


## RESEARCH ARTICLE

# The surprising power of a click requirement: How click requirements and warnings affect users' willingness to disclose personal information

Robert Epstein <sup>\*</sup>, Vanessa R. Zankich

American Institute for Behavioral Research and Technology, Vista, California, United States of America

<sup>\*</sup> [re@aibr.org](mailto:re@aibr.org) OPEN ACCESS

**Citation:** Epstein R, Zankich VR (2022) The surprising power of a click requirement: How click requirements and warnings affect users' willingness to disclose personal information. PLOS ONE 17(2): e0263097. <https://doi.org/10.1371/journal.pone.0263097>

**Editor:** Marco Cremonini, Università degli Studi di Milano, ITALY

**Received:** October 20, 2021

**Accepted:** January 11, 2022

**Published:** February 18, 2022

**Copyright:** © 2022 Epstein, Zankich. This is an open access article distributed under the terms of the [Creative Commons Attribution License](https://creativecommons.org/licenses/by/4.0/), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

**Data Availability Statement:** An anonymized version of the data can be accessed at <https://doi.org/10.5281/zenodo.5847375>. Data can also be requested from [info@aibr.org](mailto:info@aibr.org). The data have been anonymized to comply with requirements of the sponsoring institution's Institutional Review Board (IRB). The IRB granted exempt status to this study under HHS rules because (a) the anonymity of participants was preserved and (b) the risk to participants was minimal. The IRB also exempted this study from informed consent requirements (relevant HHS Federal Regulations 45 CFR 46.101).

## Abstract

What kinds of information and alerts might cause internet users to be more cautious about what they reveal online? We used a 25-item survey to determine whether the strength of Terms of Service (TOS) warnings and the inclusion of a click requirement affect people's willingness to admit to engaging in inappropriate behaviors. A racially and ethnically diverse group of 1,500 people participated in the study; 98.3% were from the US and India and the remainder from 18 other countries. Participants were randomly assigned to five different groups in which warnings and click requirements varied. In the control condition, no warning was provided. In the four experimental groups, two factors were varied in a 2 × 2 factorial design: strength of warning and click requirement. We found that strong warnings were more effective than weak warnings in decreasing personal disclosures and that click requirements added to the deterrent power of both strong and weak warnings. We also found that a commonly used TOS warning has no impact on disclosures. Participants in the control group provided 32.8% more information than participants in the two click requirement groups combined and 24.3% more information than participants in the four experimental groups combined. The pattern according to which people dropped out of the five different groups sheds further light on the surprising power of the click requirement, as well as on the importance of tracking attrition in online studies.

## 1. Introduction

Companies and governments are now collecting vast amounts of personal information online every day, and more people are becoming aware of how extensively they are being monitored. Relatively few people, however, are aware of the range of ways in which their private information is being used [1]. Some US states require immediate warnings when telephone conversations are monitored or recorded, presumably to give callers the option of moderating their speech, and research on cigarette warning labels suggests that salient warnings help some consumers behave more prudently [2]. What kinds of privacy-related warnings might cause internet users to be more cautious about what they reveal online?

(b)(2), 45 CFR 46.116(d), 45 CFR 46.117(c)(2), and 45 CFR 46.111).

**Funding:** The author(s) received no specific funding for this work.

**Competing interests:** The authors have declared that no competing interests exist.

People are becoming increasingly concerned about surveillance driven by new technologies. The National Security Agency (NSA) is a US intelligence and defense agency that specializes in cryptology and information assurance [3]. In 2013, whistleblower Edward Snowden alerted the American public about the NSA's pervasive surveillance of US citizens, a move that resulted in an increase in disapproval of government surveillance, heightened concerns about technology use, and a reduction in visits to websites that government agencies might be monitoring closely [4, 5]. A year after Snowden's disclosures, the Pew Research Center found that only 9% of American adults reported thinking that they have a high degree of control over how their data are being used, and only 6% reported confidence in the privacy and security of their data [1, 6, 7].

Most parents are also concerned about their children's online behavior [8], and 61% report worrying that their teens are disclosing too much personal information online [9]. Meanwhile, teens are now sharing more information about themselves online than they have in the past, with only 9% of teen social media users reporting being "very concerned" about third-party access to their data [10]. In addition, adolescents' concerns about online privacy are not associated with actual willingness to disclose, meaning that those who do express privacy concerns are not necessarily engaging in more privacy-protective behavior [11].

## 2. Privacy protections, threats, and behavior

### 2.1 Privacy protections outside the tech industry

Government often steps in to protect consumer data and soothe privacy concerns. Some US states require "dual consent" in phone calls, meaning that all participants on a call must be fully aware that the call is being monitored or recorded [12]. The US Federal Trade Commission (FTC) requires that any information provided by businesses that might affect consumers' behavior must be accurate [13]. There also exist laws in the US—so-called "Peeping Tom Laws"—that make it a misdemeanor to spy on or photograph someone in a private place without that person's consent [14]. These laws also prohibit nonconsensual video surveillance, or "video voyeurism," in places where there is a reasonable expectation of privacy (e.g., bathrooms, bedrooms, changing rooms, etc.).

The US Privacy Act of 1974 protects records collected by the US government that contain citizens' personal identifiers, including names and social security numbers [15]. The Privacy Act also states that individuals have the right to seek access to and request correction of any such records about them and prohibits collection and disclosure of such records without the consent of the individual to whom the records pertain. The US Fair Credit Reporting Act of 1970 holds credit reporting businesses responsible for the accuracy and security of personal information that is collected about consumers and then shared with third parties [16]. The US Gramm-Leach-Bliley Act of 1999 protects financial nonpublic personal information by requiring financial institutions to clearly and conspicuously explain their privacy practices and to safeguard any sensitive data they possess [17].

Healthcare records in the US are protected by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and other privacy laws that require healthcare providers to acquire patients' written consent before disclosing their sensitive health information to other people and organizations [18, 19].

### 2.2 Privacy constraints on tech companies

The US Children's Online Privacy Protection Act (COPPA) of 1998 was intended to protect the personal information of children 12 and under by prohibiting online companies from asking for any of their personally identifiable information without parental consent [20].

But technology companies that have emerged worldwide over the past two decades are largely unregulated, and it is only recently that a few aggressive laws and regulations have been implemented that attempt to safeguard consumer privacy. The most ambitious law passed so far is the European Union's General Data Protection Regulation (GDPR), which became effective in 2018. Among other things, the GDPR guarantees, at least in theory, that consumers can have their personal data erased, can find out how their personal data are being used, and can shift their data to other platforms [21]. As a practical matter, however, it is not clear that the GDPR has actually changed pervasive business practices or has benefitted consumers, and some evidence suggests that because of the regulatory burden the GDPR presents, it has hurt small companies and startups in Europe while benefitting the Big Tech companies [22]. Meanwhile, several countries outside the EU have implemented similar regulations, and so has the US state of California [23]. More limited data privacy laws have been enacted by the US states of Nevada and Maine [24, 25].

Unfortunately, most if not all of the new and upcoming privacy rules give tech companies free rein when they have the consent of users, and users often have no idea they have given such consent [26–28]. Few users have ever fully read a Terms of Service (TOS) agreement or Privacy Policy, and tech companies often find ways around the rules [29–32]. “When you use our services,” begins Google's 3,000-word Privacy Policy, “you're trusting us with your information” [33]. A link to that Privacy Policy is embedded in Google's 1,900-word Terms of Service Agreement [34]. Unfortunately, people are agreeing to the terms of both of these agreements even if they don't know they are using a Google service, which is the case most of the time. Millions of websites incorporate Google Analytics, for example, which helps website owners track visitors to their sites [35]. But Google Analytics is invisible to users. Its presence on a website, however, allows Google to track everything users do on that website. Users have inadvertently given their consent when they have unknowingly started using a Google service, and that makes the GDPR and similar regulations largely ineffectual.

### 2.3 Other tech threats to privacy

Implied consent is just one of many privacy problems that new technologies pose. Because fortunes can be made quickly with newly deployed computer code, most new code is poorly written, which often means it is vulnerable to hacking and infiltration [36]. This puts users' sensitive information, including login credentials, healthcare records, financial records, email content, and browsing history, at risk. Between March 2016 and March 2017, 1.9 billion usernames and passwords were exposed by data breaches and traded on black-market forums [37]. In 2010, it was discovered that Google Street View vehicles weren't just taking pictures of people's homes and businesses; they were also vacuuming up gigabytes of unprotected Wi-Fi data, including passwords, and they had been doing so in 30 countries for 3 years [38]. The ease of hacking, along with the fact that it is virtually impossible to erase data from the internet (all of which is vulnerable to hacking) [39], reminds us that the internet was not designed with security in mind.

Privacy is also at risk online because of toothless regulations and laws. COPPA, for example, supposedly shields children ages 12 and under, but a child of any age can gain full access to a pornography website simply by clicking a button reading “I am over 18.” One survey found that 7.5 million of Facebook's users were under age 13, demonstrating how difficult it can be for sites to verify the ages of their users [40, 41]. COPPA also fails to protect young people over age 12, leaving a large gap in the protection of America's youth.

Because corporations are driven by profit, their privacy policies tend to undermine user privacy rather than protect it, and they often use design features—or “dark patterns” [42]—to

frustrate, confuse, or coerce users into participation [43–45]—a practice called “malicious interface design” [46]. Privacy policies are not only excessively lengthy (the average American would need to set aside almost 250 hours to properly read all the digital contracts they accept while using online services), they are also often written in language that is difficult to understand [47–49]. This is the case even for policies regarding sensitive health information [50].

## 2.4 Privacy-protective behavior

One would think that people concerned about privacy would make an effort to protect it, but this is often not the case. The gap between the concern people express about privacy and their actual privacy-protective behavior is called “the privacy paradox” [51]. Even people who express the highest degree of concern sometimes knowingly disclose personal information online [52, 53, cf. 54], and even those who are technically skilled or confident in their ability to protect their own privacy often fail to protect their privacy [55, 56]. Most users are simply unwilling to invest the time and energy required to assure the protection of their personal information, and, generally speaking, people’s privacy concerns are easily overridden by the various ways in which they benefit by disclosing information [28, 57–59, cf. 60]. For example, simple benefits such as monetary discounts or rewards tend to increase disclosure [61–64]. Privacy concerns are also overridden by perceived control; because people believe that they are powerless against data collection, they often fail to take steps to protect their privacy [65, cf. 66].

