International Journal of Communication 16(2022), 4779–4800 1932–8036/20220005

Older Adults and "the Biggest Lie on the Internet": From Ignoring Social Media Policies to the Privacy Paradox

JONATHAN A. OBAR
York University, Canada

ANNE OELDORF-HIRSCH[1]
University of Connecticut, USA

Older adults (50+) may self-report online privacy concerns and claims of protective behaviors, but what happens when actual privacy behaviors are assessed? An experimental survey (*N* = 500) evaluated older adult engagement with the online consent process for a fictitious social networking service called NameDrop. Results demonstrate 77.6% chose the clickwrap, agreeing to the privacy policy (PP) without accessing it. For those accessing policies, average PP reading time was about 70 seconds, 81.4 seconds for terms of service (TOS). Participants convey an interest in protections but find policies long, complicated, and impeding a desire to join services quickly. Results also suggest two examples of the privacy paradox: for clickwrap use and for policy reading time. To address these ignoring behaviors, digital service providers should offer support by addressing problematic designs like clickwraps and long/complicated policies. Findings emphasize implications as 91.4% of participants accepted the NameDrop PP, which included data collection/sharing "gotcha" clauses, while 83.4% accepted the TOS, including an extreme clause requiring users to provide a kidney or other "redundant organ" in exchange for service.

Keywords: privacy, online consent, social media, privacy policy, terms of service, clickwrap

"I agree to the terms and conditions" is said to be "the biggest lie on the Internet" (Lannerö, 2012; Obar & Oeldorf-Hirsch, 2020; Terms of Service; Didn't Read, 2022). This anecdotal assertion and Internet meme suggests online interactions are defined repeatedly by a lie. When selecting "I agree" to terms of service (TOS), privacy, and other digital service policies, the suggestion is that people lie by falsely indicating

Jonathan A. Obar: jaobar@yorku.ca
Anne Oeldorf-Hirsch: anne.oeldorf-hirsch@uconn.edu
Date submitted: 2021-01-05

[1] Acknowledgements: Thank you to Valeta Wensloff for the graphic design, Michael Ross for help with the research design, and Andrew Hatelt for the research assistance. Thank you to the University of Connecticut and to York University for funding this project.

both awareness of policy details and understanding of agreement implications. The enormity of the lie is because of the omnipresence of online consent mechanisms common to digital services.

Research in this area emphasizes the challenges of ensuring meaningful consent online (see Feng, Yao, & Sadeh, 2021; Solove, 2012). Concerns are often linked to a policy framework called the Fair Information Practice Principles integral to privacy law and regulation around the world (Cate, 2016; Hartzog, 2016). Critics suggest that the notice policy component of the framework, requiring digital service providers to disclose information about data practices to data subjects, does not ensure disclosures (i.e., privacy and TOS policies) are accessible or useful (Ben-Shahar & Schneider, 2011; Nissenbaum, 2011). Instead, digital service providers maintain lackluster data privacy transparency via long and complicated privacy and TOS policies that do not engage individuals in vital information protections or help them understand the implications of agreement (McDonald & Cranor, 2008; Obar, 2022; Obar & Oeldorf-Hirsch, 2018; Reidenberg et al., 2015).

Another section of the literature questions the perspectives and behaviors of individuals and their relationship to the delivery of privacy protections (see Acquisti, Brandimarte, & Loewenstein, 2015). The current study focuses primarily on this area of inquiry but questions the extent to which the TOS and privacy policies of digital service providers contribute to privacy deliverables. Indeed, it is argued that a primary flaw of the data privacy transparency efforts of digital service providers is the impossible burden placed on the individual (McDonald & Cranor, 2008; Solove, 2012). That burden is evidenced by the individual's concurrent position at the center of a swirling and ubiquitous big data universe as both perpetual data subject and overwhelmed privacy savior. Lacking is extensive empirical evidence explaining the relationship between this burden and user behavior.

Studies of older adults engaging with digital technologies are needed (Kadylak & Cotton, 2020; Yuan, Hussain, Hales, & Cotton, 2016). This research gap contributes to fundamental privacy questions continuing without answers. For example, older adults self-report that they have concerns about online privacy (e.g., Xie, Watkins, Golbeck, & Huang, 2012; Yuan et al., 2016) and that they are willing to act on those concerns (e.g., Auxier et al., 2019). This suggests that older adults might not demonstrate the privacy paradox or a distinction between what individuals say about privacy concerns and how they respond (Nissenbaum, 2011; Norberg, Horne, & Horne, 2007). If studies of older adults do not demonstrate the privacy paradox, it would suggest the need for a clearer understanding of why, especially as there are considerable concerns about the state of privacy-related resignation and apathy (Draper & Turow, 2019; Hargittai & Marwick, 2016).

Returning to the study of "the biggest lie on the Internet," the extent to which individuals lie is one question, and why they lie is another—both questions are addressed by this study. How people lie when engaging with online consent materials is a different question. One way is via the clickwrap (see Figure 1), "a digital prompt that enables the user to provide or withhold their consent to a policy or set of policies by clicking a button, checking a box, […] suggesting "I agree" or "I don't agree" (Obar & Oeldorf-Hirsch, 2018, p. 3).

For social networking services[2] (SNS) in particular, clickwraps often appear when individuals are signing up for services and when policies change. Clickwraps often include an appealing agree or join button, above or below links to policies (Obar & Magalashvili, 2021). Accompanying text can suggest that by clicking the button, individuals agree to policies accessible via the links. How people lie with a clickwrap is that they click the agree button without first clicking on the policy links, communicating to the service provider that they have accessed, engaged with, and understood the policies, when they have not.

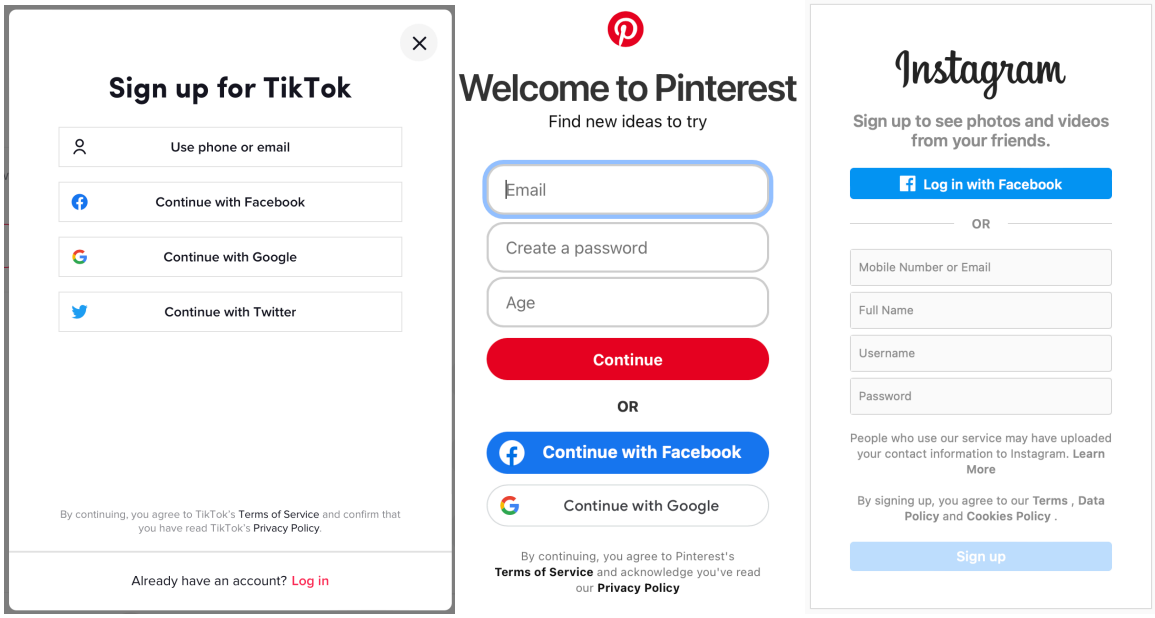

Figure 1. Clickwraps from TikTok, Pinterest, and Instagram.

