Information, Communication & Society

ISSN: 1369-118X (Print) 1468-4462 (Online) Journal homepage: www.tandfonline.com/journals/rics20

The biggest lie on the Internet: ignoring the privacy policies and terms of service policies of social networking services

Jonathan A. Obar & Anne Oeldorf-Hirsch

To cite this article: Jonathan A. Obar & Anne Oeldorf-Hirsch (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

To link to this article: https://doi.org/10.1080/1369118X.2018.1486870

INFORMATION, COMMUNICATION & SOCIETY
2020, VOL. 23, NO. 1, 128–147
https://doi.org/10.1080/1369118X.2018.1486870

Routledge
Taylor & Francis Group

The biggest lie on the Internet: ignoring the privacy policies and terms of service policies of social networking services

Jonathan A. Obar[a] and Anne Oeldorf-Hirsch [b]

[a]Department of Communication Studies, York University, Toronto, ON, Canada; [b]Department of Communication, University of Connecticut, Storrs, CT, USA

ABSTRACT

This paper addresses 'the biggest lie on the internet' with an empirical investigation of privacy policy (PP) and terms of service (TOS) policy reading behavior. An experimental survey ($N = 543$) assessed the extent to which individuals ignored PP and TOS when joining a fictitious social networking service (SNS), NameDrop. Results reveal 74% skipped PP, selecting the 'quick join' clickwrap. Average adult reading speed (250–280 words per minute), suggests PP should have taken 29–32 minutes and TOS 15–17 minutes to read. For those that didn't select the clickwrap, average PP reading time was 73 seconds. All participants were presented the TOS and had an average reading time of 51 seconds. Most participants agreed to the policies, 97% to PP and 93% to TOS, with decliners reading PP 30 seconds longer and TOS 90 seconds longer. A regression analysis identifies information overload as a significant negative predictor of reading TOS upon sign up, when TOS changes, and when PP changes. Qualitative findings suggest that participants view policies as nuisance, ignoring them to pursue the ends of digital production, without being inhibited by the means. Implications are revealed as 98% missed NameDrop TOS 'gotcha clauses' about data sharing with the NSA and employers, and about providing a first-born child as payment for SNS access.

ARTICLE HISTORY
Received 16 November 2017
Accepted 5 June 2018

KEYWORDS
Privacy policies; terms of service; privacy; consent; social networking service; social media

Effective strategies for realizing digital reputation and privacy protections remain unclear. While self-governance efforts by proprietary platforms provide de facto protections (DeNardis & Hackl, 2015), leaving privacy and reputation to companies monetized through data-driven business models seems problematic. Data resistance technologies and other privacy-enhancing services offer the possibility of bottom-up protections; however, ubiquitous and continuously effective adoption in the face of the Big Data deluge seems an 'unattainable ideal' (Obar, 2015, p. 1). Others simply suggest that privacy is dead (Morgan, 2014; Sanders, 2011). Differing from these strategies defined by neoliberalism and futility is another approach to solving difficult problems - government intervention.

CONTACT Jonathan A. Obar jaobar@yorku.ca York University, 4700 Keele Street DB 3015, Toronto, Ontario, Canada M3J 1P3

Top-down approaches to privacy and increasingly reputation protections by governments throughout the world often draw from a contentious model referred to as the 'notice and choice' privacy framework. Notice and choice evolved from a set of Fair Information Practice Principles, developed by the US Department of Health, Education and Welfare in the 1970s, and later adopted by the Federal Trade Commission (FTC) to address growing information privacy concerns raised by digitization. In the early 1980s, the FIPPs were promoted by the OECD as part of an international set of privacy guidelines (OECD, 1980), contributing to the implementation of data protection laws and guidelines in the US, Canada, the EU, Australia and elsewhere, often with language mirroring the FIPPs from the 1970s. Even in the face of considerable criticism (see: Obar, 2015; Cate, 2006; Madden, Gilman, Levy, & Marwick, 2017; McDonald & Cranor, 2008; Nissenbaum, 2011; Reidenberg, Breaux et al., 2015; Reidenberg, Russell, Callen, Qasir, & Norton, 2015; Solove, 2012), ongoing efforts to strengthen data protections continue to draw on the old framework.

The notice and choice privacy framework was designed to 'put individuals in charge of the collection and use of their personal information' (Reidenberg, Russell, Callen, Qasir, & Norton, 2014, p. 3). Though implementation differs by context, the choice components consist of a variety of access, control and security mechanisms that recommend how users might check, correct and/or approve personal data managed and used by different organizations, similar to how one monitors credit reports before applying for a loan.

The focus of our current inquiry, however, is on the notice component, characterized by the FTC as 'the most fundamental principle' (FTC, 1998, p. 7) of personal information protection. Notice consists of efforts by an entity to inform the source of data collection, sharing, etc. that the action in question is taking place. As the FTC (1998) notes, choice and related principles attempting to offer data control 'are only meaningful when a consumer has notice of an entity's policies, and his or her rights with respect thereto.' (p. 7) Notice policies typically draw from the OECD's 'openness principle' which states:

> [t]here should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller. (OECD, 1980)

Across contexts, entities involved in data management attempt to abide by notice policy by providing individuals with consent materials, typically in the form of privacy policies (PP) and terms of service (TOS) policies. These policies appear on websites, applications, are sent in the mail, provided in-person, generally when an individual connects with the entity in question for the first time, and when policies change. Despite suggestions that notice policy in particular is deeply flawed, strategies for strengthening notice policy continue to be seen as central to addressing, for example, privacy concerns associated with corporate and government surveillance, and consumer protection concerns about Big Data, data brokerage and eligibility decision-making (see: FTC, 2012; White House, 2014).

This brings us to the biggest lie on the Internet, which anecdotally, is known as 'I agree to these terms and conditions.' Upon discussing the current study with colleagues, most agree that ignoring privacy and TOS policies is both a reality and a problem. 'I never read those things' and 'nobody reads them' are common responses. The non-profit TOS; DR (Terms of Service; Didn't Read) advances a similar anecdotal assertion. The

front page of their website reads 'I have read and agree to the Terms' is the biggest lie on the web. We aim to fix that' (DR, 2018). The site www.biggestlie.com states on its homepage 'Let's STOP the biggest lie on the web!' and asks users to acknowledge and address the lie by clicking 'I confess – and protest!' – almost 6000 such confessions have been made since 2012 (Biggestlie.com, 2018) . Policy-makers often advance similar claims that individuals commonly ignore policies (e.g., DOC, 2010; FTC, 2012; OPC, 2017). For example, FTC Commissioner Jon Leibowitz once said,

> Initially, privacy policies seemed like a good idea. But in practice, they often leave a lot to be desired. In many cases, consumers don't notice, read, or understand the privacy policies. (Leibowitz, 2007, p. 4)

Whether or not the magnitude of the lie is to the degree the anecdote suggests, the idea that the practice of ignoring privacy and TOS policies is widespread, points to considerable regulatory failure. If it is true that people typically ignore policies when engaging forms of digital media, it suggests that notice policy doesn't work, and perhaps that committed and continued resources devoted to notice efforts are being wasted. Acknowledgment of this regulatory failure, supported by empirical evidence, would be a first step towards more pragmatic approaches that might actually provide individuals with digital privacy and reputation protections.