The risk/reward model may be only partially relevant to the privacy paradox, however. Because of the rapid and highly interactive way in which users interact with computers and mobile devices, they often don’t have time to make decisions about the information they are asked to disclose [67]. They are simply reacting mindlessly to queries, clicking on buttons or boxes, or pressing the Enter key without giving much thought to what they are doing [68].

## 2.5 Predictors of privacy behavior

Age and personality traits can be predictive of disclosure. Younger adults are more likely to disclose personal information than older adults [69, cf. 70]; more extroverted people and those who report low self-control are more likely to disclose intimate information online [71]; and those who rank higher in openness, lower in conscientiousness, and lower in agreeableness are more likely to disclose more information online [72]. Privacy awareness and confidence in one’s own ability to mitigate privacy concerns can predict privacy decisions [56]. Situational factors also significantly impact people’s privacy decisions. For example, the tendency to disclose is higher in large rooms than in smaller ones [73], and familiar environments where people are likely to feel a greater sense of protection may lead to higher trust and higher disclosure [74]. Disclosure is also higher when requests for information are indirect, rather than direct, and when website interfaces are unprofessional, rather than neutral or professional [75]. People are also more likely to pay for more privacy (for example, by shopping at a different website) when a privacy warning is too salient [76]. The perceived sensitivity of the information requested is another predictor of privacy behavior [77], and because different types of information, such as location, health status, and browsing history, are valued differently by different people, one cannot expect privacy behaviors to be consistent across situations [78]. After being told that other people have revealed certain types of information, people are more likely to reveal similar information themselves [79], and a similar phenomenon has even been observed when people interact with an avatar; people reveal more information to an avatar after it has shared information about itself [80]. Self-disclosure activates the brain’s reward system, perhaps demonstrating its intrinsic value [81].

## 2.6 Methods for influencing privacy concerns and behavior

Privacy concerns and privacy-protective behavior can each be impacted in various ways. Although rewards can increase disclosure, some studies have demonstrated that the offer of a reward for disclosing private information can increase privacy concerns [82], especially when the sensitivity of the information requested is high [83]. Including a privacy policy on a website has been shown to increase trust, which is associated with a decrease in disclosure concerns and increased willingness to disclose personal information [84–86]. When a privacy policy is presented as a formal, legalistic agreement, however, trust can deteriorate [87]. Some studies highlight the significance of certain policy features; to increase privacy-protective behaviors, information relevant to privacy decision making must be salient, easily accessible, complete, and threatening [76, 82, 88, cf. 89].

Timing is also important. When people are reminded about privacy at the moment they must make a decision, previously dormant privacy concerns might be awakened, leading to more privacy-protective behavior [90, 91]. This might occur because when users cannot easily bring risks to mind, they mistakenly perceive risk to be low [92].

Certain design features can be used to “push” users to make certain privacy decisions. Nudges—subtle attempts to influence people’s decisions without force [93]—have been used to improve privacy outcomes without limiting users’ choices [94]. For example, presentation nudges are used to provide necessary contextual clues to reduce the user’s cognitive load and convey the appropriate level of risk in order to mitigate biases and heuristics relevant to privacy decision-making [94]. Nudges can draw users’ attention to privacy links and decrease the posting of personal information to public audiences online [95, 96, cf. 97], and nudges that inform users about how they can mitigate privacy risks are more effective at increasing privacy-protective behavior than nudges that rely purely on fear [98]. Priming—exposure to relevant stimuli that influences the response to subsequent stimuli, regardless of awareness [99]—has also been used to deter the disclosure of personal information [100]. Framing—the way an outcome or situation is presented to an audience [101]—is another feature that influences people’s privacy-related decisions [102, 103].

These days, it is increasingly common to see a privacy-related pop-up box—or “cookie consent banner”—whenever one visits a new website. Sometimes the banner informs users that by proceeding onto the website, they are allowing the website owner or its agents to install a variety of unspecified tracking software on their computers; there is no way to opt out of this option. This is referred to as a browserwrap agreement [104]. At other times, the banner lets people click buttons that allow them to limit the tracking to what the website owner considers to be “essential” (which is generally undefined); this is referred to as a clickwrap or click-through agreement. Although clickwrap agreements might have been meant to increase user awareness of privacy threats [105], these banners are often structured in a way that encourages people to surrender their privacy [106]. For example, buttons reading “Join” or “I agree” are often visually more prominent than alternative buttons [68]—a dark pattern that has been shown to increase user acceptance [107]. Whether clickwrap agreements affect people’s tendencies to disclose sensitive information is unknown.

In the present study, we sought to determine the extent to which click requirements and privacy warnings would cause people to withhold sensitive personal information. It employed a randomized, controlled,  $2 \times 2$  factorial design with a diverse sample of participants. Our design also included a control group—people who were not shown privacy warnings and who were not required to click on a clickwrap agreement.

### 3. Methods

The federally registered Institutional Review Board (IRB) of the sponsoring institution (American Institute for Behavioral Research and Technology) approved this study with exempt status under HHS rules because (a) the anonymity of participants was preserved and (b) the risk to participants was minimal. The IRB also exempted this study from informed consent requirements (relevant HHS Federal Regulations: 45 CFR 46.101(b)(2), 45 CFR 46.116(d), 45 CFR 46.117(c)(2), and 45 CFR 46.111). The IRB is registered with OHRP under number IRB00009303, and the Federalwide Assurance number for the IRB is FWA00021545.

#### 3.1 Participants

Our participants were recruited from Amazon's Mechanical Turk (MTurk) website, which has been used by social scientists in a variety of research since 2005 [108]. In all, 1,622 people were randomly assigned to each of 5 groups. Because people take different amounts of time to complete their sessions, we ended up with unequal numbers of people in each group: 306 in Group 1, 307 in Group 2, 327 in Group 3, 314 in Group 4, and 368 in Group 5. After separating the participants in each group who either dropped out of the study after providing demographic information (by closing the browser tab) or who quit the study after seeing the questionnaire (by clicking on an "end session" button), we were left with 304 in Group 1 (2 drops or quits), 304 in Group 2 (3 drops or quits), 304 in Group 3 (23 drops or quits), 305 in Group 4 (9 drops or quits), and 333 in Group 5 (35 drops or quits). Finally, to get an even number of people in each of the groups, we used SPSS's "Random sample of cases" feature to select random samples of 300 people from each group. Our analysis therefore focused on five groups with 300 people in each. We were also able to preserve some information about 72 other people who dropped out of the study before completing it. The dropouts proved to be important in our analysis of the data (see below).

Participants ranged in age from 18 to 82 ( $M = 32.63$  [ $SD = 10.78$ ]). 853 (56.9%) identified themselves as male, 642 (42.8%) as female, and 4 (0.3%) as Other; gender was not reported for 1 (0.1%) of our participants. 1,215 (81.0%) of our participants were from the US, 259 (17.3%) were from India, and 26 (1.7%) were from 18 other countries. 949 (63.3%) of our participants identified themselves as White and 551 (36.7%) as Non-White in the following categories: 354 (23.6%) as Asian, 91 (6.1%) as Black, 49 (3.3%) as Hispanic, 20 (1.3%) as American Indian, and 37 (2.5%) as Other.

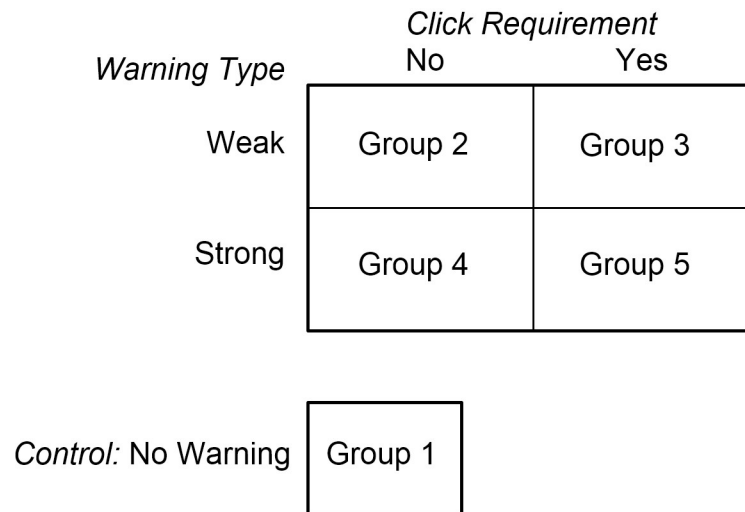
Level of education also varied over a wide range: no high school degree: 6 (0.4%); completed high school: 409 (27.3%); associate's or 2-year degree: 244 (16.3%); bachelor's degree: 642 (42.8%); master's degree: 178 (11.9%); doctoral degree: 21 (1.4%). On a 10-point scale, where 10 was the highest degree of fluency, participants rated their English fluency as high ( $M = 9.63$  [ $0.86$ ]).

The 72 dropouts were similar to the 1,500 participants who completed the experiment in age [ $t(1570) = -1.627$ ,  $p = 0.104$ ,  $d = 0.19$ ], gender ( $z = 0.68$ ,  $p = 0.497$ ), education ( $z = 0.66$ ,  $p = 0.509$ ), and race/ethnicity ( $z = 0.53$ ,  $p = 0.603$ ).

#### 3.2 Procedure

Participants were directed from the MTurk site to our own web page where they were first asked basic demographic questions. In order to protect the identities of our participants (a requirement of the exempt status granted by the institutional review board of our sponsoring institution), participants were not asked for their full names or email addresses.

