Trust and Online Privacy Concerns in a General Population of Internet Users

STELIOS STYLIANOU[♦]
Cyprus University of Technology, Cyprus

Even though research on online privacy has been accumulating for the last two decades, the etiology of online privacy concerns is still open to more inquiry. The present study investigates whether and to what extent online privacy concerns are affected by trust, a variable that has received limited dedicated attention in this respect. Using data from a telephone survey of a representative sample of the general population of Internet users in a Mediterranean society, the study models trust in people and trust in institutions as the focal predictors of Internet users' concerns about online privacy violations by other people, corporations, and governments. Five hypotheses are tested using multiple regression equations with several controls, including measures of offline and online social capital, digital literacy, length of Internet use, and privacy violation experience. The study concludes that trust, independently and consistently, albeit mildly, reduces online privacy concerns.

Keywords: online privacy concerns, trust in people, trust in institutions, social capital, digital literacy, privacy violation, general population survey

Understanding Internet users' concerns about online privacy is a challenging project. Communication research has shown that many users perceive threats to privacy as marginal or trivial, as they underestimate the risks or are overwhelmed by the benefits of online communication (Barth & de Jong, 2017). Some users do away with privacy concerns altogether, as they feel that they "have nothing to hide," a rather myopic consideration (Marwick & Hargittai, 2019; Solove, 2007, 2011). At the same time, partly because of recent alarms, such as the Cambridge Analytica data-mining scandal and Edward Snowden's revelations about mass surveillance, Internet users are becoming more aware and potentially more concerned about privacy (Blank, Dutton, & Lefkowitz, 2019; Madden & Rainie, 2015; Paine, Reips, Stieger, Joinson, & Buchanan, 2007). Consider, for example, the increasing use of anonymity-granting web-browsing applications, such as Tor, the use of which has been shown to result not so much from people's need to engage in illicit activities on the dark web, but more so from concerns arising from mass surveillance apocalypses (Lindner & Xiao, 2020) or from the needs of people who seek to avoid monitoring by repressive states (Jardine, 2018).

Stelios Stylianou: stelios.stylianou@cut.ac.cy
Date submitted: 2022-07-08

Online privacy concerns have mostly been studied as an *independent variable*, hypothesized to affect online behavior. A challenging observation in this research strand is the privacy paradox (Barnes, 2006): Despite growing concerns, people do use Internet services and sites that record personal information and do disclose or allow access to such information (Debatin, Lovejoy, Horn, & Hughes, 2009). Although effects of privacy concerns on privacy-protective behaviors have been detected, these are mild to moderate at best (Baruh, Secinti, & Cemalcilar, 2017; Dienlin, Masur, & Trepte, 2023; Preibusch, 2015). Various explanations of this paradox have been proposed. Barth and de Jong (2017) have mapped 35 theories of decision making about privacy-related behaviors and Kokolakis (2017) has detected in the literature more than 10 different theoretical or methodological explanations. Recent studies have also introduced new concepts, such as a reverse privacy paradox (Miltgen & Peyrat-Guillard, 2014), privacy cynicism (Lutz, Hoffmann, & Ranzini, 2020), and privacy fatigue (Tang, Akram, & Shi, 2021).

The rich literature outlined above is not coupled with equivalent attention to the causes of online privacy concerns. The corresponding strand of research, which models privacy concerns as the *dependent variable*, has produced important insights, but not safe conclusions. The purpose of the present study is to contribute to this line of research by focusing on the causes of online privacy concerns; specifically, on one that has received limited dedicated attention: *trust*. The study models trust as the focal cause of online privacy concerns, controlling for other theoretically relevant predictors, to report on its empirical performance, rather than to propose, test, or amend a particular theory. Consequently, the contribution of the study is in the assessment of the empirical validity of any model that predicts a causal effect of trust on online privacy concerns.