While previous research does investigate how older adults feel about online privacy and whether they are likely to engage in protections, few studies move beyond self-report assessments or question specific behaviors in the online consent context. This experimental survey attempts to address these research gaps by assessing the extent to which older adults (age 50+) ignore consent processes for a fictitious SNS, and if so, why. It compares results with those of a complementary self-report assessment (Oeldorf-Hirsch & Obar, 2019) to address any distinctions between self-report and actual behaviors.

Older Adults and Online Privacy

Older adults do appear to care about their privacy and reputation online. Hoofnagle, King, Li, and Turow (2010) found that 60% of those 55–64 and 67% of those 65+ were "more concerned about privacy issues on the Internet" (p. 15) than they were five years prior. Only about 5% of those 55+ were less

[2] As we refer to both the literatures utilizing the terms "social media" and "social networking service," we will be utilizing the terms interchangeably.

concerned. Gibson and colleagues' (2010) study of 63 86-year-olds with Internet access but without SNS, suggested older adults were "concerned at the idea of having to divulge their full details to new online groups" (p. 192). Xie and colleagues (2012) found that older adults felt "privacy was the primary concern and the key perceptual barrier to adoption" (p. 11). Similarly, Yuan and colleagues (2016) suggested "the way older adults utilize Facebook is very different from other generational groups [. . .] explained by their level of trust with the Internet and the privacy concerns" (p. 171). Even by 2019, older adults felt they had less control over online information, as compared to younger adults (Auxier et al., 2019).

The literature also suggests that older adults are interested in privacy protective behaviors. Pew found 56% of participants 50–64 and 41% of those 65+ said they manage SNS profiles by deleting people, while 22% of those 50–64 and 16% of those 65+ said they have removed their names from tagged photos (Madden, 2012). Pew found older adults also said they engage in anonymity-promoting activities, with 56% of those 50–64 and 42% of those 65+ suggesting they clear their browser histories and cookies, while about a third said they have refused to use a site where a real name is requested (Rainie, Kiesler, Kang, & Madden, 2013). Indeed, research repeatedly suggests older adults are concerned about privacy online and are interested in privacy protective behaviors, adding that those especially concerned appear more likely to engage in privacy protective behaviors (Gupta & Chennamaneni, 2018; Kezer, Sevi, Cemalcilar, & Baruh, 2016). For instance, another Pew report suggests that those more than 50 are more likely to claim that they read privacy policies than younger Internet users (Auxier et al., 2019).

If older adults are going to engage in privacy protective behaviors, it appears they will do so when they potentially mitigate concerning relationships with service providers—referred to as institutional or vertical privacy concern (Raynes-Goldie, 2010). Another form of privacy concern is social/horizontal privacy, which refers to privacy concerns associated with interpersonal relationships (Raynes-Goldie, 2010). A study of older adults in Canada, where 45% of the participants had at least one SNS account, noted:

> We found that older adult social media users and non-users shared similar privacy concerns, the most *frequently mentioned* being a concern for unauthorized access to personal information, and information misuse [. . .] (including misuse) by organizations, corporations, and governments. [. . .] The concern of misuse of personal information reflects a concern for institutional rather than social privacy. (Quan-Haase & Elueze, 2018, pp. 156–157)

Thus, the literature suggests that older adults: (a) are concerned about online privacy, (b) are interested in privacy protective behaviors, and (c) are nuanced in their privacy concerns, potentially biased toward institutional privacy concerns associated with service provider relationships. As a result, it seems plausible that older adults would both express and act upon their privacy concerns when prompted by an institutional modality—the privacy or TOS policy.

The Privacy Paradox

The privacy paradox is understood as differences between what individuals say about their privacy concerns and what they actually do (Nissenbaum, 2011; Norberg et al., 2007). This original paradox—where

individuals disclose more than they claim to—is now understood to be a function of attitudes toward information disclosure, which inform context-dependent negotiations of risks and benefits (Barth & de Jong, 2017). Indeed, subsequent research does move beyond the dichotomy addressing distinctions between what people say and do and explains how differences in perceptions, opportunities, and abilities influence expression and action (Kokolakis, 2017). It is suggested that age, for instance, has a negative relationship with how much information people will disclose, particularly sensitive information (Li, Lin, & Wang, 2015).

A meta-analysis seemingly counters the suggestion of a privacy paradox (Baruh, Secinti, & Cemalcilar, 2017) indicating that higher privacy concerns are associated with reduced use of online services, less sharing of personal information, and greater use of privacy protective measures. One alternative to the paradox is the suggestion that privacy behaviors may be explained by "privacy calculus" (Dinev et al., 2006), in which individuals weigh the costs and benefits of disclosing information online before deciding how to proceed. This suggests that privacy behaviors may be linked to perceptions of privacy trade-offs (Wottrich, van Reijmersdal, & Smit, 2018).

While we acknowledge these advances, this study returns to the simplified say/do dichotomy in an attempt to address limitations in the literature. A review of the privacy paradox literature suggests that "future studies should use evidence of actual behaviour rather than self-reported behaviour" (Kokolakis, 2017, p. 122) and "most experiments [. . .] fail to recreate a realistic context" (p. 131). Another systematic review (Gerber, Gerber, & Volkamer, 2018) similarly notes that although there is inconsistent evidence for the privacy paradox, most research has relied on behavioral intentions rather than actual behavior. Challenges associated with remembering ignoring behaviors from years ago, coupled with normative response biases, present a troubling scenario for accurate self-reporting. Perhaps the strategy of comparing self-report engagement with consent materials (i.e., say) and empirical evidence of actual engagement (i.e., do), within the same study may contribute to a clearer sense of the privacy paradox. Thus, returning to the framework with behavioral evidence may be crucial to accurate assessment.

Ignoring Digital Media Policies

Acknowledging the self-report challenge (Jensen, Potts, & Jensen, 2005), studies identify various policy reading behaviors via self-report. An early study noted 83.7% of 2,000+ participants claimed they read policies, while 17.3% claimed they do not (Milne & Culnan, 2004). Hoofnagle and colleagues (2010) found more than half of those 55+ said they read privacy policies "often" or "sometimes," while a more recent report suggested 65% of individuals more than 50 said they read them (Auxier et al., 2019).

Studies have tracked users directly to determine policy reading behaviors. Groom and Calo (2011) found that of 120 participants, zero clicked a policy link associated with a fake search engine. A study of engagement with software providers in 2007 revealed that most were not accessing or reading policies, suggesting less than 0.2% of 48,000+ users visited TOS. For those who did, average time on the page was around 30 seconds (Bakos, Marotta-Wurgler, & Trossen, 2014). A second analysis found clickwraps did not enhance policy engagement (Marotta-Wurgler & Chen, 2012). A study conducted in 2013 organized participants into two groups, one presented with a policy statement and a checkbox for agreeing, and one with only the checkbox and an accompanying link to the statement (i.e., a clickwrap). For the clickwrap

group, almost 80% of 64 participants selected the checkbox without clicking the link. Participants provided with the statement (451 words) directly spent more time looking at it—close to 1 minute (Steinfeld, 2016).