They were then instructed to complete a 25-item survey in which they were asked to indicate whether they had engaged in a number of illegal, immoral, or socially controversial



**Fig 1. Experimental design.** Participants in the control group (Group 1) were not shown a warning above the questionnaire. Participants in the other four groups were presented two levels of warning and two click conditions (click or no click required) in a  $2 \times 2$  factorial design as shown in the figure.

<https://doi.org/10.1371/journal.pone.0263097.g001>

activities within the past three years—activities such as driving recklessly, watching pornography, smoking marijuana, harming oneself, cursing God, and so on. Participants could respond by clicking “Yes,” “No,” “Maybe,” “Can’t remember,” or “Click here to end your session.” Participants could also terminate their session by closing their browser tab. The number of possible transgressions participants admitted to committing (by clicking “Yes” to items in our survey) served as our dependent variable. The 25 items on the questionnaire were selected from among 100 items we had studied in pilot procedures. We chose the 25 items that were most impacted by our warnings (indicated by the difference between the number of admissions in Groups 1 and 5, see Fig 1). After completing the questionnaire, participants were taken to a debriefing page and thanked for their participation.

Participants were randomly assigned to one of five different groups in which warnings of various sorts were displayed above the questionnaire (see S1 to S5 Figs to view the screens). Warnings stated how data might be used, and in some groups participants were required to click a link to confirm they had understood the warning they were shown. In the control condition, no warning accompanied the questionnaire. In the other four groups, two independent variables were varied in a between-subjects,  $2 \times 2$  factorial design: strength of warning and click requirement (Fig 1).

The weak warning included standard internet language telling the participants that they must comply with a Terms of Service (TOS) agreement: “Please note: By using this website you agree to our Terms of Service” [109] (see S2 and S3 Figs). The strong warning included a brief paragraph reminding participants that their answers and IP addresses were being recorded and that their information might be shared with others, as follows (see S4 and S5 Figs):

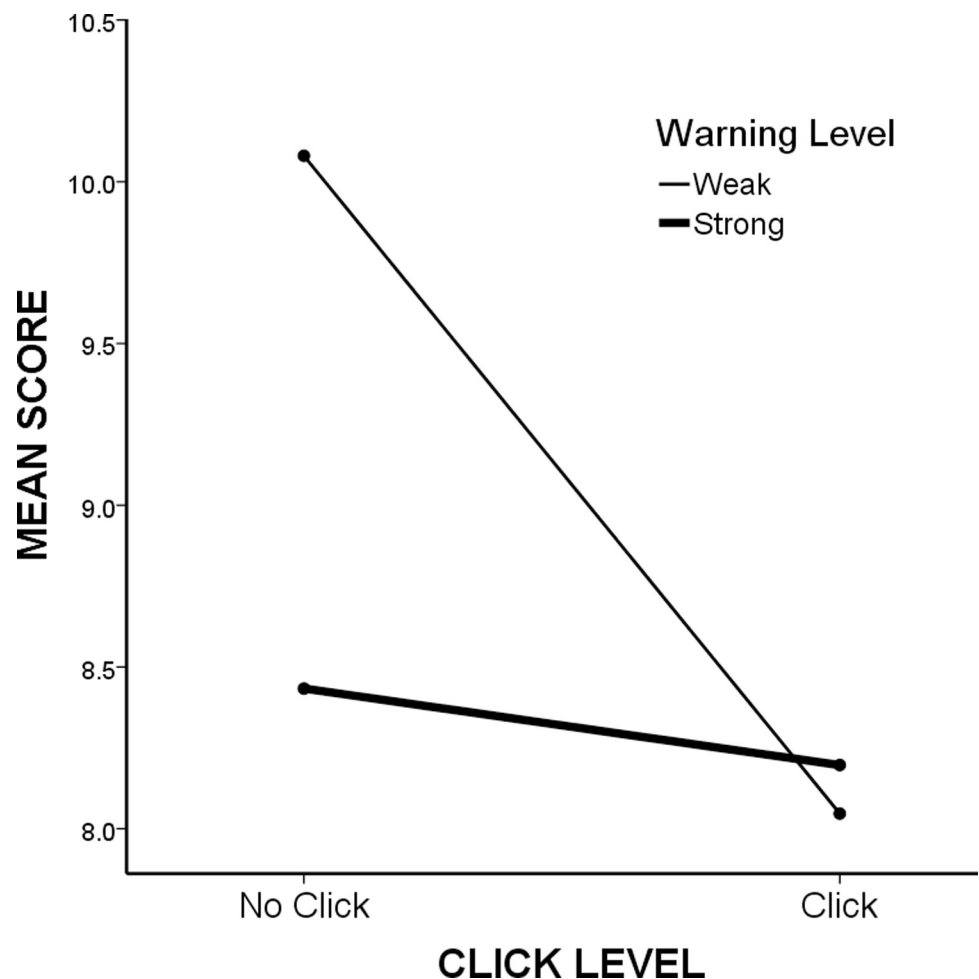
**PLEASE READ:** By using this website you agree to our Terms of Service [109]. Specifically, you give us your consent to record and store your survey answer along with identifying information such as your IP address, as well as to share this information as required or permitted by law with authorized individuals, companies, organizations, or government agencies.

In both warning conditions, participants could click a link to access a lengthy, detailed TOS agreement that contained two links to a lengthy, detailed privacy policy [110] (3,591 words in total). Both documents were modeled after corresponding Google documents. The number of people who clicked these links and the total time they kept these documents open were recorded. Participants in the click groups were required to click on the phrase “Please click here” to acknowledge that they had read and agreed to the TOS.

## 4. Results

### 4.1 Analysis of variance

A two-way ANOVA of results in the four experimental groups (2, 3, 4, and 5) revealed main effects for both of our independent variables: warning strength ( $M_{\text{strong}} = 8.32$  [5.31],  $M_{\text{weak}} = 9.06$  [5.35],  $p < 0.05$ ) and click requirement ( $M_{\text{click}} = 8.12$  [5.32],  $M_{\text{non-click}} = 9.26$  [5.30],  $p < 0.001$ ). We also found a statistically significant interaction between these variables:  $F(1, 1196) = 8.674$ ,  $p < 0.01$  (Fig 2).



**Fig 2. Graphical results of two-way ANOVA.** It shows click level (no click or click) versus mean scores (mean number of “yes” responses). The thin line shows data for the weak warning condition, and the thick line shows data for the strong warning condition.

<https://doi.org/10.1371/journal.pone.0263097.g002>



## 4.2 Control group versus experimental groups

We also found a significant difference between the mean score of the control group (Group 1, no warnings) and the mean score of the four experimental groups combined (Groups 2, 3, 4, and 5) ( $M_1 = 10.80$  [5.13],  $M_{2-5} = 8.69$  [5.34],  $t(1,498) = 6.16$ ,  $p < 0.001$ ,  $d = 0.40$ ). Pairwise comparisons between the mean score of the control group (Group 1) and the mean scores of three of the four experimental groups (Groups 3, 4, and 5) also produced significant differences ( $M_3 = 8.05$  [0.31],  $t(598) = 6.46$ ,  $p < 0.001$ ,  $d = 0.76$ ;  $M_4 = 8.43$  [5.27],  $t(598) = 5.57$ ,  $p < 0.001$ ,  $d = 0.46$ ;  $M_5 = 8.20$  [5.35],  $t(598) = 6.08$ ,  $p < 0.001$ ,  $d = 0.50$ ). It is notable that the difference in the mean scores between the control group and Group 2—people receiving the internet's common TOS warning with no click requirement—was not significant ( $M_2 = 10.08$  [5.21]),  $t(598) = 1.70$ ,  $p = 0.09$ ,  $d = 0.14$ ). Where G signifies Group, we can summarize this pattern of results as follows:

$$G1 = G2 < G3 = G4 = G5$$

This pattern shows that when we looked at the amount of sensitive personal information people disclosed, either a strong warning or a click requirement suppressed disclosure significantly. Overall, participants provided 32.8% more information when they had no privacy warning (Group 1) than when they had a click requirement (Groups 3 and 5 combined,  $M = 8.13$ [5.32]), and participants provided 24.3% more information when they had no privacy warning (Group 1) than when they had either a click requirement or a warning (Groups 2, 3, 4, and 5 combined,  $M = 8.69$ [5.34]).

## 4.3 Demographic differences

We found a marked difference between disclosures by US participants (Groups 2, 3, 4, and 5 combined,  $N = 920$ ,  $M = 9.93$  [5.01]) and disclosures by participants from India (Groups 2, 3, 4, and 5 combined,  $N = 257$ ,  $M = 4.31$  [4.07]) (see [Discussion](#)). We also found significant differences in disclosures by gender ( $M_{\text{male}} = 9.80$  [5.22],  $M_{\text{female}} = 8.21$  [5.42],  $t(1493) = 5.76$ ,  $p < 0.001$ ,  $d = 0.30$ , race/ethnicity ( $M_{\text{White}} = 10.34$  [4.95],  $M_{\text{Black}} = 8.87$  [4.93],  $M_{\text{Hispanic}} = 10.61$  [4.92],  $M_{\text{Asian}} = 6.00$  [5.16],  $M_{\text{AmIndian}} = 7.95$  [6.15],  $M_{\text{Other}} = 6.51$  [5.72],  $F(5, 1494) = 41.42$ ,  $p < 0.001$ ), and education ( $M_{\text{none}} = 7.83$  [5.19],  $M_{\text{highschool}} = 10.72$  [5.03],  $M_{\text{associates}} = 9.93$  [5.43],  $M_{\text{bachelors}} = 8.44$  [5.34],  $M_{\text{masters}} = 6.88$  [4.88],  $M_{\text{doctorate}} = 8.14$  [5.48],  $F(5, 1494) = 17.79$ ,  $p < 0.001$ ), as well as an effect for age ( $r = -.22$ ,  $p < 0.001$ ).