This experimental survey of 543 participants addresses the extent to which individuals ignore privacy and TOS policies when joining social networking services for the first time as well as when policies are updated. It begins with an original assessment of participant engagement with consent materials for what they believe is a new social networking service called NameDrop. This analysis is complemented by various self-report measures of reading behavior, including predictors. In the next section, a review of the literature on privacy and TOS policy reading behaviors is discussed, followed by the study.

Policy reading behavior: previous research, self-reporting, and clickwraps

While previous studies have assessed privacy and TOS policy reading behavior, many predate the rise of social networking services, smartphones and contemporary privacy concerns (for example, those linked to the Snowden revelations and Big Data). Furthermore, studies often rely heavily on self-report measures that can be problematic (see: Jensen, Potts, & Jensen, 2005).

A book chapter by Cate (2006) entitled *The Failure of Fair Information Practice Principles* noted that 'an avalanche of notices and consent opportunities […] are widely ignored by the public' (p. 360). To substantiate this assertion Cate cites a 1997 study from the US Postal Service suggesting 52% of unsolicited mail is never read. Cate also refers to data from 2002 whereby an unnamed ISP noted that 58% of its marketing emails remain unopened. The conflation of opening snail mail and marketing emails with privacy and TOS policy engagement is problematic; however, it does highlight the common view that it is challenging to get people to read things they may not want to. Cate goes on to discuss how in 2001 the chief privacy officer of ISP Excite@Home noted during an FTC workshop 'that the day after *60 Minutes* featured his company in a segment on Internet privacy, only 100 out of 20 million unique visitors to its website accessed that company's

privacy pages' (c.f. Cate, 2006, p. 261). Data from Yahoo is then presented noting that an average of 0.3% of users accessed its privacy policy in 2002, with the number rising to 1% during a privacy-publicity 'firestorm.'

Bakos, Marotta-Wurgler, and Trossen (2014) conducted a similar clickstream assessment of more than 48,000 individuals visiting commercial software and freeware sites in January 2007. Results revealed that TOS was generally accessed less than 0.2% of the time with median time spent on the policy page approximately 30 seconds. Among the limitations of the study was that its results did not address the possibility that many users, especially in 2007, were unaware that the services had TOS, knew how to find the terms, as well as understood the implications of ignoring them.

Some of these nuances were addressed in a complementary study by Marotta-Wurgler (2012) of the same data set from January 2007. The study assessed whether individuals accessing services with clickwraps viewed TOS, compared to those that accessed services without. A clickwrap is 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, or completing some other digitally-mediated action suggesting "I agree" or "I don't agree"' (see: Obar and Oeldorf-Hirsch, 2018). Clickwraps are common to SNS, and while they raise political economic concerns about placing users in fastlanes that bypass consent materials, speeding users to monetized sections of services (Obar and Oeldorf-Hirsch, 2018), they at least present a prompt. This differs from the process of placing a link at the margins of a user interface, such as at the bottom of a webpage (Jensen & Potts, 2004), requiring users to think about the link, find the link and click on the link, without being prompted. Marotta-Wurgler's (2012) assessment suggested that clickwraps have little to no impact on users accessing TOS, with only seven of more than 4500 users clicking the clickwrap policy link (the study did not assess user engagement with clickwraps where the policy is presented without first clicking the policy link).

Additional studies that present assessments of reading behaviors include Groom and Calo (2011) where none of the 120 participants clicked on the policy link during engagement with a fictitious search engine, and Good, Grossklags, Mulligan, and Konstan (2007) where a self-report assessment in the context of software installations highlighted that 66% of the 240 participants said they rarely read policies, and 7.7% don't notice policies.

Studies addressing privacy and TOS reading behaviors often employ self-report measures, which have proven problematic when compared with studies of actual behavior (Jensen et al., 2005). Nevertheless, various self-report studies are present in the literature, contributing a wide range of results. Milne and Culnan (2004) suggested that 17.3% of the 2468 individuals surveyed self-reported as 'non-readers,' while 83.7% of those surveyed said they read policies (p. 21). By comparison, Jensen et al. (2005) found only 24% of subjects self-reported that they read policies when first visiting a site, and Fiesler, Lampe, and Bruckman (2016) noted that 11% of participants self-reported that they read TOS.

The challenge with self-reporting, aside from traditional concerns associated with an individual's inability to accurately remember or report their behaviors, is that self-reporting often reveals a privacy paradox, which describes 'a stark contradiction at whose heart is this: people appear to want and value privacy, yet simultaneously appear not to value or want it' (Nissenbaum, 2009, p. 104). The paradox is revealed when people say they want privacy protections, but actions, such as ignoring policies, suggest otherwise (Norberg, Horne, & Horne, 2007).

Overall, much of the research on privacy and TOS policy reading behaviors pre-dates social networking services, smartphones, the Snowden revelations and the Big Data boom. Previous studies utilizing experimental designs tend not to assess social media interfaces, while many others rely on self-report measures.

In this paper, we attempt to address some of these gaps by conducting an experimental survey of the extent to which individuals ignore privacy and TOS policies when engaging social networking services using both a signup scenario involving the front page of a fictitious SNS as well as self-report. The purpose of the self-report is to further assess the extent to which self-reporting can contribute to the understanding of reading behaviors.

We address the following research questions:

RQ1: To what extent will participants ignore privacy and terms of service policies for the fictitious social networking service NameDrop?

RQ2: To what extent will participants fail to notice 'gotcha' clauses in the NameDrop policies?

RQ3: To what extent will participants read privacy and terms of service policies for real social networking services?

RQ4: What attitudes about privacy and terms of service policies predict the extent to which participants ignore them?

