., & Hoffmann, Z. T. (2018). Attention in business press to the diffusion of attention technologies, 1990–2017. *International Journal of Communication*, *12*, 26. https://ijoc.org/index.php/ijoc/article/view/8250

Rice, R. E., Pearce, K. E., & Calderwood, K. J. (2022). W(h)ither the device divide? Changing relationships between personal computer or mobile device with online activities. *Mobile Media & Communication*, 11(3), 484-506.

Rice, R. E., Zamanzadeh, N. N., & Hagen, I. (2020). Chapter 9. Media mastery by college students: A typology and review. In S. J. Yates & R. E. Rice (Eds.), *The Oxford handbook of digital technology and society* (pp. 250-298). Oxford University Press.

Sannon, S., Stoll, B., DiFranzo, D., Jung, M. F., & Bazarova, N. N. (2020). "I just shared your responses" Extending communication privacy management theory to interactions with conversational agents. *Proceedings of the ACM on human-computer interaction*, *4*(GROUP) (pp. 1-18). ACM.

Schessler, M., Gerlitz, E., Häring, M., & Smith, M. (2021, October). Replication: Measuring user perceptions in smartphone security and privacy in Germany. In *European symposium on usable security 2021* (pp. 165-179). ACM.

Silver, L., Vogels, E. A., Mordecai, M., Cha, J., Rasmussen, R. & Rainie, L. (2019, Nov 20). *Mobile divides in emerging economies*. Pew Research Center Internet & Technology. https://www.pewresearch.org/internet/2019/11/20/mobile-divides-in-emerging-economies/

Suh, J. J., & Hargittai, E. (2015). Privacy management on Facebook: Do device type and location of posting matter? *Social Media + Society*, *1*(2), 2056305115612783.

Sundar, S. S., Cho, E., & Wang, J. (2018). Interacting with mobile media. In K. Norman & J. Kirakowski (Eds.), *The Wiley handbook of human–computer interaction* (pp. 615-639). John Wiley & Sons.

Sundar, S. S., Kim, J., Rosson, M. B., & Molina, M. D. (2020, April). Online privacy heuristics that predict information disclosure. In *Proceedings of the 2020 CHI conference on human factors in computing systems* (pp. 1-12). ACM.

Taddei, S., & Contena, B. (2013). Privacy, trust and control. Which relationships with online self-disclosure? *Computers in Human Behavior*, *29*(3), 821-826.

Taylor, B. (2014, Oct. 10). Phablet vs. mini-tablet: The big choice between two smallish devices. *PCWorld*. https://www.pcworld.com/article/435752/phablet-vs-mini-tablet-the-big-choice-between-two-smallish-devices.html

Thompson, N., McGill, T. J., & Wang, X. (2017). "Security begins at home": Determinants of home computer and mobile device security behavior. *Computers & Security, 70*, 376-391.

Trepte, S. (2021). The social media privacy model: Privacy and communication in the light of social media affordances. *Communication Theory*, *31*(4), 549-570.

Tsay-Vogel, M., Shanahan, J., & Signorielli, N. (2018). Social media cultivating perceptions of privacy: A 5-year analysis of privacy attitudes and self-disclosure behaviors among Facebook users. *New Media & Society*, *20*(1), 141-161.

van Ooijen, I., Segijn, C. M., & Opree, S. J. 2024. "Privacy cynicism and its role in privacy decision-making." *Communication Research 51:* 2 146–177.

Vincent, D. (2016). *Privacy: A short history*. John Wiley & Sons.

Vincent, J. (2013). Is the mobile phone a personalized social robot. *Intervalla*, *1*(1), 60-70.

Vitak, J. (2012). The impact of context collapse and privacy on social network site disclosures. *Journal of Broadcasting & Electronic Media*, *56*(4), 451-470.

Walker, A. M., & Hargittai, E. (2021). Drills and spills: Developing skills to protect ones privacy online. In *Handbook of Digital Inequality,* edited by E. Hargittai, 358–372. Northampton, MA Edward Elgar Publishing.