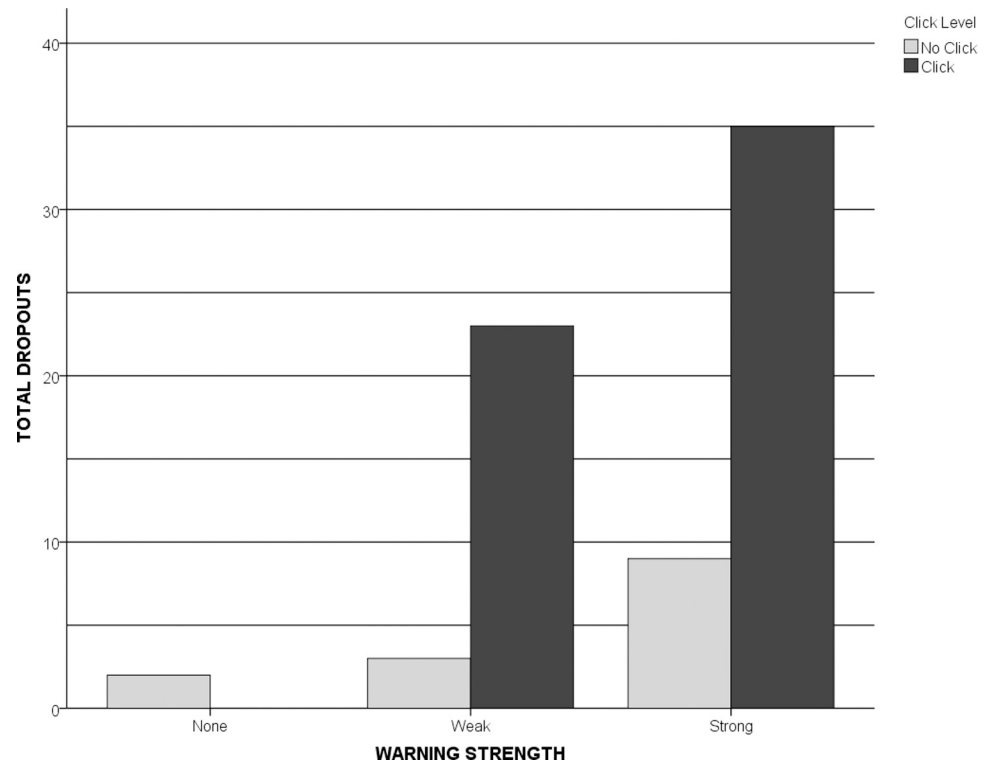
## 4.4 Impact and characteristics of dropouts

The power of the click requirement is revealed further when one looks at the pattern according to which people either dropped out of the experiment before completing it by closing their browser tab or by clicking a button we provided which read, “If you have decided not to complete the survey, please click here to end your session” (Fig 3, Table 1). (Henceforward, we will refer to both categories combined under one label: “dropouts.”).

The attrition rate in the control group (0.007) was significantly lower than the attrition rate in the experimental groups combined (0.053,  $z = 3.57$ ,  $p < 0.001$ ) (Table 1). We also found a significant difference in attrition rates across the five groups individually ( $\chi^2[4, N = 1,622] = 48.35$ ,  $p < 0.001$ ). Pairwise comparisons of attrition rates revealed another interesting pattern:

$$G1 = G2 = G4 < G3 = G5$$

In other words, the click requirement (present in Groups 3 and 5 only) affected attrition significantly.



**Fig 3. Pattern of dropouts.** Written warnings alone drove only a few people away from the study. An added click requirement increased the total number of dropouts substantially (black bars).

<https://doi.org/10.1371/journal.pone.0263097.g003>

#### 4.5 Terms of service warning

Of the 1,200 people who were prompted to view the TOS agreement, only 88 (7.3%) did so, and only 17 (19.3% of those who viewed the TOS agreement) clicked through to the privacy policy. The average amount of time these people kept these documents open was 22.9 seconds, roughly enough time to read 91 words (2.5% of the total) [111].

## 5. Conclusions

Our results support four conclusions: (1) The commonly-used TOS warning has no deterrent effect and is functionally the same as no warning at all. (2) A strong, more explicit, warning has some deterrent effect. (3) A click requirement increases the effectiveness of both weak and strong warnings, and it can also cause people to close a web page. (4) Given that most, or perhaps nearly all, internet users are exposed either to no warnings regarding the possible fate of

**Table 1. Comparison of dropouts by group number.**

Group No.	Total Dropouts	Attrition Rate	Comparison Group	z-score	p value
Group 1	2	0.007	Group 2	0.04	0.653
Group 2	3	0.010	Group 4	1.71	0.087
Group 3	23	0.070	Group 5	1.18	0.238
Group 4	9	0.029	Group 3	2.42	< 0.05
Group 5	35	0.095	–	–	–
Groups 2 thru 5	70	0.053	Group 1	3.57	< 0.001

<https://doi.org/10.1371/journal.pone.0263097.t001>

the information they are providing (our Group 1), or are exposed at most to some mention of a Terms of Service agreement (our Group 2), our results suggest that internet users may currently be disclosing at least 32.8% (our Groups 3 and 5) more personal information than they otherwise would if they were more effectively warned about the risks involved.

## 6. Discussion

### 6.1 Insights on attrition

Although we detected only 72 people who left our study before completing it, these people are in some respects the most interesting and revealing in the study. They are interesting from the perspective of experimental design because most studies never track such people. In our early pilot experiments, neither did we, and that sometimes gave us misleading results. When we had a 100-item questionnaire, we sometimes found no effects, presumably because of large attrition rates. With a short questionnaire, we found clear effects among the people who completed the survey, and we also found a clear pattern of attrition associated with the different groups.

The dropout pattern is also interesting in what it might be telling us about how the internet is segmenting societies worldwide. In Dave Egger's 2013 book, *The Circle* (subsequently made into a movie starring Emma Watson and Tom Hanks), surveillance by a Google-like company has become so pervasive and extreme that some people are going to great lengths to go "off-grid" [112]. The main character, Mae Holland—a rising star at the company—loves the surveillance, but her ex-boyfriend does not. To escape the invasive electronics, he moves to a cabin in the woods, at which point Mae asks her huge cadre of online followers to find him. Minutes later, camera-carrying drones surround his home, at which point he jumps into his pickup and drives straight off a bridge to his death. In other words, he went off-grid by literally going off-grid.

Our dropouts might be giving us a glimpse of yet another aspect of a dark electronic future. They are still connected, but they apparently don't like divulging sensitive personal information. Completely absent from our study is a much larger group of people who are already disconnected—who have quit social media platforms or perhaps never even got hooked. In age, race, gender, and education, our dropouts looked just like the people who completed our study, but we suspect they differed markedly in personality characteristics. Did our dropouts have higher perceived self-efficacy than our finishers [113–115]? Were our finishers more extroverted and open, less conscientious, or perhaps even more exhibitionistic [72, 116, 117] than our dropouts? The billions of people who post messages, photos, and videos of themselves on social media platforms every day hardly seem shy, although some might be sharing their lives online as a response to social pressure [118–120].

The internet might be dividing the world's population into two distinct groups: people we might call "LoudMouths," who compete each day for attention and followers, and people we might call "ZipMouths," who are largely absent from the space that has become increasingly dominant in our lives: Cyberspace. With more and more social science research moving online [121, 122, cf. 123], are important studies drawing erroneous conclusions because of how the internet is segmenting societies? Are we basing our research conclusions on samples that exclude certain personality types? And with major news outlets routinely basing news stories on social media trends [124] and many people turning to social media to get the latest news [125, 126, cf. 127], are Zipmouths losing their ability to influence social policy—perhaps even to influence the outcomes of elections?

What if this trend continues? Although it is clearly in the interest of online entities to extract as much personal data from users as possible, authorities are gradually forcing web

hosts to inform users about the risks associated with using their web pages. We see this trend in the increasing number of pop-ups warning us about cookies and other invasions of privacy, some of which now include a click requirement [128]. This practice might cause some people to close a web page and others to divulge less information. Over time, however, such practices will also drive more people off-grid—and, potentially, outside the bounds of a functioning society.

## 6.2 The power of the click requirement

Warnings—along, of course, with all the fake news, trolling, and bullying—might drive some people off the internet because of their official, legalistic appearance and content. They create the impression that the user is entering into a binding legal contract. A growing body of law in the US suggests, however, that the appearance of a TOS warning alone is not legally binding, but when a user clicks his or her assent to such a warning, courts have ruled that the agreement is binding [27, 39, 104]. The legalistic language in our strong warning might have been essential to its impact [see 87]. That issue should be explored in future research.

Our findings on dropouts also suggest that in studies in which attrition can have a systematic effect on study outcomes, it is essential that attrition be closely tracked. Recall that in some of our pilot experiments (when we used a 100-item questionnaire), we sometimes failed to find effects, almost certainly because we failed to track dropouts.

How effective various types of warnings are in discouraging personal disclosures online is a complex issue. It depends not only on the nature of the warning but also on the value users perceive in divulging such information. In the highly exhibitionistic environments of Facebook, Reddit, and Instagram, photos and disclosures—the more extreme, the better—bring comments, likes, and followers, all of which increase people's social capital, thus increasing their tendency to use social media and disclose more online [117, 129–131]. Disclosing personal information also allows platforms like Google and Facebook to target ads more precisely. For some people, those ads turn the internet into their personal shopper; for others, they are reminders of privacy lost. When we contemplate the power of warnings and click requirements, we also need to think about the rewards associated with the behaviors we are trying to suppress [132]. In many cases and for many people, attempts to suppress disclosures are little more than annoyances [32].

Why a click requirement had such a large impact in our experiment is unclear, but we suspect that this is an attentional phenomena. A click box is a graphical element that draws attention, especially when a click is required in order for a user to proceed. Graphical elements that draw attention on a computer screen have been shown to have a greater impact on user behavior than more subtle graphical elements [133, 134, cf. 135, 136], and that finding is consistent with a long history of research on attention in various contexts [2, 137, 138]. Because required clicks near a warning message also suggest legal liability (which is, as we noted, supported by emerging case law), it is also possible that users who encounter a click requirement are more likely to fear the associated warnings. Our Groups 3 (click requirement with weak warning) and 5 (click requirement with strong warning) begin to shed some light on such issues, but further research, including eye-tracking studies, must be conducted to learn precisely why the click requirement is so powerful.