Method

Sample

Participants ($N = 543$) consisted of undergraduate students recruited from a large communication class at a public university in the northeastern United States. The sample was 47% female, 45% male (8% not identified), and the average age was 19 years (SD = 1.45). The sample was 62% Caucasian, 15% Asian, 6% Black, 2% Hispanic or Latino/a, 3% mixed race/ethnicity, and 3% another race/ethnicity (9% not reported). All participants received course credit for completing the survey or an alternate assignment.

Procedure

The survey was hosted on Qualtrics in fall 2015 and consisted of two sections: (1) quantitative and qualitative assessments of participant interaction with a privacy and a TOS policy for a fictitious SNS, and (2) a self-report section about reading privacy and TOS policies for real SNS. To complete (1) researchers developed the front page for a fictitious SNS called 'NameDrop' (Figure 1), a hypothetical competitor of LinkedIn. There was no time limit, and participants took an average of 24 minutes to complete the survey.

Section 1: engagement with NameDrop privacy and TOS policies

Participants were informed that their university was 'contributing to a pre-launch evaluation of the site.' This deception aimed to convince participants that the evaluation would involve: signing-up, reviewing the SNS, and deleting their account if desired. At no point was an SNS evaluated.

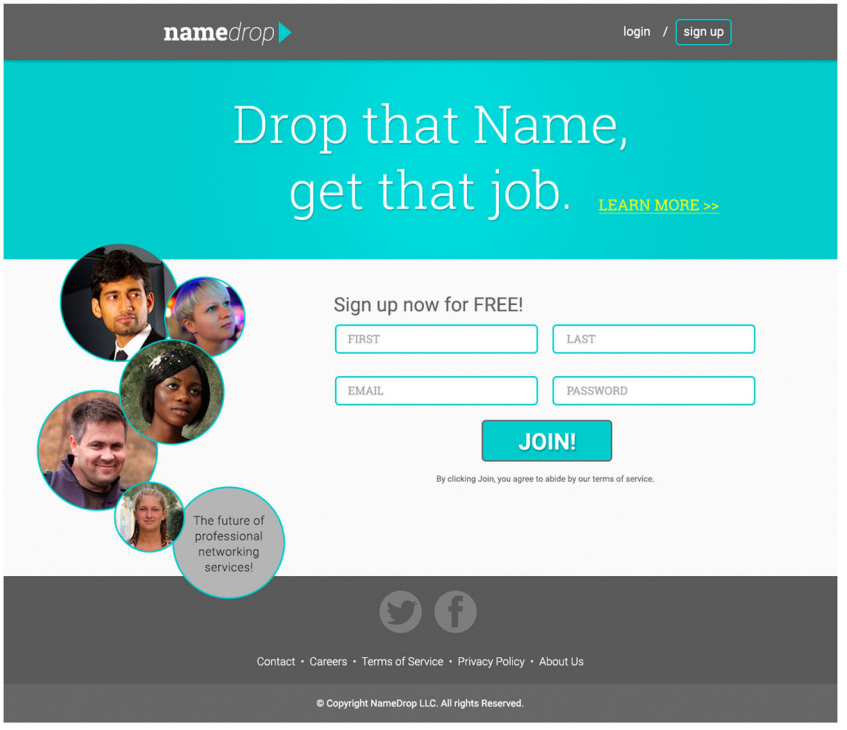

Figure 1. Front page of fictitious SNS 'NameDrop'.

After consenting to the study, participants were presented with NameDrop's front page (Figure 1), and were given a 'quick-join' clickwrap option below the image. This option, common to SNS like Facebook, Twitter, Instagram, and LinkedIn (Obar and Oeldorf-Hirsch, 2018), helps participants join services quickly through the bypassing of consent materials, accepting policies without having to access or read them (Obar and Oeldorf-Hirsch, 2017). Participants could choose 'Sign Up! (By clicking Sign Up, you agree to NameDrop's privacy policy)' or 'Click here to read NameDrop's privacy policy.' If participants declined the clickwrap they were directed to the PP, which they had to read and either accept or reject to continue. Participants were then asked to review NameDrop's TOS. Both policies could be accepted or rejected, and either choice allowed participants to proceed.

Stimuli

The NameDrop policies were modified versions of LinkedIn's to ensure comparable length to current SNS. In addition to assessing accept/reject, the software timed how long participants spent on each policy. The PP measured 7977 words and the TOS 4316 words. The literature suggests that average adult reading speed, for individuals with a grade 12 or college education is approximately 250–280 words per minute (Taylor, 1965). This suggests that it should have taken the average adult between 29 and 32 minutes to read NameDrop's PP and 15 and 17 minutes for TOS.

Two 'gotcha' clauses were added to the TOS to further assess ignoring behavior. The intention was to present clauses so outrageous that concern would be expressed after reading. The first clause dealt with data sharing, the NSA and eligibility determinations:

> **3.1.1 NameDrop Data** […] 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. National Security Agency, 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.

The second clause was more extreme, stating that by agreeing to the TOS, participants would give up their first-born child to NameDrop:

> **2.3.1 Payment types (child assignment clause):** In addition to any monetary payment that the user may make to NameDrop, by agreeing to these Terms of Service, and in exchange for service, all users of this site agree to immediately assign their first-born child to NameDrop, Inc. If the user does not yet have children, this agreement will be enforceable until the year 2050. All individuals assigned to NameDrop automatically become the property of NameDrop, Inc. No exceptions.

Measures

Time spent reading NameDrop TOS and privacy policies. Time spent reading was tracked using Qualtrics' timing option, which reports the number of seconds that participants spent on the policy pages.

NameDrop policy and general clickwrap concerns. After being presented the quick-join clickwrap option, PP, and TOS, participants were asked the following open-ended question: 'Please describe any concerns that you have with the NameDrop Terms of Service Agreement and/or Privacy Policy.' At the end of the survey the NameDrop front page was presented again and participants were asked the following 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.' A coding instrument was utilized to assess the answers to the open-ended questions. Variables 1–5 identified concerns associated with the NameDrop privacy and TOS policies (including data sharing, the NSA, the child assignment clause, the policy length and general concern). Variables 6–7 identified whether quick-join options are utilized often or sometimes. Inter-coder reliability was conducted using two trained coders and responses from 119 participants (22% of total). Holsti's (1969) percentage agreement test revealed inter-coder reliability scores ranging from $p = 0.97$ to $p = 1.00$, with an average across the seven variables of $p = 0.99$. The remaining qualitative responses were assessed employing thematic analysis.

Section 2: self-reported reading of real SNS privacy and TOS policies

Participants then reported on their usual privacy and TOS policy reading behaviors and attitudes.