Walsh, S. P., White, K. M., & Young, R. M. (2009). The phone connection: A qualitative exploration of how belongingness and social identification relate to mobile phone use amongst Australian youth. *Journal of Community & Applied Social Psychology*, *19*(3), 225-240.

Wang, L. H., & Metzger, M. J. (2023). The role of culture in privacy management on social media among emerging adult children and their parents. *Journal of International and Intercultural Communication*, *16*(2), 162-190.

Woo, J. (2016). The right not to be identified: privacy and anonymity in the interactive media environment. *New Media & Society*, *8*(6), 949-967.

Wu, P. F., Vitak, J., & Zimmer, M. T. (2019). A contextual approach to information privacy research. *Journal of the Association for Information Science and Technology*, *71*(4), 485-490.

Wu, X., Duan, R., & Ni, J. (2024). Unveiling security, privacy, and ethical concerns of ChatGPT. *Journal of Information and Intelligence*, *2*(2), 102-115.

Youker, B. W., Zielinski, A., Hunter, O. C., & Bayer, N. (2016). Who needs goals? A case study of goal-free evaluation. *Journal of MultiDisciplinary Evaluation, 12(*27), 27-43.

Zamanzadeh, N. N., & Rice, R. E. (2021). A theory of media multitasking intensity. *Journal of Media Psychology: Theories, Methods, and Applications*, *33*(4), 226-239.

Footnotes

[1]We note that online and offline privacy phenomena are often interrelated. Online privacy invasions can create consequences for offline privacy, behaviors, and psychological states (Durnell et al., 2020). For example, Ji and Lieber (2010) found that survey respondents were concerned that personally identifiable information disclosed online could be transferred or inadvertently exposed in offline contexts. One's privacy during digital media use can be compromised in the physical world through overhearing or observation by others; conversely, one's physical privacy can be invaded by others' capturing actions by device cameras or recording (Lum, 2004), leading to social embarrassment, identity theft, cyberbullying, blackmailing, etc. More subtly, digital device technology or app software can identify and track the location of the user (e.g., travel, real-time directions, nearby venues, disease outbreaks, local weather, emergency warnings, personal eHealth), creating what Primault et al. (2018) call a "mobility trace." Online information about offline physical location can be used by many parties with or without consent, constitute potential privacy threats, and can be used to identify or infer other personal information such as travel habits, religion, celebrity travel, and health visits.

[2]We use the term "mastery" for both users and media for three reasons. First, the application of the same term to both emphasizes reciprocality and mutual shaping among actors, structure, and technology highlighted in actor-network theory, adaptive structuration, and social construction of technology theories (DeSanctis & Poole, 1994; Jones & Karsten, 2008; Latour, 2007; Pinch & Bijker, 1987). Rice et al. (2020, pp. 253-255) summarize a wide range of related concepts and their overlaps with, foundations for, and differences from, the media mastery framework. The framework considers individuals and their social relations, as well as more general economic and technological infrastructure forces. According to Rice et al. (2020), "media mastery does not explicitly consider the origin, development, and design of technological innovations; rather, it is about the construction and shaping by (mastering), and of (being mastered), individuals in their social settings of the meanings, choices, uses, and consequences of, and by, new media already available to them" (p. 255).

Second, the term "mastery" serves as a metaphor for a wide variety of influences, limitations, and forms of control. These include both how users, across varying contexts, attempt to manage or master the use, balance, and outcomes of one or more media, and "the ways in and extent to which these media master us—as our activities, concerns, and relationships are being shaped through, facilitated and constrained by, and dependent upon, the use of these media" (Rice et al., 2020, p. 252). This is not a new concept. In the context of both television and computers, Postman (1996) argued that learning how media use us is more important than learning how to use media. Best and Tozer (2013), in their thematic analysis of interviews with 38 users of digital technology between 2005 and 2007, emphasized the potential reciprocality of control. Factors such as programming code, technical and interface design, regulations, and available features "subject the user to varying degrees of control, from overt control to attempts to accommodate for perceived user ignorance or ineptitude" (Best & Tozer, 2012, p. 402). They refer to studies finding that users may consider themselves in control (even if not), while others finding technologies to be in a dominant role. DeVito (2017) concluded that many negative effects of digital media use (in particular, pre-selected and filtered Facebook news) are primarily related to when the user is not in control of, including not being aware of, those designs, uses, or effects.