## 6.3 Limitations and concerns

The validity of the present study is limited by its sample—a group of people recruited from Amazon's MTurk subject pool. Most were from the US (81.0%), but a sizeable group was from India (17.3%). Further research on warnings and click requirements should reach out to

different samples, especially in cultures and countries outside the US [139]. As noted earlier, we found significant and, sometimes, surprisingly large differences in disclosure rates by different demographic groups. Participants from the US, for example, disclosed more than twice as many sensitive activities ( $M = 9.93$  [5.01]) as participants from India did ( $M = 4.31$  [4.07]). That difference could be explained by cultural differences that have been studied by anthropologists and other social scientists [140, 141]. Our study was not structured in a way, however, that allows for meaningful comparisons to be made between different cultures.

Future research on factors affecting online disclosures should also look specifically at (a) types of disclosure that are actually common online, such as information about people's personal lives, along with photos and videos, and (b) how context and environment impact disclosures. Disclosure is the norm, for example, on one's Facebook or Instagram pages, but it often occurs without people's knowledge when they use Google's search engine or Gmail. Warnings and click requirements will almost certainly have to take on very different forms to be effective in the wide range of environments that people now inhabit online, and privacy-promoting techniques that work well with one demographic group might work poorly with another.

Disclosures are also now the norm when people are interacting with personal assistants such as Apple's Siri, Microsoft's Cortana, Amazon's Alexa, and the Google Assistant (standard on Android devices). It is not at all clear how, query by query and device by device, we can meaningfully warn people about the fact that they are disclosing personal information, possibly to their detriment. An increasing body of evidence also indicates that these and other personal assistants constantly record whatever they are hearing [142–144]. Again, how can we meaningfully warn people about invisible surveillance that never stops?

The growing internet of things is rapidly complicating the disclosure problem. In 2014, for example, Google bought Nest Labs [145]. Several years later, it was revealed that Google had installed microphones into the Nest Guard alarm system without disclosing this to users [146]. When the company was called out, it could hardly deny the existence of the microphones, but it claimed it had not yet activated them (then why install them?) [147].

There is good news and bad news here. The good news is that click requirements seem to be surprisingly powerful in discouraging people from disclosing personal information. The bad news is that corporate surveillance is so pervasive and aggressive and so thoroughly embedded into the online environment that no attempts to discourage personal disclosure are likely to make much difference. We join with other scholars and scientists in calling upon our leaders to make the surveillance business model—a fundamentally deceptive model that was invented by Google and that is now being imitated by thousands of businesses worldwide [148]—illegal [148–152].

## Supporting information

**S1 Fig. Group 1 screen (partial view).**  
(TIF)

**S2 Fig. Group 2 screen (partial view).**  
(TIF)

**S3 Fig. Group 3 screen (partial view).**  
(TIF)

**S4 Fig. Group 4 screen (partial view).**  
(TIF)

**S5 Fig. Group 5 screen (partial view).**  
(TIF)

## Acknowledgments

We thank R. Robertson for help with running the experiment and T. Vasconcellos for help in conducting the literature review. We are especially grateful to J. Johnston for helping us improve our research design.

## Author Contributions

**Conceptualization:** Robert Epstein.

**Data curation:** Robert Epstein.

**Formal analysis:** Vanessa R. Zankich.

**Investigation:** Robert Epstein.

**Project administration:** Robert Epstein.

**Supervision:** Robert Epstein.

**Writing – original draft:** Robert Epstein, Vanessa R. Zankich.

**Writing – review & editing:** Robert Epstein, Vanessa R. Zankich.

## References

1. Auxier B, Rainie L. Key takeaways on Americans' views about privacy, surveillance and data-sharing [Internet]. Pew Research Center. 2019 [cited 14 October 2021]. Available from: <https://www.pewresearch.org/fact-tank/2019/11/15/key-takeaways-on-americans-views-about-privacy-surveillance-and-data-sharing/>
2. Azagba S, Sharaf MF. The Effect of Graphic Cigarette Warning Labels on Smoking Behavior: Evidence from the Canadian Experience. *Nicotine Tob Res*, 2012; 15(3):708–17. <https://doi.org/10.1093/ntr/nts194> PMID: 22990228
3. Values Mission [Internet]. National Security Agency. [cited 19 October 2021]. Available from: <https://www.nsa.gov/about/mission-values/>
4. Geiger AW. How Americans have viewed surveillance and privacy since Snowden leaks [Internet]. Pew Research Center. 2018. Available from: <https://www.pewresearch.org/fact-tank/2018/06/04/how-americans-have-viewed-government-surveillance-and-privacy-since-snowden-leaks/>
5. Penney JW. Chilling effects: Online surveillance and Wikipedia use. *Berkeley Technol Law J*, 2016; 31(1):117–182. <https://doi.org/10.15779/Z38SS13>
6. Madden M, Rainie L. Americans' view about data collection and security [Internet]. Pew Research Center. 2015. Available from: <https://www.pewresearch.org/internet/2015/05/20/americans-views-about-data-collection-and-security/>
7. Auxier B, Rainie L, Anderson M, Perrin A, Kumar M, Turner E. Americans and privacy: Concerned, confused and feeling lack of control over their personal information [Internet]. Pew Research Center. 2020. Available from: <https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/>
8. Madden M, Cortesi S, Gasser U, Lenhart A, Duggan M. Parents, teens, and online privacy [Internet]. Pew Research Center. 2012. Available from: <https://www.pewresearch.org/internet/2012/11/20/parents-teens-and-online-privacy/>
9. Anderson M. How parents feel about—and manage—their teens' online behavior and screen time [Internet]. Pew Research Center. 2019. Available from: <https://www.pewresearch.org/fact-tank/2019/03/22/how-parents-feel-about-and-manage-their-teens-online-behavior-and-screen-time/>
10. Madden M, Lenhart A, Cortesi S, Gasser U, Duggan M, Smith A, et al. Teens, social media, and privacy. Pew Research Center. 2013. Available from: <https://www.pewresearch.org/internet/2013/05/21/teens-social-media-and-privacy/>

11. Shin W, Kang H. Adolescents' privacy concerns and information disclosure online: The role of parents and the internet. *Comput Human Behav*, 2016; 54:114–123. <https://doi.org/10.1016/j.chb.2015.07.062>
12. Call Recording Laws by State | SmithMarco [Internet]. Protecting Consumer Rights. [cited 19 October 2021]. Available from: <https://protectingconsumerrights.com/debt-collection-problems/fair-debt-collection-practices-act/call-recording-laws-by-state/>
13. 14 Consumer Protection Laws You Should Know [Internet]. Zebersky Payne Shaw Lewenz. 2019 [cited 19 August 2021]. Available from: <https://zpllp.com/the-14-areas-of-consumer-protection-laws-you-should-know/>
14. Video Voyeurism Prevention Act of 2004. 18 U.S.C. § 1801 et seq. (2004). Available from: [https://uscode.house.gov/view.xhtml?req=\(title:18%20section:1801%20edition:prelim](https://uscode.house.gov/view.xhtml?req=(title:18%20section:1801%20edition:prelim)
15. Privacy Act of 1974, 5 U.S.C. § 552a (1974). Available from: <https://www.govinfo.gov/content/pkg/USCODE-2018-title5/pdf/USCODE-2018-title5-partI-chap5-subchapII-sec552a.pdf>
16. Fair Credit Reporting Act, 15 U.S.C. § 1681 et seq. (1970). Available from: <https://www.govinfo.gov/content/pkg/USCODE-2015-title15/pdf/USCODE-2015-title15-chap41-subchapIII.pdf>
17. Act Gramm-Leach-Bliley, 15 U.S.C. §§ 6801–6809, §§ 6821–6827. (1999). Available from: <https://www.ftc.gov/enforcement/statutes/gramm-leach-bliley-act>
18. Health Insurance Portability and Accountability Act, Pub. L. 104–191. Stat. 1936 (1996). Available from: <https://www.congress.gov/104/plaws/publ191/PLAW-104publ191.pdf>
19. Health Information Privacy Law and Policy [Internet]. The Office of the National Coordinator for Health Information Technology. 2018 [cited 11 October 2021]. Available from: <https://www.healthit.gov/topic/health-information-privacy-law-and-policy>
20. Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501–6506 (1998). Available from: <https://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title15-chapter91&edition=prelim>
21. Data protection under GDPR [Internet]. Your Europe. 2021 [cited 7 October 2021]. Available from: <https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/>
22. The 10 problems of the GDPR: The US can learn from the EU's mistakes and leapfrog its policy, Senate Judiciary Committee on the General Data Protection Regulation and California Consumer Privacy Act: Opt-ins, Consumer Control, and the Impact on Competition and Innovation. (2019) (testimony of Rosalyn Layton). Available from: <https://www.judiciary.senate.gov/imo/media/doc/Layton%20Testimony1.pdf>
23. California Consumer Privacy Act, AB 375 (2018). Available from: [https://leginfo.ca.gov/faces/billTextClient.xhtml?bill\\_id=201720180AB375](https://leginfo.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375)
24. SB 220, 80th Session. (2019). Available from: <https://www.leg.state.nv.us/App/NELIS/REL/80th2019/Bill/6365/Overview>
25. SP 275, An Act to Protect the Privacy of Online Customer Information, 129th Maine Legislature, First Regular Session. (2019). Available from: [http://legislature.maine.gov/legis/bills/bills\\_129th/chapters/PUBLIC216.asp](http://legislature.maine.gov/legis/bills/bills_129th/chapters/PUBLIC216.asp)
26. Acquisti A, Brandimarte L, Loewenstein G. Privacy and human behavior in the age of information. *Science*. 2015; 347(6221):509–514. <https://doi.org/10.1126/science.aaa1465> PMID: 25635091
27. Dasteel JH. Consumer click arbitration: A review of online consumer arbitration agreements. *Yearbook on Arbitration and Mediation*, 2017; 9(1). Available from: <https://elibrary.law.psu.edu/cgi/viewcontent.cgi?article=1215&context=arbitrationlawreview>
28. Gomez-Barroso JL. Experiments on personal information disclosure: Past and future avenues. *Telemat Inform*, 2018; 35(5):1473–1490. <https://doi.org/10.1016/j.tele.2018.03.017>
29. Jensen C, Potts C, Jensen C. Privacy practices of internet users: Self-reports versus observed behavior. *Int J Hum Comput Stud*, 2005; 63(1–2):203–227. <https://doi.org/10.1016/j.ijhcs.2005.04.019>
30. Plaut VC, Bartlett RPIII. Blind consent? A social psychological investigation of non-readership of click-through agreements. *Law and Human Behavior*, 2011; 36(4):293–311. <https://doi.org/10.1037/h0093969> PMID: 22849415
31. Malaga RA. Do web privacy policies still matter? *Academy of Information and Management Sciences Journal*, 2014; 17(1):95–99.
32. Obar JA, Oeldorf-Hirsch A. The biggest lie on the internet: Ignoring the privacy policies and terms of service policies of social networking services. *Information, Communication Society*, 2018; 23(1):128–147. <https://doi.org/10.1080/1369118X.2018.1486870>
33. Google. Privacy policy [Internet]. 2021 Jul 1 [cited 2021 Aug 21]. Available from: <https://policies.google.com/privacy?hl=en>