Measures

Reported time spent reading privacy and TOS policies. Participants were asked how many minutes (on a slider ranging 0–60 minutes) they spent reading privacy and TOS policies for the following services upon signup and again when policies change: Facebook, Twitter, Instagram, Skype, SnapChat, Yik Yak, Xbox Live, iPhone Messenger, Gmail, and iTunes. All provide SNS functionality, except iTunes, which was selected to assess behaviors associated with a different digital service.

Privacy and TOS policy reading behavior. Four matched pairs of items (8 items total) measured participants' PP and TOS reading behavior: 'I agree to privacy policies/Terms of Service agreements without reading them,' 'I skim privacy policies/Terms of Service agreements,' 'I read privacy policies/Terms of Service agreements thoroughly,' and 'I review privacy policies/Terms of Service agreements when notified that there have been updates'. These were measured as 7-point Likert-type scale items (Strongly Disagree – Strongly Agree). For both scales, reliability was improved when the 'I skim' item was removed, resulting in reliable three-item scales for PP ignoring, $\alpha = .78$, and TOS ignoring, $\alpha = .75$.

Privacy and TOS policy attitudes. Sixteen matched pairs of items (32 items total) were developed to measure participants' attitudes toward the policies. These items were factor analyzed using Principal Axis Factoring and Varimax rotation, revealing a three-factor structure. Using a criterion of items loading at .5 or higher on one factor with no cross-loadings of .5 or higher on other factors, 23 items loaded onto the three factors, explaining 42% of the variance. See factor items in Table 1.

Demographics. Participants were asked to indicate their age, gender, and race/ethnicity.

Results

Section 1: engagement with NameDrop privacy and TOS policies

RQ1 was addressed by recording whether participants skipped the NameDrop privacy policy via a 'quick-join' clickwrap option, and then the extent to which they read the privacy policy (for those declining 'quick-join') and TOS policy.

The 'quick-join' clickwrap option

Upon encountering the quick-join clickwrap option for the NameDrop PP, 399 of 543 participants (74%) accepted the option and skipped reading the PP entirely. This means that these participants accepted NameDrop's PP without accessing, viewing, or reading any part of it.

To expand upon this finding, responses to open-ended questions about quick-join clickwraps were assessed. From the 527 participants that provided qualitative responses, 411 (78%) said they use quick-join clickwraps often. Of the remaining participants, 17 suggested that they sometimes quick-join. Removing responses labeled 'unclear' (most of these were critical of the process of reading policies but didn't answer the question), more than 90% of those surveyed said they use quick-join options often or sometimes, with the vast majority using them often.

Participants noting that they often use quick-join clickwraps usually provided an explanation. An overarching theme present in many of the responses suggests that participants

Table 1. Policy attitudes factor analysis.

Items	Factors and item loadings		
	Information overload	Nothing to hide	Difficult to understand
Privacy policies are too long	**.819**	.093	.088
There are too many privacy policies to read	**.802**	.149	.086
There are too many terms of service agreements to read	**.732**	.093	.086
Terms of service agreements are too long	**.720**	.048	.073
I don't have time to read privacy policies for every site that I visit	**.630**	.203	.178
I don't have time to read terms of service agreements for every site that I visit	**.609**	.161	.177
It is normal to sign up for websites/apps without reading the terms of service agreements	**.593**	.145	.110
It is normal to sign up for websites/apps without reading the privacy policies	**.556**	.160	.153
Most people don't read terms of service agreements	**.539**	.086	−.050
Most people don't read privacy policies	**.526**	.119	−.022
Most people don't understand terms of service agreements	.455	.010	.428
I don't have time to read privacy policies	.445	.219	.195
I don't have time to read terms of service agreements	.420	.219	.241
I am not doing anything wrong, so what privacy policies say doesn't matter	.179	**.776**	−.029
I am not doing anything wrong, so what terms of service agreements say doesn't matter	.217	**.714**	−.044
The only users seriously affected by privacy policies are people who break the rules	.150	**.634**	−.149
Companies will never bother you whether you read their privacy policies or not	.115	**.626**	.042
Companies will never bother you whether you read their terms of service agreements or not	.127	**.581**	.000
The only users seriously affected by terms of service agreements are people who break the rules	.097	**.532**	−.215
I've got nothing to hide (privacy policies)	.269	**.517**	−.167
I've got nothing to hide (terms of service)	.250	**.501**	−.178
Companies will do what they want, regardless of whether I read the privacy policies	.096	.499	.188
It's important to read terms of service agreements to avoid trouble	−.007	−.483	−.252
It's important to read privacy policies to avoid trouble	.090	−.483	−.275
Companies will do what they want, regardless of whether I read the terms of service agreements	.096	.426	.129
The language in privacy policies is clear	−.133	.120	**−.711**
The language in terms of service agreements is clear	−.152	.133	**−.693**
Privacy policies are difficult to understand	.403	−.041	**.575**
Terms of service agreements are difficult to understand	.437	−.069	**.537**
Most people don't understand privacy policies	.429	−.003	**.511**
Privacy policies provide helpful information	.100	−.355	−.450
Terms of service agreements provide helpful information	−.030	−.278	−.440

are generally uninterested in the notice component of SNS. The quick-join clickwrap was often praised for making the notice process 'easy,' 'quick,' 'simple,' and 'convenient.' One participant noted, 'it expedites the process.' Participants were critical of the policies themselves, suggesting that they are 'too long' and 'wordy.' Feelings of apathy as well as futility were common, with the latter sometimes linked to the perception that policies wouldn't be understood even if they were read.

Expanding upon the 'quick' and 'easy' comments was the suggestion that participants are disinterested in the notice process because it is perceived as an unwanted and/or unnecessary barrier between the user and the desired SNS experience. One participant justified using the quick-join clickwrap by saying, 'regardless of the policy, if a mass majority

of my friends and family are on the networking site I want to be included as well in order to interact with them.' Another noted, 'my friends use this social media in oder [*sic*] to catch up with their life i [*sic*] signup for this as quick as possible.' Indeed, the desire to enjoy the ends of digital media production without being inhibited by the means was clear, with one participant noting 'I'm in a hurry to use the service,' while another said 'its a hassle to deal with a massive amount of boring pages about privacy and security when the site you are joining is there to do something much more interesting.' Indeed, the perception that these attitudes are the norm was acknowledged, 'it feels like a cultural norm not to read them and I'm too lazy to read them in detail.'