The current study attempts to add to this literature by expanding on an earlier study of undergraduates (N = 543) and their engagement with consent materials for a fictitious SNS called NameDrop (Obar & Oeldorf-Hirsch, 2020). Participants in the previous study were presented with an image of NameDrop's front page and provided the opportunity to select a clickwrap to skip and agree to the privacy policy (PP). Seventy-four percent of the participants did. Of those who accessed the PP, which should have taken about 30 minutes to read, the average reading time was 76 seconds, with a 14-second median. All participants accessed the TOS requiring 16 minutes to read. Average reading time was 51 seconds with a 14-second median. The required reading times were calculated using an average reading speed assessment for adults with a grade 12 or college education of 250 words per minute (Taylor, 1965). To reveal implications, two "gotcha clauses" were added to the TOS. The first said NameDrop would share data with the U.S. National Security Agency (NSA) and data brokers. The second, more extreme, was a first-born clause, suggesting that users would have to provide their child as payment for service. Ninety-seven percent of participants agreed to the PP and 93% to the TOS, with 98% missing the gotcha clauses. Participants repeatedly praised the clickwrap for helping to expedite the consent process that was perceived to be a nuisance and tangential to desired SNS activity. Indeed, participants were clear that they aimed to "pursue the ends of digital production, without being inhibited by the means" (Obar & Oeldorf-Hirsch, 2020, p. 128).

In what follows, a similar experimental survey is conducted, directed by the following research questions:

RQ1: To what extent will older adults (50+ years) ignore NameDrop's privacy and TOS policies?

RQ2: To what extent will older adults miss NameDrop's "gotcha clauses"?

Method

The current study is part of a larger online survey hosted on Qualtrics in June 2017. The full survey had two parts: (1) an experimental survey with quantitative and qualitative measures, assessing participant engagement with online consent materials (i.e., clickwrap, privacy, and TOS policies) for a fictitious SNS, and (2) a set of self-report survey measures about digital media policy reading behavior. This study addresses (1), with the results of (2) addressed in a separate analysis (Oeldorf-Hirsch & Obar, 2019). Average survey-taking time for the entire survey was 23 minutes (SD = 15.32, range = 4–117 minutes).

For the experimental survey, the researchers amended an image from Obar and Oeldorf-Hirsch (2020) of the front page for the fictitious SNS "NameDrop" (see Figure 2), designed to appear as a competitor of LinkedIn. The original version had images of younger individuals. These were replaced with images of older adults.

Sample

Participants (N = 500) were recruited and paid through a Qualtrics online survey panel, which claims to provide a representative sample from the United States—in this case, of participants aged 50 and older. Participants identified 74% females and 26% males. The average age was 58.7 years old (SD = 7.16), and the range was 50–86 years. Eighty percent reported as White or Caucasian, 12% Black or African American, 2% Hispanic or Latino, 2% Indigenous, 2% mixed ethnicity, 1% Asian, 1% other ethnicity, and 1% did not identify.

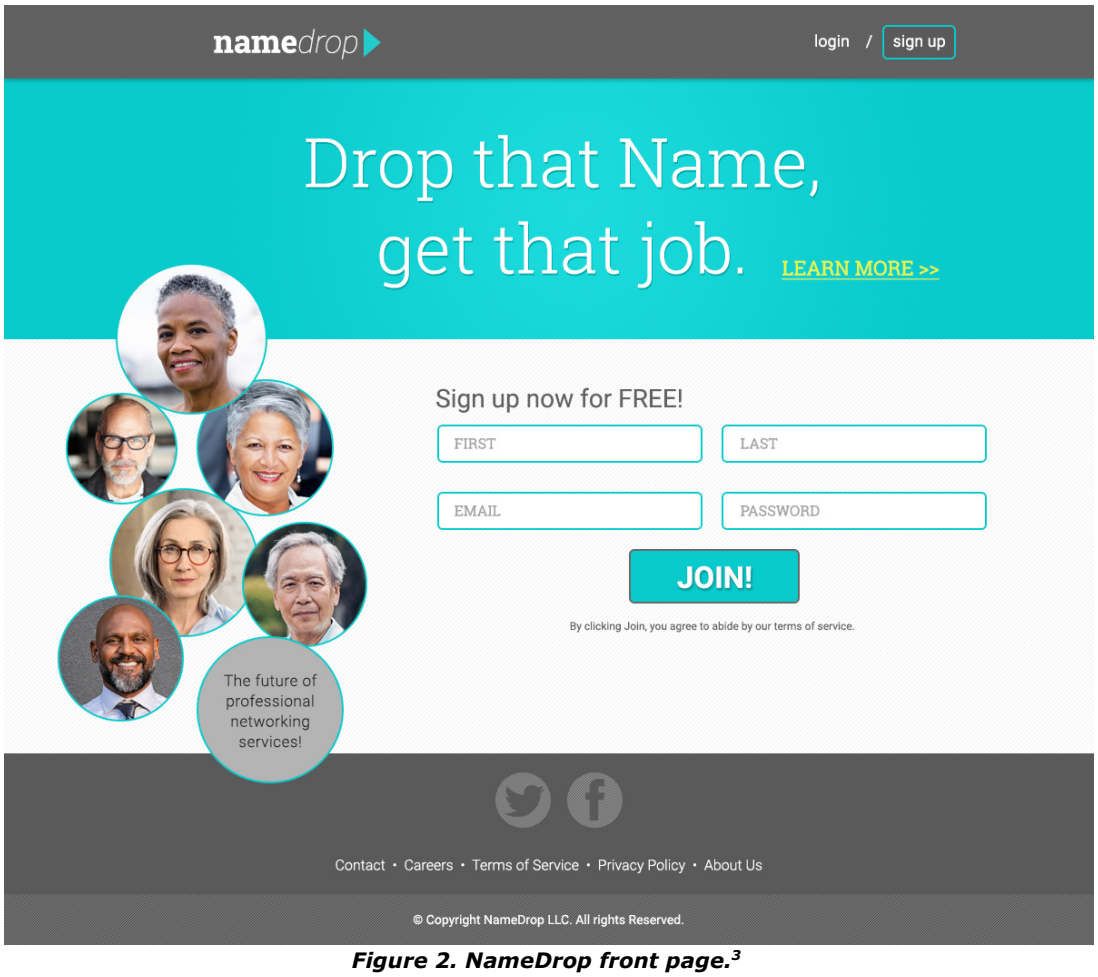

Figure 2. NameDrop front page.[3]

[3] Figure 2 photos are replacements that are similar to those in the original stimulus for this study. Photos from iStock.com/GlobalStock, NADOFOTOS, PaulSimcock, pixelfit, Ridofranz, and Vadym Pastukh.

Procedure

Participants were presented with university-approved consent materials. After agreeing, participants were shown the image of NameDrop's front page. Accompanying text read:

> NameDrop invites you to contribute to a pre-launch evaluation of the site. [. . .] To complete the review you will be signing up for the site and entering some basic personal information. Your account can be deleted after completing the review.

The claim of a prelaunch evaluation was a university research ethics-approved deception that attempted to convince participants they would be signing up to NameDrop to complete an evaluation, when in fact the study was assessing engagement with the consent process. At no time did participants sign up for a real SNS.