Other examples of media constraining, shaping, or "mastering" users include biased emphases in platform algorithms, such as YouTube's presentation of videos (Bishop, 2018). A

more common example of media mastering users is the pervasive dependency on smartphones: "A study of 2,097 American smartphone users reported that 60% of users cannot go 1 hr without checking their smartphones with 54% reporting they checked their smartphones while lying in bed, 39% checked their smartphone while using the bathroom, and 30% checked it during a meal with others (Lookout Mobile Security, 2012)" (Hussain et al., 2017, p. 378). Problematic, harmful, or addictive video game playing is a recurring concern as well (King & Delfabbro, 2020). We do not claim, from a denotative interpretation of the term "mastery", that digital media have conscious agency or full control over human behavior (although recent developments in artificial intelligence may question both of those points), but rather that, depending on their awareness, knowledge, and expertise, and the medium's features and constraints, users may have more or less control over some aspects and effects of those media. Thus users need to better understand how to shift the balance from being mastered by media to being masters of media.

Third, considering the possibility of, and challenges from, both kinds of mastery also implies that digital media use has both positive and negative implications, often simultaneously (see Katz & Rice, 2002). This is a pervasive and fundamental perspective of media effects and communication technology literature (for example, mobile phone use as distraction, David et al., 2015; association of social media use with addiction and life satisfaction, Hawi & Samaha, 2017; Internet as neither utopian nor dystopian but rather syntopian, Katz & Rice, 2002).

[3]"Portability" is applicable to laptop and tablet computers too, because they can be carried to use in different locations. But this is not the same as being continuously "mobile" like mobile phones are, easy to carry, and ready to use in nearly any situation or location; few people text or talk through their tablet while walking, though we note that even in 2014 some large phones ("phablets") were nearing the size of minitablets (Taylor, 2014). Further, the kinds of programs and connections available via computers (laptops, desktops, tablets) differ somewhat from those via mobile phones. For example, email use on a laptop requires logging in and having an internet connection, while texting on mobile phones is typically quickly available and can be performed while physically moving. Indeed, Müller et al. (2015), in a large-scale diary study, demonstrated that smartphones were primarily used for communication needs that have important privacy implications, whereas tablets were used most frequently for consumption and entertainment activities that are similar to those provided by desktop computers and television. In terms of device use locations, smartphones were used more outside of home, demonstrating their mobility, whereas the vast majority of tablet use occurred at home, with some outside use at work and school. Other research has also found that users' smartphone use was more associated with the location or situation than tablet use (IAB, ABI Research, 2012). These findings provide strong supporting evidence for the grouping of mobile phones vs. desktop, laptop, and tablet computers.

Table 1
SubComponents, Code Definition, and Examples of Privacy-related Boundary Codes for Computers and Mobile Phones

Boundary Sub-Component	Code Definition	Computer	Mobile Phone	Example Privacy Literature Reference	Illustrative Quote
Anonymity	remaining unidentified; lacking personal features	being anonymous when using public computers	using pseudonyms on mobile apps	Trepte, 2021; Woo, 2016	"and stuff like that. Do you know what—it's a site where you anonymously ask questions and people can be brutal on it." (FG5, 2016, PC, L367)
Audience	observers, intended or unintended viewers or consumers of personal information	Internet browser and online shopping websites tracking browsing activities for personalized recommendation	family, friends and strangers seeing social media posts and direct or indirect messaging	Bazarova & Masur, 2021; Masur & Trepte, 2021	"Oh, did you see what he said about her? Oh, did you see that Snapchat where he was doing this? Stuff like that where maybe you don't see it in person, but there's some sort of visual or documentation of it. Then not only that, but it can also be sent to many, many other people." (FG31 2016, PC, L382)
Context collapse	the capacity for many social groups to overlap online	personal information exposed on multiple collaborative workspaces (e.g., Google docs, emails)	social media posts being read by people from different groups (e.g., through hashtags)	Papacharissi, 2010; Vitak, 2012	"It's easy when you talk to a lot of people, the same with Facebook a lot of people are making specific groups, just to communicate with a bunch of people at once, which is