Reading or ignoring NameDrop policies

The average adult reading speed for individuals with a grade twelve or college education is approximately 250–280 words per minute (Taylor, 1965). This suggests that it should take between 29 and 32 minutes to read the NameDrop PP (7977 words). For those who read the PP (the 26% who did not skip it using the quick-join clickwrap option), the actual time spent reading ranged from 2.96 seconds to 2220.67 seconds (37 minutes), with a median of 13.60 seconds ($M = 73.72$, SD = 237.26). As noted in Figure 2, 81% of these participants spent less than one minute reading the NameDrop PP, with an additional 15% reading for less than five minutes.

The NameDrop TOS was 4316 words, suggesting it should take 15–17 minutes to read. Participant reading times ranged between 3.48 seconds and 6699.35 seconds (111 minutes) with a median of 14.04 seconds ($M = 51.12$ seconds, SD = 297.93). Similar to the PP, 86% of participants spent less than one minute reading the TOS, with an additional 12% spending less than five minutes (Figure 2). In sum, of participants that accessed the NameDrop policies (i.e. didn't select the clickwrap) 96% spent less than 5 minutes on the PP and 98% spent less than 5 minutes on the TOS.

The 'gotcha' clauses in the NameDrop terms of service policy

RQ2 was assessed by coding open-ended responses about NameDrop's privacy and TOS policies for any mention of the 'gotcha' clauses. Responses revealed that just 83

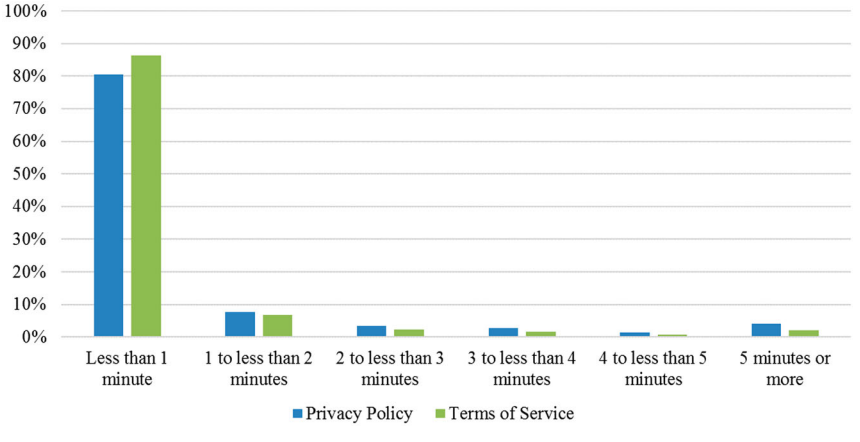

Figure 2. Time spent reading NameDrop privacy policy and terms of service.

participants (15%) had concerns about the policies. Of those, 9 (1.7% of those surveyed) mentioned the child assignment clause and 11 (2%) mentioned concerns with data sharing; however, only one of the 11 mentioned the NSA. The remainder of the comments dealt with a variety of concerns including the length of the policies, and the trustworthiness of the SNS.

A number of participants did not agree to the NameDrop policies.[1] Seventeen individuals that did not select the clickwrap did not agree to the PP. A total of 37 individuals (7% of sample) did not accept the TOS. Seven of the nine participants who identified the child assignment clause and the one participant who identified the NSA mention were among those that declined the TOS. On average, these individuals spent significantly more time reading the TOS ($M = 150.81$ seconds, SD = 220.05), $t(540) = -2.77$, $p < 0.01$) than those who did accept it ($M = 43.81$, SD = 301.72). Those who did not accept the PP also spent more time reading the policy ($M = 102.30$, SD = 115.51) than those who did access and accept it ($M = 69.89$, SD = 249.14), but this difference was not statistically significant.

Section 2: self-reported reading of real SNS privacy and TOS policies

RQ3 was addressed by averaging reported time spent reading the TOS and PP for various services when participants signed up and when policies change. Thirty-nine percent of participants stated they never read TOS agreements for any of the services assessed when signing up. For each given service, 52–65% stated that they ignored the TOS completely (spent zero minutes reading it) when signing up. For those that do read policies, reported time spent ranged from 1 minute to 43 minutes ($M = 4.68$, Median = 2.00).

Reading times for privacy policies showed a similar pattern. Thirty-five percent of participants acknowledged not reading the PP for any of the services when signing up. For any given service, 42–67% ignored the PP when signing up. Reported time spent reading ranged from 1 minute to 60 minutes ($M = 4.91$, Median = 2.35). Reading patterns when TOS and privacy policies change were similar.

What predicts time spent reading policies

The factor analysis revealed three attitude factors. The first, *Information overload* (10 items, $\alpha = .90$), contained items about participants perceiving TOS and privacy policies as being too long, too numerous, and taking up too much time. The second factor, *Nothing to hide* (8 items, $\alpha = .87$), drawing on Solove (2007) expressed the idea that the individual in question perceives that policies are irrelevant because the individual is doing nothing wrong, companies will not bother them, and only those who are breaking the rules are affected. The third factor, *Difficult to understand* (5 items, $\alpha = .85$), indicated that individuals perceive that they are unable to understand the language in TOS and privacy policies (Table 1).

To answer RQ4, these factors were entered into a hierarchical regression model for the four outcomes: reported average time spent reading TOS and privacy policies when signing up for a service and when the TOS and privacy policies change. The models included age and gender as control variables in block 1, reported TOS and PP reading behavior in block 2, and the three attitude factors in block 3. See final models in Table 2.

Of the three factors, information overload was a significant negative predictor of reading TOS when signing up, $\beta = -.17$, $p < 0.01$, and of reading TOS when they change, $\beta =$

Table 2. Final regression models predicting time spent reading terms of service and privacy policies upon signup and when policies change.

	Terms of service						Privacy policies					
	Upon sign up			When they change			Upon sign up			When they change		
	B	SE *B*	*β*	*B*	SE *B*	*β*	*B*	SE *B*	*β*	*B*	SE *B*	*β*
Age	.39	.16	.09*	−.07	.14	−.02	−.08	.18	−.02	−.22	.16	−.06
Gender	.19	.47	.02	−.05	.42	−.01	−.06	.52	−.01	−.46	.46	−.04
TOS reading	2.14	.31	.40***	1.57	.28	.37***	1.60	.34	.29***	1.36	.31	.28***
PP reading	.21	.29	.04	.09	.26	.02	1.19	.32	.24***	.62	.28	.14*
Information overload	−1.35	.41	−.17**	−1.54	.36	−.24***	−.40	.46	−.05	−1.54	.40	−.22***
Nothing to hide	.15	.22	.03	.23	.19	.06	−.01	.24	−.00	.17	.22	.04
Difficult to understand	.23	.22	.05	.29	.19	.07	−.05	.24	−.01	.24	.21	.05
Model R^2	.30***			.27***			.27***			.27***		

*$p < 0.05$.
**$p < 0.01$.
***$p < 0.001$.