The clickwrap visualized in the image could not be clicked. To facilitate the clickwrap process, below the image was a set of Qualtrics radio buttons. The first button was accompanied by text reading: "Sign Up! (By clicking Sign Up, you agree to NameDrop's privacy policy)." A second button was accompanied by: "Click here to read NameDrop's privacy policy." Participants who chose "Sign Up!" demonstrated the behavior of skipping a policy, agreeing to the NameDrop PP without accessing it. These participants were directed past the PP to the TOS, which had to be accessed. Participants that chose the second button for the PP were presented with the PP text and then the TOS. At the bottom of the PP and the TOS were two radio buttons noting "I AGREE" or "I DO NOT AGREE." A selection had to be made to continue the survey, and whether participants agreed or not, they proceeded to the next section.

Stimuli

The NameDrop PP and TOS were essentially the same modified LinkedIn policies from Obar and Oeldorf-Hirsch (2020) to mimic current SNS policies. Qualtrics software helped assess how long each policy was accessed and whether policies were accepted or rejected. The length of the PP was 7,727 words and the TOS 4,741 words. While the previous literature suggests that the average adult reading speed is 250 words per minute (Taylor, 1965), a more recent meta-analysis of 190 studies and 17,887 participants suggests that based on differences between adults, a summary range of 175–300 words per minute for nonfiction texts is an accurate range for average reading speeds (Brysbaert, 2019). Reading speeds are slower for children, adults more than 60 years old, and those where English is not their first language (Brysbaert, 2019). Based on this speed range, the PP should have required between 44 and 26 minutes to read, and the TOS between 27 and 16 minutes for those 50–60 years of age. As average reading speeds for those 60+ are slower, average reading times should be even longer.

Similar to the previous study, three "gotcha clauses" were added to assess potential implications of ignoring policies. Two were included in the PP and one in the TOS. The content of the PP clauses was relevant to data collection and analysis and thus seemed appropriate for the PP. The TOS clause had more to do with the method of payment and therefore seemed more appropriate for the TOS.

The first gotcha clause added to the PP addressed the ability for NameDrop to access the user's camera or microphone, noting:

> 1.10.1. Device Access: In accordance with the terms set out in NameDrop's Privacy Policy, and in accordance with NameDrop's commitment to user experience, NameDrop reserves the right, at any time, to turn on and record from the camera and/or microphone of any device being used to access the NameDrop service. No further notification, beyond the text listed here, will be provided to alert users to device access.

The second clause was similar to a clause from the previous study about data sharing with the U.S. NSA and data brokers, reputation management, and eligibility. It was included within a section of the PP labeled "2.6 Sharing Information with Affiliates":

> Any and all data generated and/or collected by NameDrop, by any means, may be shared with third parties. For example, NameDrop may be required to share data with government agencies, including the U.S. NSA, and other security agencies in the United States and abroad. NameDrop may also choose to share data with third parties involved in the development of data products designed to assess eligibility. This could impact eligibility in the following areas: employment, financial service (bank loans, insurance, etc.), university entrance, international travel, the criminal justice system, etc. Under no circumstances will NameDrop be liable for any eventual decision made as a result of NameDrop data sharing.

In the TOS, we included a third gotcha clause that aimed to be the most extreme of the three. In the study of undergraduates, we included a "child assignment clause," which stated that by clicking agree, participants agreed to "immediately assign their first-born child to NameDrop" (Obar & Oeldorf-Hirsch, 2020, p. 7) Feedback received suggested that this clause be modified for the older adult population assessed. So instead we added an "organ-assignment clause." Included in the "3.3 Payment" section of the TOS, this new extreme clause read:

> 3.3.1 Payment types (organ-assignment clause): In addition to any monetary payment that the user may make to NameDrop, by agreeing to these TOS, and in exchange for service, all users of this site agree to immediately assign one of their human kidneys to NameDrop, Inc. This payment process involves immediate enrollment in NameDrop's Organ-Share Initiative, and within six months of signup the surgical extraction must be completed. In the event that the user has one or no functioning human kidney, NameDrop's Organ-Share Initiative will assess redundant organ needs, and require a substitute share within the same time period: hand, arm, foot, leg, eyeball, ear, etc. All surgical costs to be paid by the NameDrop account holder. No exceptions. All organs assigned to NameDrop automatically become the property of NameDrop, Inc. No exceptions.

Measures

NameDrop Policy Clickwrap Selection

Clickwrap selection was measured by whether participants selected "Sign Up!" to skip the PP (via the clickwrap) or selected to read the PP.

NameDrop Policy Reading Time

Time participants took to read both the PP and TOS was reported by Qualtrics, which tracked how many seconds individuals were on each page.

NameDrop Policy and Online Consent Process Concerns

Once participants completed their selections for the PP and TOS, they were presented with the open-ended item "Please describe any concerns that you have with the NameDrop Terms of Service Agreement and/or Privacy Policy." After completing the self-report reading behavior section noted earlier, participants were again presented with the NameDrop image and the open-ended question: "When you encounter signup prompts like this (name, password, etc.), do you often click "JOIN" without reading Terms of Service? Explain why or why not."

To assess the answers to these open-ended items, a content analysis coding instrument was used. Nine variables were assessed. The first seven addressed the initial question about concerns associated with the NameDrop PP and TOS, including concerns in general, concerns about data management, the NSA, the webcam/microphone clause, the organ-assignment clause, and policy length or complexity. Variables eight and nine assessed responses about how often clickwraps are used. Intercoder reliability was assessed by two trained coders comparing responses for 100 participants (20% of the sample). A standard percentage agreement test (Holsti, 1969) was used and determined a reliability range of $p = .98$ to $p = 1.00$ for the first seven variables ($m = .996$), and $p = .98$ and $p = .99$ for variables eight and nine ($m = .985$). Responses were also assessed via qualitative thematic analysis (Braun & Clarke, 2006).

Demographics

All participants were prompted to identify age, gender, and race/ethnicity in an open-ended format.

Results

The extent to which participants ignored NameDrop's PP and TOS (RQ1) was first assessed by evaluating whether individuals chose the clickwrap option for the PP—agreeing to the policy without accessing or reading it. Ignoring behavior was then assessed by recording and analyzing how long the remaining participants spent on the PP, and how long all participants spent with the TOS (as there was no TOS clickwrap). Whether participants agreed to policies was also assessed. The first set of qualitative

responses was content-analyzed to assess any policy concerns, including the text of the gotcha clauses, and the second set to determine how often clickwraps are used.

Ignoring NameDrop's Privacy and TOS Policies

NameDrop's Clickwrap

After being presented with the front page of the NameDrop SNS, as well as a clickwrap option, 388 of 500 participants (77.6%) chose the clickwrap, agreeing to the PP without accessing or reading it.

Participants were asked if they use clickwraps often and to explain why or why not. A content analysis of responses revealed that 166 of 500 participants (33%) reported that they use clickwraps often. An additional 76 said they use clickwraps sometimes, suggesting that 48.4% use clickwraps often or sometimes. Some responses (73) were coded "unclear," as participants did not answer the question. Removing these (reducing sample to 427), the percentage that said they use clickwraps often rises to 38.8%, and to 56.7% for often or sometimes. In total, 261 of 427 participants (61%) were coded as not using clickwraps often, though as 76 were coded as using them sometimes, 185 of 427 (43.3%) were coded as not using clickwraps often or sometimes.

Participants often emphasized that they tend to "skim" policies, with some seeming to state adamantly that they oppose ignoring behaviors. One said "No I do not click 'join' right away. I like to find out what they are about," another said, "No! Need more information," and another "Never join anything without reading," while another wrote, "I read everything before I join." Some wrote the term "should" when describing engagement with consent materials; for example, "You *should* always read to know what they are going to do with your information," and "I know I *should* (read) but sometimes I'm too busy, or just lazy" (emphasis added).