34. Google. Terms of service [Internet]. 2020 Mar 31 [cited 2020 Aug 21]. Available from: <https://policies.google.com/terms?hl=en-US>
35. McGee M. As Google Analytics turns 10, we ask: How many websites use it? MarTech [Internet]. 2015 Nov 12. Available from: <https://martech.org/as-google-analytics-turns-10-we-ask-how-many-websites-use-it/>
36. Schneier B. 2018. Click here to kill everybody: Security and survival in a hyper-connected world. W. W. Norton Company.
37. Thomas K, Li F, Zand A, Barrett J, Ranieri J, Invernizzi L, et al. Data breaches, phishing, or malware? Understanding the risks of stolen credentials. Google Research, 2017. <https://doi.org/10.1145/3133956.3134067>
38. Google 'accidentally' snooped on wifi data. Network Security, 2010; 2010(5):2. [https://doi.org/10.1016/S1353-4858\(10\)70052-0](https://doi.org/10.1016/S1353-4858(10)70052-0)
39. MacLean CE. It depends: Recasting internet clickwrap, browserwrap, "I agree," and click-through privacy clauses as waivers of adhesion. Cleveland State Law Review, 2017; 65(1):43–58. Available from: <https://engagedscholarship.csuohio.edu/clevstrev/vol65/iss1/7>
40. CR survey: 7.5 million Facebook users are under the age of 13, violating the site's terms. [Internet]. Consumer Reports. 2011 [cited 2021 Oct 15]. Available from: <https://www.consumerreports.org/media-room/press-releases/2011/05/cr-survey-75-million-facebook-users-are-under-the-age-of-13-violating-the-sites-terms/>
41. Perloth N. Verifying ages online is a daunting task, even for experts [Internet]. The New York Times. 2012 Jun 17. Available from: <https://www.nytimes.com/2012/06/18/technology/verifying-ages-online-is-a-daunting-task-even-for-experts.html>
42. Gray CM, Kou Y, Battles B, Hoggatt J, Toombs AL. The dark (patterns) side of UX design. CHI '18: Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems. 2018 Apr 21; pp. 1–14. <https://doi.org/10.1145/3173574.3174108>
43. Mathur A, Acar G, Friedman MJ, Lucherini E, Mayer J, Chetty M, et al. Dark Patterns at scale: Findings from a crawl of 11k shopping websites. Proceedings of the ACM on Human-Computer Interaction, 2019; 3:1–32. <https://doi.org/10.1145/3359216> PMID: 34322658
44. Di Geronimo L, Braz L, Fregnan E, Palomba F, Bacchelli A. UI Dark Patterns and where to find them: A study on mobile applications and user perception. CHI '20: Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems. <https://doi.org/10.1145/3313831.3376600>
45. Narayanan A, Mathur A, Chetty M, Kshirsagar M. Dark Patterns: Past, present, and future. Communications of the ACM, 2020; 63(9):42–47. <https://doi.org/10.1145/3397884>
46. Conti G, Sobiesk E. Malicious interface design: Exploiting the user. WWW '10: Proceedings of the 19th International Conference on World Wide Web. 2010 Apr 26–30; pp. 271–280. <https://doi.org/10.1145/1772690.1772719>
47. Jensen C, Potts C. Privacy policies as decision-making tools: An evaluation of online privacy notices. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, ACM, 2004;:471–478.
48. LePan N. 2020. Visualizing the length of the fine print, for 14 popular apps. Visual Capitalist, Technology. <https://www.visualcapitalist.com/terms-of-service-visualizing-the-length-of-internet-agreements/>
49. Reidenberg JR, Breaux T, Cranor LF, French B, Grannis A, Graves JT, et al. Disagreeable privacy policies: Mismatches between meaning and users' understanding. Berkeley Technol Law J, 2015; 30(1):39–88.
50. Chua HN, Herbrand A, Wong SF, Chang Y. Compliance to personal data protection principles: A study of how organizations frame privacy policy notices. Telemat Inform, 2017; 34(4):157–170. <https://doi.org/10.1016/j.tele.2017.01.008>
51. Barth S, de Jong MDT. The privacy paradox—Investigating discrepancies between expressed privacy concerns and actual online behavior—A systematic literature review. Telemat Inform, 2017; 34(7):1038–1058. <https://doi.org/10.1016/j.tele.2017.04.013>
52. Acquisti A, Gross R. Imagined communities: Awareness, Information sharing, and privacy on the Facebook. Privacy Enhancing Technologies. 2006;:36–58.
53. Spiekermann S, Grossklags J, Berendt B. Stated privacy preferences versus actual behaviour in EC environments: A reality check. Buhl HU, Kreyer N, Steck W. (eds) e-Finance. Springer-Verlag, Berlin, Heidelberg, 2001, pp. 129–147. [https://doi.org/10.1007/978-3-642-59504-2\\_8](https://doi.org/10.1007/978-3-642-59504-2_8)
54. Prince C. Do consumer want to control their personal data? Empirical evidence. Int J Hum Comput Stud, 2018; 110:21–32. <https://doi.org/10.1016/j.ijhcs.2017.10.003>



55. Barth S, de Jong MDT, Junger M, Hartel PH, Roppelt JC. Putting the privacy paradox to the test: Online privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources. *Telemat Inform*, 2019; 41:55–69. <https://doi.org/10.1016/j.tele.2019.03.003>
56. Lee H, Kobsa A. Confident privacy decision-making in IoT environments. *ACM Trans Comput Hum Interact*, 2019; 27(1). <https://doi.org/10.1145/3364223>
57. Seigel DA. Will you accept the government's friend request? Social networks and privacy concerns. *PLoS ONE*, 2013; 8(11). <https://doi.org/10.1371/journal.pone.0080682> PMID: 24312236
58. Shaw J. The watchers: Assaults on privacy in America [Internet]. *Harvard Magazine*; 2018. Available from: <https://www.harvardmagazine.com/2017/01/the-watchers>
59. Steinfeld N. Situational user consent for access to personal information: Does purpose make any difference? *Telemat Inform*, 2019; 48(4). <https://doi.org/10.1016/j.tele.2019.101341>
60. Keith MJ, Thompson SC, Hale J, Lowry PB, Greer C. Information disclosure on mobile devices: Re-examining privacy calculus with actual user behavior. *Int J Hum Comput Stud*, 2013; 71:1163–1173. <https://doi.org/10.1016/j.ijhcs.2013.08.016>
61. Babula E, Mrzyglod U, Poszowiecki A. Consumers' need of privacy protection—experimental results. *Journal of Scientific Papers, Economics Sociology*. 2017; 10(2):74–86.
62. Carrascal JP, Riederer C, Erramilli V, Cherubini M, de Oliveira R. Your browsing behavior for a Big Mac: Economics of personal information online. *WWW '13: Proceedings of the 22nd international conference on World Wide Web*, 2013 May 13. pp. 189–200. <https://doi.org/10.1145/2488388.2488406>
63. Munzert S, Selb P, Gohdes A, Stoetzer LF, Lowe W. Tracking and promoting the usage of a COVID-19 contact tracing app. *Nat Hum Behav*, 2021; 5:247–255. <https://doi.org/10.1038/s41562-020-01044-x> PMID: 33479505
64. Premazzi K, Castaldo S, Grosso M, Raman, P, Brudvig S, Hofacker CF. Customer information sharing with e-vendors: The roles of incentives and trust. *International Journal Electronic Commerce*, 2010; 14(3):63–91. <https://doi.org/10.2753/JEC1086-4415140304>
65. Xie W, Fowler-Dawson A, Tvaauri A. Revealing the relationship between rational fatalism and the online privacy paradox. *Behavior and Information Technology*, 2018; 38(7):742–759. <https://doi.org/10.1080/0144929X.2018.1552717>
66. Brandimarte L, Acquisti A, Loewenstein G. Misplaced confidences: Privacy and the control paradox. *Social Psychological and Personality Science*, 2012; 4(3):340–347. <https://doi.org/10.1177/1948550612455931>
67. Custers B. Click here to consent forever: Expiry dates for informed consent. *Big Data Society*, 2016; 3(1). <https://doi.org/10.1177/2053951715624935>
68. Obar JA, Oeldorf-Hirsch A. The clickwrap: A political economic mechanism for manufacturing consent on social media. *Social Media + Society*, 2018; 4(3). <https://doi.org/10.1177/2056305118784770>
69. Kezer M, Sevi B, Cemalcilar Z, Baruh L. Age differences in privacy attitudes, literacy and privacy management on Facebook. *Cyberpsychology*, 2016; 10(1). <https://doi.org/10.5817/CP2016-1-2>
70. Pereira S, Robinson JO, Peoples HA, Gutierrez AM, Majumder MA, McGuire AL, et al. Do privacy and security regulations need a status update? Perspectives from an intergenerational survey. *PLoS ONE*, 2017; 12(9). <https://doi.org/10.1371/journal.pone.0184525> PMID: 28926626
71. Yu S. Does low self-control explain voluntary disclosure of personal information on the internet? *Comput Human Behav*, 2014; 37:210–215. <https://doi.org/10.1016/j.chb.2014.04.055>
72. Hollenbaugh EE, Ferris AL. Facebook self-disclosure: Examining the role of traits, social cohesion, and motives. *Comput Human Behav*, 2014; 30:50–58. <https://doi.org/10.1016/j.chb.2013.07.055>
73. Okken V, van Rompay T, Pruyn A. Room to move: On spatial constraints and self-disclosure during intimate conversations. *Environment Behavior*, 2013; 45(6):737–760. <https://doi.org/10.1177/0013916512444780>
74. Norberg PA, Horne DR, Horner DA. The privacy paradox: Personal information disclosure intentions versus behaviors. *J Consum Aff*, 2007; 41(1):100–126. <https://doi.org/10.1111/j.1745-6606.2006.00070.x>
75. John LK, Acquisti A, Loewenstein G. Strangers on a plane: Context-dependent willingness to divulge sensitive information. *The Journal of Consumer Research*, 2011; 37(5):858–873. <https://doi.org/10.1086/656423>
76. Tsai JY, Egelman S, Cranor L, Acquisti A. The effect of online eprivacy information on purchasing behavior: An experimental study. *Information Systems Research*, 2010; 22(2):254–268. <https://doi.org/10.1287/isre.1090.02604>