					convenient, and it's easy to organize, because everyone is talking in one place. It's not he said, she said." (FG1, 2016, MP, L169)
Parental access	parental access to information about their children	parents checking on children's computer devices	parents checking on children's mobile phones	Kanter et al., 2012; Wang & Metzger, 2023	"but when I was living with my parents it [mobile phone] provided me with, like, when a lot of like, well obviously like independence but like, like, ways to keep secrets from your parents, like, they weren't listening to your conversations, you know what I mean, they didn't have to say, like "Oh, who were you talking to on the phone?" They don't know, like, who exactly you're talking to." (FG5, 2006, MP, L1166)
Privacy management	the desire and the (in)ability for a person to *seclude* their personal information from other entities	using proxy server, anti-tracking software, or browser plug-in for privacy	creating private disclosure list, turning off location tracking setting, asking mobile apps not to track personal information	Epstein & Quinn, 2020; Hoffmann et al., 2016	"I like to press the little button at the top, um, the "I" so if I'm like talking to like two people, and those are the only people I want to talk to, I'll click to I and see, you can't, like other people can't like see you but you can still be online." (FG1, 2006, PC, L177)

Public	personal information that is open to general groups of people	creating a professional public website	creating a social media account that's open to the public	Marwick & Boyd, 2014; Papacharissi, 2009	"It's nice to always have access to everything. Everything's very immediate. You can look up information in no time. You can look up someone's profile. If you're talking to someone and you're talking about another person they're like, oh, I don't know who that is. You pull up a picture in two seconds, and they're like, oh, I know who that person is." (FG3, 2016, PC, L463)
Safety	the (in)ability to be protected from danger	using antivirus app, ad block configuration, duo login authentication	using data erasing function after phone lost, app/file lock and hiding function, fingerprint/face ID authentication	Dodel & Mesch, 2018; Li et al., 2018	"the only like, the biggest problem is like, the whole like credit card fraud and everything and that's pretty secure unless you go into like a really crappy web site that you've never heard of or like…" (FG5, 2006, PC, L611)
Self-broadcasting	publicly and continuously sharing of manifestations of personal information to a certain group of people	posting web tweets	posting mobile tweets	Bazarova & Choi, 2014	"Just posting about what you're doing so that others can see your activities, Snapchat." (FG5, 2016, MP, L567)
Surveillance	other people or institutions actively	Internet browser and online shopping	social media stalking; mobile	Büchi et al., 2022;	"My, uh, my roommates are kind of like Internet

	monitoring or observing or obtaining personal information without conscious permission or awareness	websites tracking browsing activities	apps tracking location	Krasnova et al., 2009	stalkers,...and then they'll like look at their pictures, and like, find out if they're dating people,...but then they have this tracker thing, that whoever looks at your pictures it'll tell you like, who looked at them, so it's kind of weird, like just how so many people…" (FG4, 2006, PC, L430)
Trust	willingness or tendency to rely on another	using online banking as a result of trusting the web platform	disclose personal information via direct messaging as a result of trusting the communication partner	Joinson et al., 2010; Trepte, 2021	"I have a hard time trusting information that I find until it's like repeated like a bunch, you know what I mean, like you were saying oh if I have a question about anything, I can look it up, I kind of look it up, like for me, I have to look it up on like six different web sites, otherwise I wouldn't trust it." (FG5, 2006, PC, L826)
Visibility - Transparency	capacity for aspects and/or manifestations of personal information to be visible to others, either intentionally or unintentionally	posting comments on online forums that are visible to other members	setting social media posts to be only visible to certain groups of followers	Pearce et al., 2018	"Yeah, it's almost like they're there because you're not saying, 'Oh, this is what I'm doing, this is what I did today.' You're just like—you show them. That's what my boyfriend and I do. We just send each other pictures, so we know what we're doing." (FG5, 2016, MP, L741)