Policy Reading Times

Instead of choosing the clickwrap, 112 participants (22.4%) chose "Click here to read NameDrop's privacy policy" and proceeded to the policy. For these participants, the average time spent on NameDrop's PP was M = 69.95 seconds, with a range of 6.27 seconds–1,642.37 seconds (27.37 minutes). The median reading time = 24.24 seconds, SD = 177.78. As the average adult reading speed of nonfiction text is 175–300 words per minute (Brysbaert, 2019), the PP at 7,727 words, should have taken 26–44 minutes to read for those 50–60 years old.

For NameDrop's TOS, average reading time was M = 81.42 seconds, with a range of 6.47–1,242.02 seconds (20.70 minutes). The median reading time = 31.63 seconds, SD = 151.97. The TOS at 4,741 words should have taken about 16–27 minutes for those 50–60. Again, the literature suggests that for those more than 60 years of age, average reading times are longer (Brysbaert, 2019).

Of the 112 participants who chose to access the PP, the majority, 87 (77.7%), spent 1 minute or less reading it. Twelve (10.7%) spent 1–2 minutes, 5% spent 2–3 minutes, 2% spent 3–4 minutes, and

only 5% spent 5 or more minutes reading the PP. Thus, 107 (95.5%) of the 112 older adult participants spent less than 5 minutes on the NameDrop PP (see Figure 3). Including those who skipped the policy through the clickwrap, 495 of 500 participants (99%) spent less than 5 minutes with NameDrop's PP.

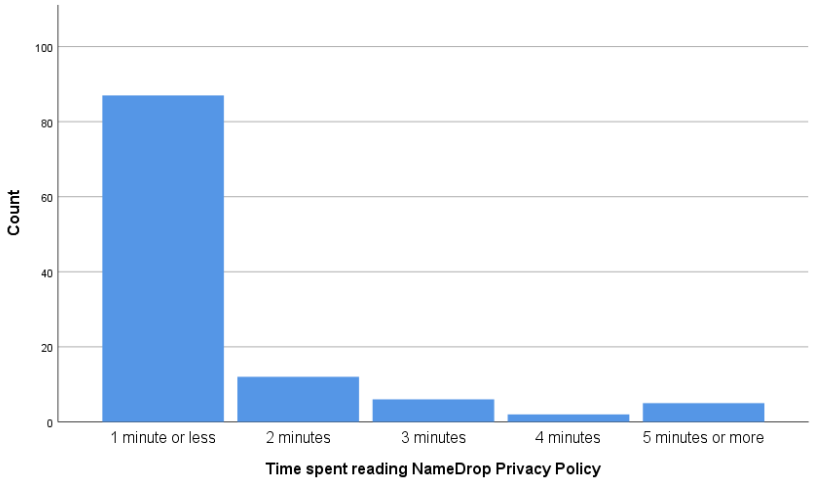

Figure 3. Count of participants reading privacy policy in 1 minute or less to 5 minutes or more.

As noted in Figure 4, most participants—360 of 500 (72%)—spent 1 minute or less on NameDrop's TOS. The next largest group of 59 participants (11.8%) spent between 1 and 2 minutes, 6% spent 2–3 minutes, and 2% spent 4–5 minutes. Thirty-seven participants (7.4%) spent 5 minutes or more on the TOS. Said another way, 463 of 500 participants (92.6%) spent less than 5 minutes on the TOS.

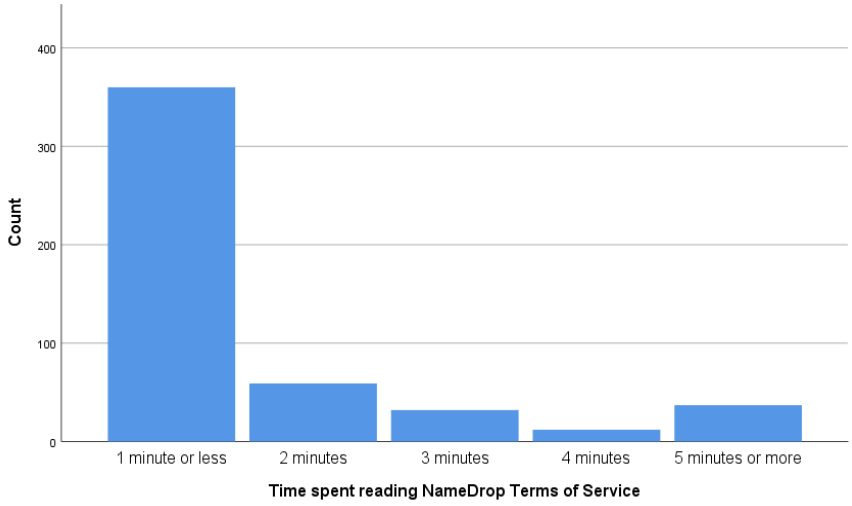

Figure 4. Count of participants reading terms of service in 1 minute or less to 5 minutes or more.

The "Gotcha Clauses" and Other Policy Concerns

In the PP, there were two "gotcha clauses." The first, a "device access" clause, suggested NameDrop could activate the participant's device microphone and/or camera to engage in data collection. NameDrop would not provide further notification about this activity. The second suggested NameDrop could share data with the U.S. NSA and third parties developing data products, leading to a potential impact on eligibility determinations, for which NameDrop would shoulder no responsibility. A content analysis of the qualitative responses revealed 146 of 500 (29%) expressed a concern about the policies, with 43 participants (8.6%) suggesting concerns about data management or privacy. In terms of specific references to the gotcha clauses, only one participant mentioned the device access clause, and zero participants mentioned the NSA.

The "redundant organ" or "organ-assignment" clause was included in the TOS and suggested that NameDrop requires organ donation as a form of payment for service. The content analysis revealed only 4 of 500 participants (0.8%) expressed concern about the redundant organ-assignment clause.

Policy concern was also assessed by coding for concern about the length and complexity of the policies. In total, 39 participants (7.8%) expressed concern about policy length, while 16 (3.2%) expressed concern about policy complexity.

Responses from participants emphasized policies are "too long" and "too hard to understand." Extending from this were comments suggesting policies are "too time consuming"; "I'm too busy"; "it's a hassle to read them"; and "I'm in a hurry to sign up." One participant added "I click join, excited to start exploring new site. Get too anxious and just want to get in site." Even more participants said, "I hate being bothered" or "I hate reading Terms of Service," they are "boring," "tedious," "confusing," and "I'm too busy, or just lazy." Participants also added "I am multi-tasking," and ignoring policies is a "habit."

Accepting or Rejecting Policies

For NameDrop's PP, 388 participants agreed to the policy by selecting the clickwrap. An additional 69 agreed after accessing it, totaling 457 of 500 participants (91.4%) that accepted the PP. It should be reiterated that the PP included both the device access and NSA/data sharing clauses. All 500 accessed the TOS as there was no clickwrap. In total, 417 of 500 participants (83.4%) accepted NameDrop's TOS, which included the redundant organ-assignment clause.

In terms of rejecting the policies, 43 of 500 (8.6%) participants accessed the PP and rejected it. For the TOS, all participants accessed the policy, and 83 participants (16.6%) rejected it. Those who agreed to the PP did not spend any longer reading than those who rejected it, $t(74.97) = 1.90$, $p = .06$. Likewise, there was no significant difference in reading time between those who agreed to the TOS and those who did not, $t(498) = -.283$, $p = .78$.