77. Mothersbaugh DL, Foxx WK II, Beatty SE, Wang S. Disclosure antecedents in an online service context: The role of sensitivity of information. *Journal of Service Research*, 2012; 15(1):76–98. <https://doi.org/10.1177/1094670511424924>
78. Kokolakis S. Privacy attitudes and privacy behavior: A review of current research on the privacy paradox phenomenon. *Computers & Security*, 2015. <https://doi.org/10.1016/j.cose.2015.07.002>
79. Acquisti A, John L, Loewenstein G. The impact of relative standards on the propensity to disclose. *Journal of Marketing Research*. 2012; 49(2):160–174. <https://doi.org/10.1509%2Fjmr.09.0215>
80. Moon Y. Intimate exchanges: Using computers to elicit self-disclosure from consumers. *Journal of Consumer Research*, 2000; 26(4):323–339. <https://doi.org/10.1086/209566>
81. Tamir DI, Mitchell JP. Disclosing information about the self is intrinsically rewarding. *PNAS*, 2012; 109(21):8038–8043. <https://doi.org/10.1073/pnas.1202129109> PMID: 22566617
82. Andrade EB, Kaltcheva V, Weitz B. Self-disclosure on the web: The impact of privacy policy, reward, and company reputation. *Advances in Consumer Research*, 2002; 29:350–353.
83. Lee H, Park N, Hwang Y. A new dimension of the digital divide: Exploring the relationship between broadband connection, smartphone use and communication competence. *Telemat Inform*, 2015; 32(1):45–56. <https://doi.org/10.1016/j.tele.2014.02.001>
84. Chen Y-H, Chien S-H, Wu J-J, Tsai P-Y. Impact of signal and experience on trust and trusting behavior. *Cyberpsychol Behav Soc Netw*, 2010; 13(5):539–546. <https://doi.org/10.1089/cyber.2009.0188> PMID: 20950178
85. Hui KL, Teo HH, Lee S-YT. The value of privacy assurance: An exploratory field experiment. *MIS Q*, 2007; 31(1):19–33. <https://doi.org/10.2307/25148779>
86. Wu K-W, Huang SY, Yen DC, Popova I. The effect of online privacy policy on consumer privacy concern and trust. *Comput Human Behav*, 2011; 28(3):889–897. <https://doi.org/10.1016/j.chb.2011.12.008>
87. Martin K. Do privacy notices matter? Comparing the impact of violating formal privacy notices and informal privacy norms on consumer trust online. *The Journal of Legal Studies*, 2016; 45(52). <https://doi.org/10.1086/688488>
88. Krol K, Preibusch S. Control versus effort in privacy warnings for webforms. *Proceedings of the 2016 ACM on Workshop on Privacy in the Electronic Society [Internet]; 2016 Oct 16; Vienna, Austria.* <https://doi.org/10.1145/2994620.2994640>
89. Strahilevitz LJ, Kugler MB. Is privacy policy language irrelevant to consumers? *The Journal of Legal Studies*, 2016; 45(S2):S69–S95.
90. Hughes-Roberts T. Privacy as a secondary goal problem: An experiment examining control. *Information and Computer Security*, 2015; 23(4):382–393.
91. Marreiros H, Tonin M, Vlassopoulos M, Schraefel MC. “Now that you mention it”: A survey experiment on information, inattention and online privacy. *Journal of Economic Behavior Organization*, 2017; 140:1–17. <https://doi.org/10.1016/j.jebo.2017.03.024>
92. Tay SW, Teh PS, Payne SJ. Reasoning about privacy in mobile application install decisions: Risk perception and framing. *Int J Hum Comput Stud*, 2020; 145. <https://doi.org/10.1016/j.ijhcs.2020.102517>
93. Thaler RH, Sunstein CR. *Nudge: Improving decisions about health, wealth and happiness*. New York, NY: Penguin; 2009.
94. Acquisti A, Adjerid I, Balebako R, Brandimarte L, Cranor LF, Komanduri S, et al. Nudges for privacy and security: Understanding and assisting users’ choices online. *ACM Computing Surveys*, 2017; 50(3). <https://doi.org/10.1145/3054926>
95. Alemany J, del Val E, Alberola J, García-Fornes A. Enhancing the privacy risk awareness of teenagers in online social networks through soft-paternalism mechanisms. *Int J Hum Comput Stud*. 2019; 129:27–40.
96. Rodríguez-Priego N, van Bavel R, Monteleone S. The disconnection between privacy notices and information disclosure: An online experiment. *Economia Politica*, 2016; 33(3):433–461. <https://doi.org/10.1007/s40888-016-0040-4>
97. Ioannou A, Tussyadiah I, Miller G, Li S, Weick M. Privacy nudges for disclosure of personal information: A systematic literature review and meta-analysis. *PLoS ONE*, 2021; 16(8). <https://doi.org/10.1371/journal.pone.0256822> PMID: 34449821
98. van Bavel R, Rodriguez-Priego N, Vila J, Briggs P. Using protection motivation theory in the design of nudges to improve online security behavior. *Int J Hum Comput Stud*, 2019; 123:29–39. <https://doi.org/10.1016/j.ijhcs.2018.11.003>
99. Molden DC. Understanding priming effects in social psychology: What is “social priming” and how does it occur? *Social Cognition*, 2014; 32:1–11.

100. Sundar S, Kang H, Wu M, Go E, Zhang B. 2013. Unlocking the privacy paradox: Do cognitive heuristics hold the key? CHI '13 Extended Abstracts on Human Factors in Computing Systems. 2013 Apr 27. 811–816. <https://doi.org/10.1145/2468356.2468501>
101. Entman RM. Framing: Toward clarification of a fracture paradigm. *Journal of Communication*, 1993; 43(4):51–58. <https://doi.org/10.1111/j.1460-2466.1993.tb01304.x>
102. Baek YM, Bae Y, Jeong I, Kim E, Rhee JW. Changing the default setting for information privacy protection: What and whose personal information can be better protected? *The Social Science Journal*, 2014; 51(4):523–533. <https://doi.org/10.1016/j.soscij.2014.07.002>
103. Johnson EJ, Bellman S, Lohse GL. Defaults, framing and privacy: Why opting in-opting out. *Marketing Letters*, 2001; 13(1):5–15. <https://doi.org/10.1023/A:1015044207315>
104. Garcia M. Browsewrap: A unique solution to the slippery slope of the clickwrap conundrum. *Campbell Law Rev*, 2013; 36(1):31–44. [http://scholarship.law.campbell.edu/clr?utm\\_source=scholarship.law.campbell.edu%2Fclr%2Fvol36%2Fiss1%2F2utm\\_medium=PDFutm\\_campaign=PDFCoverPages](http://scholarship.law.campbell.edu/clr?utm_source=scholarship.law.campbell.edu%2Fclr%2Fvol36%2Fiss1%2F2utm_medium=PDFutm_campaign=PDFCoverPages)
105. Kunz CL, Del Duca MF, Thayer H, Debrow J. Click-through agreements: Strategies for avoiding disputes on validity of assent. *The Business Lawyer*, 2001; 57(1):401–429. <https://www.steptoe.com/images/content/4/6/v1/4616/220b.pdf>
106. Soe TH, Nordberg OE, Guribye F, Slavkovik M. Circumvention by design—dark patterns in cookie consent for online news outlets. NordiCHI '20: Proceedings of the 11th Nordic Conference on Human-Computer Interaction. 2020 Oct 25–29. <https://doi.org/10.1145/3419249.3420132>
107. Utz C, Degeling M, Fahl S, Schaub F, Holz T. Un(informed) consent: Studying GDPR consent notices in the field. CCS '19: SIGSAC Conference on Computer and Communications Security. 2019 Nov 11–15. <https://doi.org/10.1145/3319535.3354212>
108. Pew Research Center. Research in the crowdsourcing age, a case study [Internet]. 2016 Jul 11. Available from: <https://www.pewresearch.org/internet/2016/07/11/what-is-mechanical-turk/>
109. “Terms of Service” linked to a 1,518-word document at <https://aibr.org/privacy-click/TOSA.html>.
110. “Privacy Policy” linked to a 2,073-word document at [https://aibr.org/privacy-click/privacy\\_policy.html](https://aibr.org/privacy-click/privacy_policy.html).
111. Brysebaert M. How many words do we read per minute? A review and meta-analysis of reading rate, 2019. <https://doi.org/10.31234/osf.io/xynwg>
112. Eggers D. *The Circle*. Knopf; 2013.
113. Maddux JE, Rogers RW. Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology*, 1983; 19(5):469–479. [https://doi.org/10.1016/0022-1031\(83\)90023-9](https://doi.org/10.1016/0022-1031(83)90023-9)
114. Shih D-H, Hsu S-F, Yen DC, Lin C-C. Exploring the individual's behavior on self-disclosure online. *Int J Hum Comput Interact*, 2012; 28(10):627–645. <https://doi.org/10.1080/10447318.2011.654198>
115. Tannenbaum MB, Hepler J, Zimmerman RS, Saul L, Jacobs S, Wilson K, et al. Appealing to fear: A meta-analysis of fear appeals effectiveness and theories. *Psychological Bulletin*, 2015; 141(6):1178–1204. <https://doi.org/10.1037/a0039729> PMID: 26501228
116. Sorokowska A, Oleszkiewicz A, Frackowiak T, Pisanski K, Chmiel A, Sorokowski P. Selfies and personality: Who posts self-portrait photographs? *Personality and Individual Differences*, 2016; 90:119–123.
117. Trepte S, Reinecke L. The reciprocal effects of social network site use and the disposition for self-disclosure: A longitudinal study. *Comput Human Behav*, 2012; 29(3):1102–1112. <https://doi.org/10.1016/j.chb.2012.10.002>
118. Masur PK., DiFranzo D, Bazarova NN. Behavioral contagion on social media: Effects of social norms, design interventions, and critical media literacy on self-disclosure. *PLoS ONE*, 2021; 16(7). <https://doi.org/10.1371/journal.pone.0254670> PMID: 34280233
119. Waheed H, Anjum M, Rehman M, Khawaja A. Investigation of user behavior on social networking sites. *PLoS ONE*, 2017; 12(2). <https://doi.org/10.1371/journal.pone.0169693> PMID: 28151963
120. Yang C. Social media social comparison and identity processing styles: Perceived social pressure to be responsive and rumination as mediators. *Applied Developmental Science*, 2021;:1–12. <https://doi.org/10.1080/10888691.2021.1894149>
121. Evans JR, Mathur A. The value of online surveys. *Internet Research*, 2005; 15(2):195–219. <https://doi.org/10.1108/10662240510590360>
122. Peyton K, Huber GA, Coppock A. The generalizability of online experiments conducted during the COVID-19 pandemic. *Journal of Experimental Political Science*, 2021;:1–16. <https://doi.org/10.1017/XPS.2021.17>
123. Burton JW, Cruz N, Hahn U. Reconsidering evidence of moral contagion in online social networks. *Nat Hum Behav*, 2021. <https://doi.org/10.1038/s41562-021-01133-5> PMID: 34112981