Vulnerability	perceptions and/or capacity of being wounded or attacked; a weakness that normally manifests in previous negative experiences	being attacked by computer viruses	smart phone lost, stolen, or damaged	Van Ooijen et al., 2022	"I have all my phone numbers written down because twice I've lost all my phone numbers, it's just, when my phone's broke, and then, like I couldn't see the screen, and couldn't get any numbers, and then my phone got stolen, so I had to write all of my numbers down, it's such a pain." (FG1, 2006, MP, L919)
Watchfulness	an alertness; an awareness of the dynamics of information disclosure and collection online; attending to information with caution	avoiding clicking fishing links/icons, forbidding pop-up window	ignoring fraud/scam messages	Walker & Hargittai, 2021	"That relates to what you were just talking about – how over the past 15 or 20 years or so, privacy policies, how they've kind of evolved, and how social media and wireless networks have information so readily available, and how even the government uses it against us. It uses the technology we have these days against us, which is kind of scary." (FG1, 2016, PC, L100)

Note. For each illustrative quote, identifiers are focus group number, year, device, and transcript line.

Table 2

Internet, Computer, and Mobile Phone Adoption, 2006 & 2016

Digital Device	**2006**	**2016**
Internet access [1]	71%	84%
Desktop/laptop [2]	74%	74%
Tablet [2]	2010: 3%	51%
Mobile phone (either non-smart or smart) [2] *	73%	91%
Smart mobile phone [3]	3%	81% (72% [2])

[1] https://www.pewresearch.org/internet/2015/06/26/americans-internet-access-2000-2015/

[2] https://www.pewresearch.org/internet/fact-sheet/mobile/; https://www.pewresearch.org/fact-tank/2017/01/12/evolution-of-technology/

[3] https://www.comscore.com/Insights/Blog/US-Smartphone-Penetration-Surpassed-80-Percent-in-2016

[4] https://www.zippia.com/advice/us-smartphone-industry-statistics/

* By 2022, only 12% owned a non-smart mobile phone [4]

Table 3

Questions Used to Generate Focus Group Discussion

1. On a normal day, for what purposes do you use the …?
2. Follow up questions (if the group participants do not talk about this): For what school-related tasks do you use the … ?
3. What personal or social purposes do you use the … for?
4. Do you feel that you achieve what you would like to with your … ?
5. Please describe negative experiences you may have had with your ….
6. Please describe situations where you really enjoy using the ….
7. What would your life look like if you did not have a …?

Note: Each set of seven questions was first asked for personal computers and laptops (tablets were added in 2016), and then asked for mobile phones.

Table 4
Agreement and Reliability of Focus Group Codes, Computer and Mobile Phone Comments Combined, 2006, 2016, and Years Combined

	2006		2016		2006 & 2016	
Code	**% Agree**	**Cohen's Kappa**	**% Agree**	**Cohen's Kappa**	**% Agree**	**Cohen's Kappa**
Anonymity	99.9	.749	99.9	.857	99.9	.818
Audience	99.6	.949	98.5	.781	99.0	.852
Context collapse	100	1.00	99.9	.800	99.9	.800
Parental access	100	1.00	100	1.00	100	1.00
Privacy	99.7	.874	99.4	.904	99.6	.829
Public	99.6	.855	100	1.00	99.8	.899
Safety	99.4	.815	99.9	.963	99.7	.872
Self-broadcasting	99.8	.879	99.6	.900	99.7	.894
Surveillance	100	1.00	99.9	.947	100	.960
Trust	100	1.00	100	1.00	100	1.00
Visibility – transparency	99.6	.935	98.5	.772	98.9	.839
Vulnerability	99.9	.952	99.9	.928	99.9	.938
Watchfulness	100	1.00	99.9	.941	100	.960