−.24, $p < 0.001$. For privacy policies, information overload was a significant negative predictor of reading privacy policies when they change, $\beta = -.22$, $p < 0.001$, but not when signing up for a new service, $\beta = -.05$, $p = 0.38$. The more individuals experience information overload regarding TOS and PP, the less time they reportedly spent reading TOS when signing up, TOS when they change, and privacy policies when they change. Participants' attitudes that they have nothing to hide and that policies are difficult to understand did not predict reported reading behavior for TOS or privacy policies. That is, while individuals may hold these beliefs, they have no effect on reported reading behavior.

Discussion

The results of this study suggest that individuals often ignore privacy and TOS policies for social networking services. This behavior appears to be common both when signing up for new services and when policies change for services individuals are already using. When people do read policies, they often remain on the relevant pages just long enough to scroll to the 'accept' button, and in the few instances where detailed reading takes place, almost all participants demonstrate reading times far below the average reading time needed. It should be kept in mind that the participants described herein are communication students who study privacy, surveillance and Big Data issues in class. If communication scholars-in-training cannot be bothered to read SNS policies, let alone demonstrate concern about the implications of ignoring notice opportunities, it seems likely that the general public would commonly ignore policies as well. Perhaps there is some truth to the 'biggest lie on the internet' anecdote.

This study attempts to build on the previous literature emphasizing a tendency to ignore policies when engaging online (e.g., Bakos et al., 2014; Cate, 2006; Good et al., 2007; Marotta-Wurgler, 2012), with a unique empirical assessment of individuals interacting with the privacy and TOS policies of what they believe to be a real SNS. Even though none of the participants had heard of the service before, and none had any friends or family members to vouch for its quality, most of the participants agreed to NameDrop's PP without even looking at it. Students may have placed their trust in the university's vetting of the service, and therefore did not consider the policies as closely as they may have otherwise. They also were not asked to actually use the site, but only to evaluate it briefly for the study. While it is possible that without these potential confounds, a higher percentage might have read the policies, the self-report and qualitative data suggest otherwise. As participants were undergraduate students from a public northeastern US university, the sample is not representative. While it may be the case that this population is less-likely to read policies, the literature suggests that age may not be associated with this type of ignoring behavior (e.g.: Jensen, et al., 2005).

The role of the clickwrap in facilitating policy acceptance is worth emphasizing. Of the 543 individuals surveyed, 74% accepted the privacy policy via the quick-join clickwrap option which allowed participants to by-pass the policy without even requiring a glimpse. Qualitative responses suggest that 78% of individuals often use the quick-join clickwrap option and more than 90% use it often or sometimes. These findings raise political economic concerns about the role SNS providers play in facilitating (or circumventing) consent

processes and delivering (or impeding) privacy and reputation protections. As was noted in a related study:

> (clickwraps) maintain flow to monetized sections of services, while diverting attention from policies that might encourage dissent. Clickwraps accomplish this through an agenda-setting function whereby prompts encouraging circumvention are made more prominent than policy links. Results emphasize that clickwraps discourage engagement with privacy and reputation protections by suggesting that consent materials are unimportant, contributing to the normalization of this circumvention. (Obar and Oeldorf-Hirsch, 2018)

This suggests that the implementation of clickwraps by SNS providers contributes to ignoring behaviors. Clickwraps feed the desire to pursue the ends of digital production as quickly as possible, while facilitating fastlanes to monetized sections of services and the maintenance of the status quo. More research is needed to address clickwrap alternatives that will help users realize desired SNS affordances, while also ensuring engagement with consent materials.

Even when participants do not bypass policies, the vast majority barely spends any time reading them. Most appear to take a quick look and then simply scroll to the bottom to click 'accept.' The NameDrop PP, which was the same length as LinkedIn's policy at the time the study was completed, should have taken more than half an hour to read; the TOS, more than 15 minutes. Some engaging with NameDrop's privacy and TOS policies spent two and three seconds on the policies, respectively. The average reading time across participants for the PP was 74 seconds, and 51 seconds for the TOS. Though these averages demonstrate reading times well below the time required, the averages were skewed by a few outliers. The median for both privacy and TOS policies is a more accurate representation of the general trend, at approximately 14 seconds for both. Fourteen seconds is hardly enough time to read, understand and provide informed consent to policies between 4000 and 8000 words in length. Spending 14 seconds (or 60 seconds for that matter) is akin to not reading the policies at all. Said another way, of those that read the PP, 81% spent less than a minute reading, and 96% less than five minutes. Eighty-six percent of participants spent less than a minute reading the TOS, 98% less than five minutes.

Though 97% of participants agreed to the PP and 93% agreed to the TOS, it is important to focus attention on the small percentage that did not agree. These individuals, on average, spent more time reading: 30 seconds more reading the PP (the longer of the two documents), and 90 seconds longer reading the TOS. Almost all of the individuals that found the child assignment clause and the one that noticed the NSA mention declined the TOS. Though the average reading times for those that declined were still far below what average reading speeds require, which suggests that these individuals might have declined the policies under any circumstances, it must be emphasized that longer reading times were associated with identifying the gotcha clauses as well as the decision to decline the policies.

When asked about engaging with policies for Facebook, Twitter, Instagram, Skype, SnapChat, Yik Yak, Xbox Live, iPhone Messenger, Gmail, and iTunes, 35–39% said they ignore policies. Of those that read, the average time reported was about five minutes, with the median approximately two minutes. Though iTunes is not an SNS at the moment, it was revealing to see that the tendency to ignore policies goes beyond SNS engagement

and includes other digital media services. This suggests again that, as one participant noted, 'it feels like a cultural norm not to read (policies).' These results support previous assertions that individuals are habituated to quickly accepting tangential consent prompts when engaging with services online (Böhme & Köpsell, 2010).

The privacy paradox

While almost all participants demonstrated that they either ignore or pay insufficient attention to the policies, the slight differences in reading time between the NameDrop analysis and the self-report analysis support previous concerns about the inaccuracies associated with self-report measures (Jensen et al., 2005) and also hint at a privacy paradox. The paradox suggests that when asked, individuals appear to value privacy, but when behaviors are examined, individual actions suggest that privacy is not a high priority (Nissenbaum, 2009; Norberg et al., 2007). To a small degree, this is what was revealed by the analysis. When participants were asked to self-report their engagement with privacy and TOS policies, results suggested average reading times of approximately five minutes. The NameDrop analysis, which tested actual engagement with SNS policies upon signup revealed average reading times around one minute, with medians of 14 seconds.