Discussion

The results of this study suggest that older adults aged 50+ often ignore privacy and TOS policies during social media signup. While the previous literature asserts that older adults care about online privacy (e.g., Hoofnagle et al., 2010; Quan-Haase & Elueze, 2018), and are interested in privacy protective behaviors (e.g., Gupta & Chennamaneni, 2018; Kezer et al., 2016; Madden, 2012; Rainie et al., 2013), the findings of the current study suggest otherwise.

Results suggest that many older adults signing up for SNS engage in two ignoring behaviors: (1) the use of clickwraps, and (2) a lack of engagement with policies when accessed. Beginning with the clickwrap, more than three-quarters (77.6%) of the 500 older adults chose NameDrop's clickwrap and agreed to the PP without accessing, viewing, reading, or understanding it. The PP could have been 10 or 100,000 words. It might have had information connecting data collection to future artificial intelligence initiatives. It might have mentioned connections between data use, privacy, reputation, and eligibility. It might have had information about opt-out mechanisms, a privacy dashboard, or information about dissent opportunities such as contact information for privacy advocacy organizations, ombudsmen, or references to applicable law and policy. But because of the decision many participants made to agree without accessing or reading the PP via NameDrop's clickwrap, users quickly circumvented these education, engagement, and dissent opportunities.

Close to 39% of participants said they use clickwraps often. The number increases to 56.7% when asked if clickwraps are used often or sometimes. In a study entitled "The Clickwrap" (Obar & Oeldorf-Hirsch, 2018), we argued that clickwraps serve a political economic function by failing to make users aware of online consent processes, training users to miss online consent opportunities and to view these processes and opportunities as unimportant. Through the presentation of an appealing "JOIN" or "I AGREE" button, in a position that is easy to see, compared to smaller, less-appealing links to policies, sometimes in a less-obvious position, as users read from top-to-bottom, the clickwrap facilitates an agenda setting function that prioritizes joining as quickly as possible over policy access and review. This speeds users toward monetized sections of services, keeping them away from dissent opportunities (Obar & Oeldorf-Hirsch, 2018). Furthermore,

> By maintaining a "buying mood" or in the social media context, the mindset where consent materials are invisible, irrelevant, or irritating, social media providers maintain the status quo [. . .] By encouraging a form of user activity, namely, the circumvention of consent materials, [. . .] social media services extend traditional strategies associated with the corporate media. (Obar & Oeldorf-Hirsch, 2018, p. 11)

Clickwraps help users maintain a focus on consumption, as opposed to a tangential privacy engagement, education, or dissent. This is akin to research into deceptive user-interface design, asserting that the design of technologies can exploit users, directing individuals to pursue online behaviors that are preferential to service providers (e.g., Bösch, Erb, Kargl, Kopp, & Pfattheicher, 2016).

When participants did access policies, they often spent little time reviewing them (a second ignoring behavior). For the 22.4% who accessed NameDrop's PP, average reading time was 69.95 seconds. This is certainly not enough time to read, let alone understand, a technical nonfiction text that should have taken between 26 and 44 minutes to read. The median time of 24.24 seconds further reveals how many participants likely engaged in ignoring behaviors that include skipping, scrolling, and skimming of policy text. Similar behaviors were observed with NameDrop's TOS, which all participants accessed. Average reading time increased to 81.42 seconds, with a 31.63-second median. The policy required between 16 and 27 minutes to read, acknowledging that this reading speed range is for adults 50–60 years of age, with the literature suggesting those 60+ require more time (Brysbaert, 2019). Again, 30 seconds or even a minute and a half is not nearly enough time to read through or understand the policy. Overall, ignoring behaviors were common with the PP and TOS. Of the 112 who accessed the PP, 77.7% spent 1 minute or less reading, and including the participants who chose the clickwrap, 99% of participants spent less than 5 minutes with NameDrop's PP. With all participants accessing NameDrop's TOS, 72% spent 1 minute or less with the document, and 92.6% spent less than 5 minutes.

Two Examples of the Privacy Paradox

The results suggest two different privacy paradoxes. The first is via the clickwrap: 388 of the 500 participants (77.6%) chose NameDrop's clickwrap, whereas only 48.4% said they use clickwraps often or sometimes, increasing to 56.7% with unclear responses removed. This suggests a difference between what older adults say about their use of clickwraps and what they do.

The results suggest another privacy paradox when compared to a complementary self-report assessment of digital media policy reading behavior (Oeldorf-Hirsch & Obar, 2019). For Facebook and Instagram, for example, participants reported that upon signup, they spent more than 16 minutes reading the PP and around 15 minutes for Twitter and YouTube. TOS reported reading times were around 12–13 minutes. Comparing these self-report results to those of the experimental survey suggest a more considerable privacy paradox. Participants spent on average about a minute and a half on both the PP and TOS, with a considerable majority spending under a minute, contributing to medians between 24 and around 31 seconds. When these reading times are compared to the self-report times, it is difficult to overlook the considerable differences.

While the literature suggests moving beyond the say/do privacy paradox dichotomy because of the different reasons people say one thing and do another (e.g., Baruh et al., 2017; Kokolakis, 2017), the dichotomy does appear helpful in this instance. Possible overstatements about time spent reading policies, along with claims about skimming policies, seemingly adamant opposition to ignoring behaviors, and statements that individuals "should" engage before clicking agree, suggests that older adults know better.

If this is the case, why are older adults deciding to avoid accessing or reading policies? Participants did note repeatedly that policies are long and complicated, boring, and a waste of time. Similar to the findings in Obar and Oeldorf-Hirsch (2020), a study of undergraduates, "notice [. . .] equals nuisance" (p. 144). Participants emphasize that they "hate being bothered," are in a "hurry," and are "excited to start exploring." Indeed, online consent processes are seen as tangential impediments to the primary purpose

for accessing a site or downloading an app in this context—to social network. The differences in the say/do dichotomy suggest that the demand for privacy and reputation deliverables may be real, but the instruments and opportunities for realizing them may be prohibitive.

Indeed, assertions suggesting privacy disengagement whether because of digital resignation (Draper & Turow, 2019), feeling a lack of control (Hargittai & Marwick, 2016), or perhaps "privacy fatigue" (Choi, Park, & Jung, 2018), may all be linked to issues with policy and online consent interface design. While the European Union's General Data Protection Regulation provides reasons for optimism, it still emphasizes that online consent processes should not be "unnecessarily disruptive" to service use and that "ticking a box" is an acceptable form of user engagement (EU, 2016, Section 32). The form and content of SNS consent materials, that problematic policy directs, SNS organizations design, and users experience, are not moving individuals from privacy concern to privacy protective behavior—or from say to do. Policy and self-regulatory (i.e., digital service provider) approaches are achieving little if "I agree to the terms and conditions" is "the biggest lie on the Internet." Far more needs to be done to ensure the delivery of protections and should continue to be the subject of considerable research efforts.

The Implications of Ignoring SNS Policies—the "Gotcha Clauses"

The findings suggest various potential implications of SNS policy-ignoring behaviors. The PP included two gotcha clauses meant to articulate some of these concerns. The first dealt with data collection through device access, suggesting that NameDrop could turn on the participants' microphones and cameras at any time for data-collection purposes. The second dealt with data use, articulating that NameDrop might share data with third parties developing data products for assessing eligibility, and even with the NSA. The clause highlighted that this sharing might have implications at an individual's bank, school, work, at the border, with the criminal justice system, and so forth, where eligibility decisions might take place. Furthermore, the clauses suggest a connection between NameDrop data collection/management processes and the development of machine learning/artificial intelligence products and services.