Table 5
Focus Group Code Descriptives, across Devices and Years

Boundary Code	M	SD
Anonymity	.0033	.0570
Audience	.0355	.1852
Context	.0012	.0344
Parental	.0003	.0172
Privacy	.0127	.1122
Public	.0095	.0969
Safety	.0110	.1041
Self-broadcasting	.0136	.1160
Surveillance	.0036	.0595
Trust	.0006	.0243
Visibility – Transparency	.0350	.1837
Vulnerability	.0071	.0840
Watchfulness	.0039	.0619

Note: N = 3376; values are percentages, i.e., .33% and 3.55%

Table 6
Multivariate Analysis of Variance in Code Percentages, by Devices and Years

	Descriptive Statistics								Tests of Between-Subjects Effects							
	PC 2006		MP 2006		PC 2016		MP 2016		Intercept		Year		Device		Year * Device	
Boundary Code	M	SD	M	SD	M	SD	M	SD	*F*	η_p^2	*F*	η_p^2	*F*	η_p^2	*F*	η_p^2
Anonymity	.003	.050	.003	.050	.005	.059	.001	.033	11.2 ***	.003	.17	.000	.10	.000	2.4	.001
Audience	.057	.231	.007	.082	.030	.171	.042	.201	109.0 ***	.031	.46	.000	8.4 **	.002	23.0 ***	.007
Context	.000	.000	.000	.000	.001	.031	.003	.056	2.9	.001	2.9	.001	.83	.000	.83	.000
Parental	.000	.000	.002	.041	.000	.000	.000	.000	1.9	.001	1.9	.001	1.9	.001	1.9	.001
Privacy	.015	.122	.005	.071	.008	.088	.021	.144	38.6 ***	.009	1.2	.000	.17	.000	8/9 **	.003
Public	.029	.168	.000	.000	.008	.088	.001	.033	31.0 ***	.009	8.89 **	.003	27.7 ***	.008	10.8 **	.003
Safety	.020	.151	.012	.108	.010	.098	.004	.065	39.0 ***	.011	6.0 *	.002	3.6	.001	.17	.000
Self-broadcasting	.015	.122	.000	.000	.016	.127	.018	.133	36.9 ***	.011	5.6 *	.002	2.8	.001	4.2 *	.001
Surveillance	.004	.061	.000	.000	.002	.044	.007	.086	9.8 **	.003	1.8	.001	.16	.000	4.8 *	.002

Trust	.001	.036	.002	.041	.000	.000	.000	.000	2.9	.001	2.9	.001	.06	.000	.06	.000
Visibility – Transparency	.056	.229	.007	.082	.318	.173	.04	.196	106.8 ***	.031	.50	.000	9.4 **	.003	20.3 ***	.006
Vulnerability	.008	.087	.007	.082	.007	.084	.007	.084	23.0 ***	.007	.0	.000	.00	.000	.07	.000
Watchfulness	.003	.050	.003	.058	.005	.069	.004	.062	11.7 ***	.003	.54	.000	.00	.000	.11	.000