124. Harper RA. The social media revolution: Exploring the impact on journalism and news media organizations. *Inquiries Journal*, 2010; 2(3). Available from: <http://www.inquiriesjournal.com/articles/202/the-social-media-revolution-exploring-the-impact-on-journalism-and-news-media-organizations>
125. Anderson M, Caumont A. How social media is reshaping news [Internet]. Pew Research Center. 2014. Available from: <https://www.pewresearch.org/fact-tank/2014/09/24/how-social-media-is-reshaping-news/>
126. Margetts H. Political behaviour and the acoustics of social media. *Nat Hum Behav*, 2017; 1(4). <https://doi.org/10.1038/s41562-017-0086>
127. Valenzuela S, Rojas H. Taming the digital information tide to promote equality. *Nat Hum Behav*, 2019; 3:1134–1136. <https://doi.org/10.1038/s41562-019-0700-9> PMID: 31384024
128. Balke J. What's with all the privacy notices and website Cookie notifications? [Internet]. Houston Press. Houston Press; 2021. Available from: <https://www.houstonpress.com/news/why-are-you-seeing-privacy-notifications-online-all-of-a-sudden-10510337>
129. Ellison NB, Vitak J, Gray R, Lampe C. Cultivating social resources on social network sites: Facebook relationship maintenance behaviors and their role in social capital processes. *J Comput Mediat Commun*, 2014; 19(4):855–870. <https://doi.org/10.1111/jcc4.12078>
130. Rykov Y, Koltsova O, Sinyavskaya Y. Effects of user behaviors on accumulation of social capital in an online social network. *PLoS ONE*, 2020; 15(4). <https://doi.org/10.1371/journal.pone.0231837> PMID: 32324820
131. Valenzuela S, Park N, Kee KF. Is there social capital in a social network site?: Facebook use and college students' life satisfaction, trust, and participation. *J Comput Mediat Commun*, 2009; 14:875–901. <https://doi.org/10.1111/j.1083-6101.2009.01474.x>
132. Ramnerö J, Törneke N. The ABCs of human behavior: Behavioral principles for the practicing clinician. New Harbinger. 2008.
133. Bravo-Lillo C, Cranor LF, Downs J, Komanduri S, Reeder RW, Schechter S, et al. Your attention please: Designing security-decision UIs to make genuine risks harder to ignore. Symposium on Usable Privacy and Security; 2013 Jul 24–26.
134. Munoz Y, Chebat J, Suissa JA. Using fear appeals in warning labels to promote responsible gambling among VLT players: The key role of depth of information processing. *J Gamb Stud*, 2010; 26:593–609. <https://doi.org/10.1007/s10899-010-9182-4> PMID: 20217197
135. Lindegren D, Karegar F, Kane B, Perrersson JS. An evaluation of three designs to engage users when providing their consent on smartphones. *Behaviour & Information Technology*, 2019; 40(4):398–414. <https://doi.org/10.1080/0144929X.2019.1697898>
136. Mendel J, Mayhorn CB, Hardee JB, West RT, Pak R. The effect of warning design and personalization on user compliance in computer security dialogs. Proceedings of the Human Factors and Ergonomics Society 54th Annual Meeting. 2010. <https://doi.org/10.1177/154193121005402312>
137. Sundar RP, Becker MW, Bello NM, Bix L. Quantifying age-related differences in information processing behaviors when viewing prescription drug labels. *PLoS ONE*; 2012;7(6);e38819. <https://doi.org/10.1371/journal.pone.0038819> PMID: 22719955
138. DeCarlo TE. Alcohol warnings and warning labels: An examination of alternative alcohol warning messages and perceived effectiveness. *The Journal of Consumer Marketing*, 1997; 14(6):448–460. <https://doi.org/10.1108/07363769710186060>
139. Fleming P, Bayliss AP, Edwards SG, Seger CR. The role of personal data value, culture and self-construal in online privacy behaviour. *PLoS ONE*, 2021; 16(7). <https://doi.org/10.1371/journal.pone.0253568> PMID: 34270577
140. Dincelli E, Goel S. Research design for study of cultural and societal influence on online privacy behavior. Proceedings of IFIP 8.11/11.13 Dewald Roode Information Security Research Workshop; 2015. Available from: [https://www.researchgate.net/publication/282252158\\_Research\\_Design\\_for\\_Study\\_of\\_Cultural\\_and\\_Societal\\_Influence\\_on\\_Online\\_Privacy\\_Behavior](https://www.researchgate.net/publication/282252158_Research_Design_for_Study_of_Cultural_and_Societal_Influence_on_Online_Privacy_Behavior)
141. Hofstra B, Corten R, van Tubergen F. Understanding the privacy behavior of adolescents on Facebook: The role of peers, popularity and trust. *Comput Human Behav*, 2016; 60:611–621. <https://doi.org/10.1016/j.chb.2016.02.091>
142. Edu JS, Such JM, Suarez-Tangil G. Smart home personal assistants: A security and privacy review. *ACM Computer Survey*, 2020; 53(6). <https://doi.org/10.1145/3412383>
143. Stanley J. The privacy threat from always-on microphones like the Amazon Echo [Internet]. ACLU. 2017. Available from: <https://www.aclu.org/blog/privacy-technology/privacy-threat-always-microphones-amazon-echo>

144. Verheyden T, Baert D, Van Hee L, Van Den Heuvel R. Google employees are eavesdropping, even in your living room, VRT NWS has discovered [Internet]. VRT NWS. 2019. Available from: <https://www.vrt.be/vrtnws/en/2019/07/10/google-employees-are-eavesdropping-even-in-flemish-living-rooms/>
145. Whitney L. Google closes \$3.2 billion purchase of Nest [Internet]. CNET. 2014. Available from: <https://www.cnet.com/tech/services-and-software/google-closes-3-2-billion-purchase-of-nest/>
146. Pino N. Google fesses up to Nest Secure's undisclosed microphone [Internet]. TechRadar. 2019. Available from: <https://www.techradar.com/news/google-fesses-up-to-nest-secures-undisclosed-microphone>
147. Porter J. Google claims built-in Nest mic was 'never intended to be a secret' [Internet]. The Verge. 2019. Available from: <https://www.theverge.com/circuitbreaker/2019/2/20/18232960/google-nest-secure-microphone-google-assistant-built-in-security-privacy>
148. Zuboff S. The age of surveillance capitalism: The fight for a human future at a new frontier of power (p. 7). Public Affairs. 2019.
149. Epstein R. Google's dance [Internet]. TIME. 2013 Mar. Available from: <https://techland.time.com/2013/03/27/googles-dance/>
150. Epstein R. Free isn't freedom: How Silicon Valley tricks us [Internet]. Motherboard. 2016. Available from: <https://www.vice.com/en/article/8q8vav/free-isnt-freedom-epstein-essay>
151. Schneier B. Surveillance as a business model [Internet]. Schneier on Security. 2013. Available from: [https://www.schneier.com/blog/archives/2013/11/surveillance\\_as\\_1.html](https://www.schneier.com/blog/archives/2013/11/surveillance_as_1.html)
152. Torbert PM. "Because it is wrong": An essay on the immorality and illegality of the online service contracts of Google and Facebook. *Journal of Law, Technology, and the Internet*, 2021; 12(1). Available from: <https://scholarlycommons.law.case.edu/jolti/vol12/iss1/2/>