After proceeding through the online consent process, participants were asked if they had any concerns. Only 8.6% of the 500 participants expressed a concern about data management, with many making general comments about privacy, suggesting that they might not have noticed the device access or data sharing clauses in the PP. This is furthered by the fact that only one individual mentioned the device access clause, and zero mentioned the NSA. Keep in mind that more than three-quarters of the participants agreed to the device access and data sharing policies via the clickwrap, meaning they accepted these clauses without accessing them. In total, 457 of 500 participants, or 91.4%, agreed to the PP. This is surprising with this population, as the previous literature suggests not only that older adults care about online privacy, but are especially concerned about institutional privacy, or privacy associated with institutional (i.e., service provider) relationships (Quan-Haase & Elueze, 2018). It is worth noting that the device access clause mentioned that the PP would be the only place where this data-collection process would be brought to the participant's attention. No dynamic consent process or online consent notification would take place when the microphone or camera was activated. This is another issue for consideration as improvements to policy and self-regulatory approaches continue to be the focus of future research.

The TOS also included a redundant organ-assignment clause. Even though all 500 participants accessed NameDrop's TOS, only four mentioned that the clause was a concern. That likely means 496 of 500 participants (99.2%) did not notice the clause. In total, 83.4% of participants (417 of 500 individuals) accepted NameDrop's TOS and agreed not only to provide NameDrop with a (so-called) "redundant" organ within the next six months (joining NameDrop's "Organ-Share Initiative"), but to pay all surgical costs as well.

The purpose of including such an extreme clause is to suggest that policy-ignoring behaviors can have wide-ranging implications. Although it is unlikely that a company could ever legally require organ donation as payment for service, if 417 of 500 participants would agree to donate a kidney or an eyeball for access to a social networking service, it is possible that many other problematic possibilities, within legal boundaries, could be agreed to as well.

Government and industry must do far more to address the ignoring behaviors this study suggests. As long as the individual continues to be at the center of the big data universe as continuous data subject and overburdened privacy savior (see Obar, 2015; Solove, 2012), individuals will be left without the instruments for realizing online privacy and reputation deliverables.

Limitations and Future Research

The experimental setting of this study poses limitations in terms of understanding how participants might behave in the real world. First, the limitations of self-report seem clear, as participants vastly overestimate, are embarrassed to admit, or fail to remember their actual engagement with policies upon signup. While the privacy paradox literature emphasizes the importance of contextual nuances to explaining why people say one thing and do another (Kokolakis, 2017), the findings of this study suggest not only that ignoring SNS consent materials is common, but that participants seem to have difficulty demonstrating the extent of that behavior via self-report. Additionally, participants knew that they were taking part in an academic study. Thus, whatever trust they may have in the university or academic research could have made them more apt to accept the policies without scrutiny. That said, individuals may accept policies in real life via different trust-based scenarios, including those developed through friends and colleagues, for example. Furthermore, universities ask individuals to consent to privacy-threatening services all the time (e.g., e-mail and course-management software). This suggests trust is difficult to remove from online consent processes and that privacy threats exist even when people think they can trust those associated with services. The sample is skewed in terms of age (on the younger end of the range), gender (more female participants), and race (more Caucasian participants) which do not match the demographics of 50+ users in the United States, and thus are not conclusively representative of the 50+ population.

Last, the site presented here—a fictitious employment site—may not have been as relevant to this population, influencing policy concern. Considering these limitations, we suggest that more research be conducted that attempts to emulate real contexts where individuals sign up for digital services, and that providers, scholars, advocates, and policymakers avoid future policy directed by self-report results alone.

Conclusion

Even though older adults may say they care about privacy and also that they will engage in privacy protective behaviors, the findings here assert otherwise. When presented with an opportunity to engage with SNS policy materials during signup, policy skipping, skimming, and ignoring were the primary privacy protective behaviors. To support older adults as they attempt to realize privacy deliverables, policymakers and digital service providers must do more to address the burden placed on individuals through deceptive interface designs like the clickwrap, and via TOS and privacy policies that are long and complicated.

References

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science, 347*(6221), 509–514. doi:10.1126/science.aaa1465

Auxier, B., Rainie, L., Anderson, M., Perrin, A., Kumar, M., & Turner, E. (2019). *Americans and privacy: Concerned, confused and feeling lack of control over their personal information*. Pew Research Center. Retrieved from https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/

Bakos, Y., Marotta-Wurgler, F., & Trossen, D. R. (2014). Does anyone read the fine print? Consumer attention to standard-form contracts. *The Journal of Legal Studies, 43*(1), 1–35. doi:10.1086/674424

Barth, S., & de Jong, M. D. T. (2017). The privacy paradox—Investigating discrepancies between expressed privacy concerns and actual online behavior—A systematic literature review. *Telematics and Informatics, 34*(7), 1038–1058. doi:10.1016/j.tele.2017.04.013

Baruh, L., Secinti, E., & Cemalcilar, Z. (2017). Online privacy concerns and privacy management: A meta-analytical review. *Journal of Communication, 67*(1), 26–53. doi:10.1111/jcom.12276

Ben-Shahar, O., & Schneider, C. E. (2011). The failure of mandated disclosure. *University of Pennsylvania Law Review, 159*(3), 647–749.

Bösch, C., Erb, B., Kargl, F., Kopp, H., & Pfattheicher, S. (2016). Tales from the dark side: Privacy dark strategies and privacy dark patterns. *Proceedings on Privacy Enhancing Technologies, 2016*(4), 237–254. doi:10.1515/popets-2016-0038

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology, 3*(2), 77–101. doi:10.1191/1478088706qp063oa

Brysbaert, M. (2019). How many words do we read per minute? A review and meta-analysis of reading rate. *Journal of Memory and Language, 109*, 1–30. doi:10.1016/j.jml.2019.104047

Calo, R. (2011). Against notice skepticism in privacy (and elsewhere). *Notre Dame Law Review, 87*(3), 1027–1072. Retrieved from https://scholarship.law.nd.edu/ndlr/vol87/iss3/3

Cate, F. H. (2016). The failure of fair information practice principles. In J. K. Winn (Ed.), *Consumer protection in the age of the "information economy"* (pp. 341–377). New York, NY: Routledge.

Choi, H., Park, J., & Jung, Y. (2018). The role of privacy fatigue in online privacy behavior. *Computers in Human Behavior, 81*, 42–51. doi:10.1016/j.chb.2017.12.001

Dinev, T., Bellotto, M., Hart, P., Russo, V., Serra, I., & Colautti, C. (2006). Privacy calculus model in e-commerce—A study of Italy and the United States. *European Journal of Information Systems*, *15*(4), 389–402. https://doi.org/10.1057/palgrave.ejis.3000590

Draper, N. A., & Turow, J. (2019). The corporate cultivation of digital resignation. *New Media & Society, 21*(8), 1824–1839. doi:10.1177/1461444819833331

European Union. (2016, May 4). Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Office Journal of the European Union, L119.