Pursuing the ends of digital production without being inhibited by the means

It is important to consider privacy paradox findings in combination with the attitudinal and qualitative analyses. These analyses suggest a similar finding, that the majority of participants see notice components as nothing more than an unwanted impediment to the real purpose users go online – the desire to enjoy the ends of digital production (i.e., accessing SNS). The only predictor found was a concern over information overload, which included concerns such as 'Privacy policies are too long,' 'There are too many privacy policies to read,' and 'I don't have time to read Terms of Service agreements for every site that I visit.' Privacy and TOS policies were seen as more of a nuisance than anything else.

The qualitative assessment reinforced this finding. While a small minority of participants did express privacy concerns, the vast majority praised quick-join clickwrap options for helping them by-pass notice components. It's not just that privacy and TOS policies are perceived as boring or even pointless, it's that users are going online and engaging with SNS to complete a list of desired tasks, namely, engaging with friends and family online, and all of the other affordances offered by SNS. As one participant noted, 'my friends use this social media in oder [*sic*] to catch up with their life i [*sic*] signup for this as quick as possible' while another said 'its a hassle to deal with a massive amount of boring pages about privacy and security when the site you are joining is there to do something much more interesting.'

It is clear that getting into a tangential legal discussion or even education about data sharing, the NSA and privacy in general is far from the reason that individuals choose to go online. Solove (2012) appropriately analogizes engagement with policies to the process of students receiving homework. Challenges arise when multiple teachers assign too much reading, creating a problematic scenario for ensuring the work is completed. While this analogy correctly describes one of the problems associated with achieving data privacy

self-management across all entities involved in data management, the analogy highlights a point more relevant to the current analysis. Users aren't looking for homework when they go online, quite the contrary, it is likely that many users are looking for an escape from their homework when accessing SNS. Users want to engage with the ends of digital production, without being inhibited by an education or a discussion about the means.

The negative implications of this behavior were suggested by the 'gotcha clause' analysis. Instead of notice components helping users control their digital destinies and corresponding consequences in both online and offline contexts, the vast majority of participants completely missed a variety of potentially dangerous and life-changing clauses. As noted in the first gotcha clause, data could be shared 'with government agencies, including the U.S. National Security Agency, and other security agencies in the United States and abroad.' Furthermore, data could be shared '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.' These data sharing possibilities are real, and raise a host of expanding concerns associated with data collection and use (see: Lyon, 2002; Madden et al., 2017; Pasquale, 2015). Furthermore, TOS often address legal relationships with users that go well-beyond issues of privacy.

Not caring about notice is relevant to Solove's (2007) critique of the 'I've got nothing to hide' argument. A common justification for privacy disinterest, this fallacy incorrectly assumes, as one participant in this study noted when justifying clickwrap use, 'Nothing too bad happened yet, but it's not like I post anything interesting or worthy.' By dismissing responsibility in order to get to the enjoyment of SNS, those who demonstrate Solove's fallacy ignore a variety of possible implications. As Solove notes,

> it is hard to claim that programs […] will not reveal information people might want to hide, as we do not know precisely what is revealed. […] data mining aims to be predictive of behavior, striving to prognosticate about our future actions. People who match certain profiles are deemed likely to engage in a similar pattern of behavior. It is quite difficult to refute actions that one has not yet done. Having nothing to hide will not always dispel predictions of future activity. (p. 766)

Not only is future behavior difficult to predict, so too are the future uses and concerns associated with the Big Data industry. This is precisely the reason we included the child assignment clause in this study, which more than 93% of participants accepted and more than 98% of participants missed. What could be worse than a corporation taking your child away in payment for use of their services? Being ignorant or resigned to the trade-offs associated with digital media usage (see: Turow, Hennessy, & Draper, 2015) is unacceptable if we are to protect ourselves from potential implications now and in the future.

The policy implications of these findings contribute to the community of critique suggesting that notice and choice policy is deeply flawed, if not an absolute failure (Obar, 2015; Nissenbaum, 2011; Reidenberg, Breaux et al., 2015; Solove, 2012). Transparency is a great place to start, as is notice and choice policy; however, all are terrible places to finish. They leave digital citizens with nothing more than an empty promise of protection, an impractical opportunity for data privacy self-management, and as Solove (2012)

analogizes, too much homework. This doesn't even begin to address the challenges unique to children in the realm of digital reputation, as if there is little hope for adults, what chance is there for children to protect themselves?

It is worth noting that this study is being completed at a time when there is considerable debate about the future of consent processes online. The Cambridge Analytica scandal has raised questions about the implications of Facebook's role in facilitating user consent processes which may or may not have contributed to the data leak of, allegedly, 87 million user accounts (Kang & Frenkel, 2018, April 4). The consent debate is also amplified by the European Union's General Data Protection Regulation (GDPR), which is going into effect in 2018. The GDPR aims to give citizens of the EU greater control over their data and over consent processes, within and outside of the EU. Attempts to promote engagement with consent processes are associated with GDPR requirements that consent materials be easier to understand and use. While the regulation encourages services to do more to engage users in these processes, Section 32 of the regulation does note 'This could include ticking a box when visiting an internet website' (EU, 2016, p. 6), and the mechanism must not be 'unnecessarily disruptive to the use of the service for which it is provided' (EU, 2016). The former suggests that clickwraps are still acceptable, and the latter acknowledges that users are uninterested in tangential privacy debates when accessing services. Overall this suggests that while elements of the current discussion provide reasons for optimism, notice still equals nuisance, and more needs to be done to discover pragmatic alternatives that actually produce privacy and reputation deliverables (see: Obar, 2015). Indeed, if governments continue to cling to romantic ideals and fallacy, the internet's biggest lie will surely move from anecdote to liability.

Acknowledgements

Thank you to Valeta Wensloff for your wonderful work on the NameDrop front page. Thank you also to Afifah Khawaja for your research assistance.

Note

1. In an earlier working version of the manuscript posted online, this section included a data analysis error. The earlier version incorrectly noted that 100% of participants agreed to both the privacy and TOS policies. This was discovered and addressed during the peer review process.

Disclosure statement

No potential conflict of interest was reported by the authors.