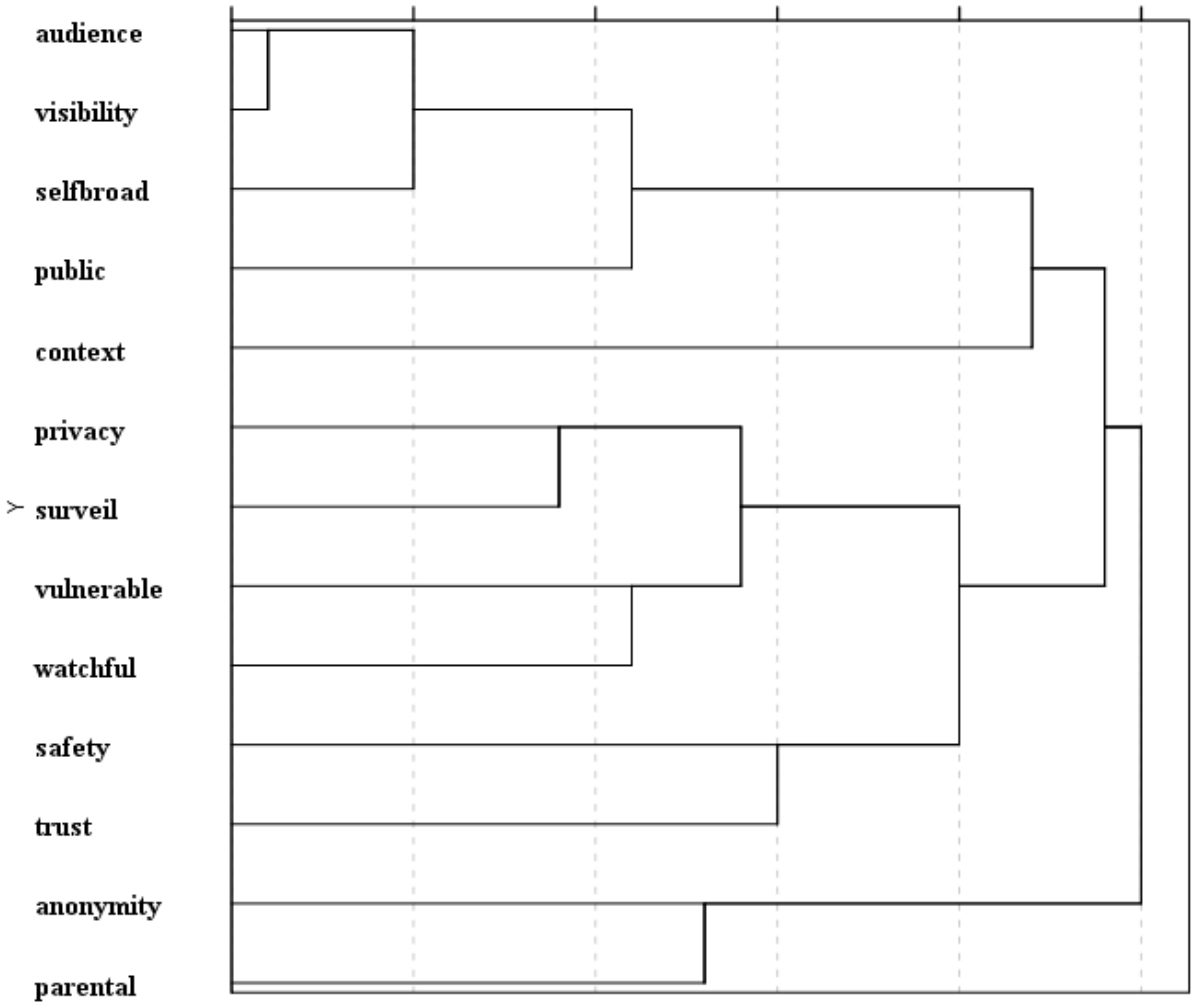
	Multivariate Tests		
Intercept & Factors	Wilks' Lambda	F (13,3360)	η_p^2
Intercept	.958	11.33 ***	.042
Year	.969	2.80 ***	.011
Device	.988	3.24 ***	.012
Year*Device	.989	2.94 ***	.011

* $p < .05$, ** $p < .01$, *** $p < .001$

N: PC 2006 = 794; MP 2006 = 599; PC 2016 = 1036; MP 2016 = 947

Figure 1

Privacy Phenomena Themes: Hierarchical Clustering of Privacy-Related Boundary Codes across Focus Groups (Dendrogram)



Note: Hierarchical clustering based on Pearson correlation coefficient similarities, and average linkage between groups method (SPSS).