Feng, Y., Yao, Y., & Sadeh, N. (2021, May). A design space for privacy choices: Towards meaningful privacy control in the Internet of things. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (pp. 1–16). New York, NY: ACM. doi:10.1145/3411764.3445148

Gerber, N., Gerber, P., & Volkamer, M. (2018). Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Computers and Security, 77*(August), 226–261. doi:10.1016/j.cose.2018.04.002

Gibson, L., Moncur, W., Forbes, P., Arnott, J., Martin, C., & Bhachu, A. S. (2010). Designing social networking sites for older adults. In *Proceedings of the 24th BCS Interaction Specialist Group Conference* (pp. 186–94). New York, NY: ACM. doi:10.14236/ewic/HCI2010.24

Groom, V., & Calo, R. (2011). *Reversing the privacy paradox: An experimental study*. TPRC. Retrieved from https://ssrn.com/abstract=1993125

Gupta, B., & Chennamaneni, A. (2018). Understanding online privacy protection behavior of the older adults: An empirical investigation. *Journal of Information Technology Management, 29*(3), 1–13. Retrieved from https://digitalcommons.csumb.edu/cob_fac/8/

Hargittai, E., & Marwick, A. (2016). "What can I really do?" Explaining the privacy paradox with online apathy. *International Journal of Communication, 10*, 3737–3757. Retrieved from https://ijoc.org/index.php/ijoc/article/view/4655

Hartzog, W. (2016). The inadequate, invaluable fair information practices. *Maryland Law Review, 76*(4), 952–983. Retrieved from https://digitalcommons.law.umaryland.edu/mlr/vol76/iss4/4/

Holsti, O. R. (1969). *Content analysis for the social sciences and humanities.* Don Mills, Ontario: Addison-Wesley.

Hoofnagle, C. J., King, J., Li, S., & Turow, J. (2010). How different are young adults from older adults when it comes to information privacy attitudes and policies? *SSRN*. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1589864

Jensen, C., Potts, C., & Jensen, C. (2005). Privacy practices of Internet users: Self-reports versus observed behavior. *International Journal of Human-Computer Studies*, *63*(1–2), 203–227. https://doi.org/10.1016/j.ijhcs.2005.04.019

Kadylak, T., & Cotten, S. R. (2020). United States older adults' willingness to use emerging technologies. *Information, Communication & Society, 23*(5), 736–750. doi:10.1080/1369118X.2020.1713848

Kezer, M., Sevi, B., Cemalcilar, Z., & Baruh, L. (2016). Age differences in privacy attitudes, literacy and privacy management on Facebook. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 10*(1), Article 2. doi:10.5817/CP2016-1-2

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security, 64*, 122–134. doi:10.1016/j.cose.2015.07.002

Lannerö, P. (2012, January 27). *Previewing online terms and conditions: CommonTerms alpha proposal*. Retrieved from http://commonterms.org/commonterms_alpha_proposal.pdf

Li, K., Lin, Z., & Wang, X. (2015). An empirical analysis of users' privacy disclosure behaviors on social network sites. *Information and Management, 52*(7), 882–891. doi:10.1016/j.im.2015.07.006

McDonald, A. M., & Cranor, L. F. (2008). The cost of reading privacy policies. *I/S: A Journal of Law and Policy for the Information Society, 4*(3), 540–565.

Madden, M. (2012, February 24). *Privacy management on social media sites*. Pew Research Center. Retrieved from https://www.pewresearch.org/internet/2012/02/24/privacy-management-on-social-media-sites/

Marotta-Wurgler, F., & Chen, D. L. (2012). Does contract disclosure matter? [with comment]. *Journal of Institutional and Theoretical Economics, 168*(1), 94–123. Retrieved from https://www.jstor.org/stable/41474939

Milne, G. R., & Culnan, M. J. (2004). Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices. *Journal of Interactive Marketing, 18*(3), 15–29. doi:10.1002/dir.20009

Nissenbaum, H. (2011). A contextual approach to privacy online. *Daedalus, 140*(4), 32–48. doi:10.1162/DAED_a_00113

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs, 41*(1), 100–126. doi:10.1111/j.1745-6606.2006.00070.x

Obar, J. A. (2015). Big data and *The Phantom Public*: Walter Lippmann and the fallacy of data privacy self-management. *Big Data & Society, 2*(2), 1–16. doi:10.1177/2053951715608876

Obar, J. A. (2022). Defining and assessing data privacy transparency: A third study of Canadian Internet carriers. *International Journal of Communication, 16*, 1688–1712. Retrieved from https://ijoc.org/index.php/ijoc/article/view/15785

Obar, J. A., & Magalashvili, L. (2021). The clickwrap as platform governance: Assessing the frequency of manipulative interface designs during digital service sign-up. *SSRN*. Retrieved from https://dx.doi.org/10.2139/ssrn.3898254

Obar, J. A., & Oeldorf-Hirsch, A. (2018). The clickwrap: A political economic mechanism for manufacturing consent on social media. *Social Media+ Society, 4*(3), 1–14. doi:10.1177/2056305118784770

Obar, J. A., & Oeldorf-Hirsch, A. (2020). The biggest lie on the Internet: Ignoring the privacy policies and terms of service policies of social networking services. *Information, Communication & Society, 23*(1), 128–147. doi:10.1080/1369118X.2018.1486870

Oeldorf-Hirsch, A., & Obar, J. A. (2019). Overwhelming, important, irrelevant: Terms of service and privacy policy reading among older adults. In *Proceedings of the 10th International Conference on Social Media and Society* (pp. 166–173). New York, NY: ACM. doi:10.1145/3328529.3328557

Quan-Haase, A., & Elueze, I. (2018). Revisiting the privacy paradox: Concerns and protection strategies in the social media experiences of older adults. In *Proceedings of the 9th International Conference on Social Media and Society* (pp. 150–159). New York, NY: ACM. doi:10.1145/3217804.3217907

Rainie, L., Kiesler, S., Kang, R., & Madden, M. (2013, September 5). *Anonymity, privacy, and security online*. Pew Research Center. Retrieved from https://www.pewresearch.org/internet/2013/09/05/anonymity-privacy-and-security-online/

Raynes-Goldie, K. (2010). Aliases, creeping, and wall cleaning: Understanding privacy in the age of Facebook. *First Monday, 15*(1). doi:10.5210/fm.v15i1.2775

Reidenberg, J. R., Breaux, T., Cranor, L. F., French, B., Grannis, A., Graves, J. T., . . . Schaub, F. (2015). Disagreeable privacy policies: Mismatches between meaning and users' understanding. *Berkeley Technology Law Journal, 30*(1), 39–68.

Solove, D. J. (2012). Introduction: Privacy self-management and the consent dilemma. *Harvard Law Review, 126*, 1880–1903.

Steinfeld, N. (2016). "I agree to the terms and conditions": (How) do users read privacy policies online? An eye-tracking experiment." *Computers in Human Behavior, 55*, 992–1000. doi:10.1016/j.chb.2015.09.038

Taylor, S. E. (1965). Eye movements in reading: Facts and fallacies. *American Educational Research Journal, 2*(4), 187–202. doi:10.3102/00028312002004187

Terms of Service; Didn't Read. (2022). Terms of service; didn't read. Retrieved from https://tosdr.org

Wottrich, V. M., van Reijmersdal, E. A., & Smit, E. G. (2018). The privacy trade-off for mobile app downloads: The roles of app value, intrusiveness, and privacy concerns. *Decision Support Systems, 106*, 44–52. doi:10.1016/j.dss.2017.12.003

Xie, B., Watkins, I., Golbeck, J., & Huang, M. (2012). Understanding and changing older adults' perceptions and learning of social media. *Educational Gerontology, 38*(4), 282–296. doi:10.1080/03601277.2010.544580

Yuan, S., Hussain, S. A., Hales, K. D., & Cotten, S. R. (2016). What do they like? Communication preferences and patterns of older adults in the United States: The role of technology. *Educational Gerontology, 42*(3), 163–174. doi:10.1080/03601277.2015.1083392