Notes on contributors

Jonathan A. Obar (PhD, The Pennsylvania State University) is an Assistant Professor in the Department of Communication Studies at York University. He also serves as a Research Associate with the Quello Center at Michigan State University. His research focuses on information and communication policy, and the relationship between digital technologies, civil liberties and the inclusiveness of public culture [email: jaobar@yorku.ca].

Anne Oeldorf-Hirsch (PhD, The Pennsylvania State University) is an Assistant Professor in the Department of Communication at the University of Connecticut. Her research focuses on information sharing as a form of communication in online social networks. Specifically, her work investigates the effects of social media activities such as news discussion, content sharing, and self-disclosure on outcomes such as engagement, learning, and well-being [email: anne.oeldorf-hirsch@uconn.edu].

ORCID

Anne Oeldorf-Hirsch http://orcid.org/0000-0002-3961-3766

References

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.org/10.1086/674424

Biggestlie.com. (2018). Let's stop the biggest lie on the web! www.biggestlie.com.

Böhme, R., & Köpsell, S. (2010). Trained to accept? A field experiment on consent dialogs. *Proceedings of the SIGCHI conference on human factors in computing systems*, ACM (pp. 2403–2406). doi:10.1145/1753326.1753689.

Cate, F. H. (2006). The failure of fair information practice principles. In J. K. Winn (Ed.), *Consumer protection in the age of the information economy* (pp. 343–379). Surrey: Ashgate Publishing.

DeNardis, L., & Hackl, A. M. (2015). Internet governance by social media platforms. *Telecommunications Policy*, *39*(9), 761–770. doi:10.1016/j.telpol.2015.04.003

Department of Commerce. (2010). *Commercial data privacy and innovation in the internet economy: A dynamic policy framework*. Washington, DC: Department of Commerce Internet Policy Task Force.

DR. (2018). Terms of service; didn't read. https://tosdr.org.

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. Retrieved from http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&qid=1490179745294

Federal Trade Commission. (1998). *Privacy online: A report to congress* (pp. 1–71). Washington, DC: Federal Trade Commission. June.

Federal Trade Commission. (2012). Protecting consumer privacy in an era of rapid change. Federal Trade Commission Report.

Fiesler, C., Lampe, C., & Bruckman, A. S. (2016). Reality and perception of copyright terms of service for online content creation. *Proceedings of the 19th ACM conference on computer-supported cooperative work & social computing* (pp. 1450–1461). ACM. doi:10.1145/2818048.2819931

Good, N. S., Grossklags, J., Mulligan, D., & Konstan, J. A. (2007). Noticing notice: A large-scale experiment on the timing of software license agreements. *Proceedings of the SIGCHI conference on human factors in computing systems* (pp. 607–616). ACM. doi:10.1145/1240624.1240720

Groom, V., & Calo, R. (2011). Reversing the privacy paradox: An experimental study. Paper presented at TPRC 2011, Arlington, VA.

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

Jensen, C., & Potts, C. (2004). Privacy policies as decision-making tools: An evaluation of online privacy notices. *Proceedings of the SIGCHI conference on human factors in computing systems* (pp. 471–478). ACM. doi:10.1145/985692.985752

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), 203–227. doi:10.1016/j.ijhcs.2005.04.019

Kang, C., & Frenkel, S. (2018, April 14). Facebook says Cambridge Analytica harvested data of up to 87 million users. *New York Times*. https://www.nytimes.com/2018/04/04/technology/mark-zuckerberg-testify-congress.html

Leibowitz, J. (2007, November 1). *So private, so public: Individuals, the internet & the paradox of behavioral marketing*. Remarks at FTC town hall meeting on 'behavioral advertising: Tracking, targeting & technology'.

Lyon, D. (2002). Everyday surveillance: Personal data and social classifications. *Information, Communication & Society*, *5*(2), 242–257. doi:10.1080/13691180210130806

Madden, M., Gilman, M. E., Levy, K. E. C., & Marwick, A. E. (2017). Privacy, poverty and big data: A matrix of vulnerabilities for poor Americans. *Washington University Law Review*, *95*(1), 53–125.

Marotta-Wurgler, F. (2012). Does contract disclosure matter? *Journal of Institutional and Theoretical Economics*, *168*(1), 94–119. doi:10.1628/093245612799440122

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*, 540–565.

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

Morgan, J. (2014, August 19). Privacy is completely and utterly dead, and we killed it. *Forbes*. Retrieved from https://www.forbes.com/sites/jacobmorgan/2014/08/19/privacy-is-completely-and-utterly-dead-and-we-killed-it/

Nissenbaum, H. (2009). *Privacy in context: Technology, policy, and the integrity of social life*. Redwood City, CA: Stanford University Press.

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*, *2015*, 1–16. doi:10.1177/2053951715608876.

Obar, J. A., & Oeldorf-Hirsch, A. (2017). Clickwrap impact: Quick-join options and ignoring privacy and terms of service policies of social networking services. In *Proceedings of the 8th International Conference on Social Media & Society*. New York: ACM.

Obar, J. A., & Oeldrof-Hirsch, A. (2018). The clickwrap: A political economic mechanism for manufacturing consent on social media. *Social Media and Society*.

OECD. (1980). *OECD guidelines on the protection of privacy and transborder flows of personal data*.

Office of the Privacy Commissioner of Canada. (2017). *2016–2017 annual report to parliament on the personal information protections and electronic documents act*.

Pasquale, F. (2015). *The black box society: The secret algorithms that control money and information*. Cambridge, MA: Harvard University Press.

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.

Reidenberg, J. R., Russell, N. C., Callen, A. J., Qasir, S., & Norton, T. B. (2014). Privacy harms and the effectiveness of the notice and choice framework. Paper presented at TPRC 2014, Arlington, VA.

Reidenberg, J. R., Russell, N. C., Callen, A. J., Qasir, S., & Norton, T. B. (2015). Privacy harms and the effectiveness of the notice and choice framework. *I/S A Journal of Law and Policy for the Information Society*, *11*(2), 485–524.

Sanders, S. D. (2011). Privacy is dead: The birth of social media background checks. *Southern University Law Rev*, *39*, 243–264.

Solove, D. J. (2007). 'I've got nothing to hide' and other misunderstandings of privacy. *San Diego Law Review*, *44*, 745–772.

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

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

Turow, J., Hennessy, M., & Draper, N. (2015). *The tradeoff fallacy: How marketers are misrepresenting American consumers and opening them up to exploitation*. Philadelphia, PA: Annenberg School for Communication, University of Pennsylvania.

White House. (2014). *Big data: Seizing opportunities, preserving values*. Washington, DC: Executive Office of the President.