Online Privacy Concerns

Starting with the concept of privacy, various definitions have been proposed, mostly fueling debates rather than leading to consensus (Nissenbaum, 2009; Tavani, 2007). Solove (2007) argued that "the quest for a traditional definition of privacy has led to a rather fruitless and unresolved debate" (p. 759), to suggest that issues related to privacy can be dealt with without a single definition. Some convergence in the conception of privacy has been documented by Bélanger and Crossler (2011), who observed that researchers in many fields have approached privacy as "one's ability to control information about oneself" (p. 1018). Although not without criticism (e.g., Trepte, 2021), defining privacy as control has gained popularity in communication research.

Smith, Dinev, and Xu (2011) suggested that definitions of privacy are either "value-based" (privacy as a human right) or "cognate-based" (privacy as a psychological state; pp. 994–995). The latter approach reduces privacy to an object that can be accommodated under various theoretical approaches. For example, privacy as a psychological state can be conceived as a construct constituted by conditions, such as anonymity, solitude, reserve, and intimacy (Westin, 1967), as the belief of ownership of private information and the right to protect it (Petronio, 2002), or as the ability to control such information (Smith et al., 2011). Following this approach, the present study defines privacy as a state whereby (private) information about the individual is not shared against the individual's will.

Consistently, the concept of *privacy concerns* stands for concerns that (private) information about the individual could be shared against the individual's will. Since the focus of the present study is on online privacy concerns, the definition applies to online communication. Based on Li (2011), this definition is general, rather than specific, as it refers to overall concerns and not to concerns about specific platforms or services. Deliberately, the definition does not specify what information is shared, how or when it is shared, and with whom it is shared. This approach is appropriate here, as privacy concerns are modeled as a dependent variable, hypothetically affected by trust, social capital, and other variables, whose "impacts on privacy concerns are irrelevant of contexts" (Li, 2011, p. 467), and not as a predictor of personal data disclosure or privacy-protecting behaviors, where a specific definition would be more appropriate (Bartol, Vehovar, & Petrovčič, 2021).

Another issue that has received attention is whether privacy concerns is a unidimensional or a multidimensional concept. A well-established scale (Smith, Milberg, & Burke, 1996) includes four dimensions of concern about personal data: collection, unauthorized secondary use, improper access, and errors. Stewart and Segars (2002) suggested that, although these dimensions are reliable, considerable common variation among them implies the existence of a higher-order factor. Jia and Xu (2016) suggested that privacy concerns about social networking sites can be conceptualized both as three separate dimensions of concern (control, access, and diffusion) and as one second-order factor. Similarly, Männiste and Masso (2018) factor-analyzed general population survey data about concerns for privacy violations by nine different entities (including institutions, companies, and individuals), and supported both a two-factor and a one-factor solution. Following this discussion, the present study first models three measures of concerns about online privacy violations (by individuals, corporations, and governments) as separate outcomes and then models a privacy concerns construct as a single outcome.

Etiology of Online Privacy Concerns

The question guiding the present inquiry is what makes Internet users more (or less) concerned that their privacy is violated online. Various answers to this question have been proposed and empirically investigated. Miltgen and Peyrat-Guillard (2014) presented a review of empirical studies, listing hypotheses about causes at the micro level (e.g., demographics, psychological traits, skills, experiences), the contextual level (e.g., the reputation of organizations, privacy policy, rewards), and the macro level (e.g., culture and formal regulations). They discuss trust separately to stress its importance and to note that its causal role is still unclear.

Trust

The concept of trust is neither new nor exclusive to communication studies. In a functionalist sociological sense, trust is the core ingredient of social solidarity and society is only possible given a certain amount of trust (Misztal, 1992). The rational-utilitarian tradition in social philosophy, while being at odds with functionalist assumptions, also places trust in the center of theoretical interest, as absent rather than present; hence, the vital role of rationality in the classical theories of Hobbes and Bentham. The corresponding rational choice tradition in the social sciences descends at the micro level to study the rational, self-interested, profit-maximizing individual. Social exchange theory (Cook & Rice, 2003; Homans, 1961), in particular, explains social behavior as the outcome of rational decision making, whereby the individual chooses to follow a course of action if its perceived benefits outweigh its perceived costs. In this theoretical context, trust is a modifier of perceived costs. In offline and online communication, trust is expected to reduce the perceived risks of personal information disclosure and therefore reduce privacy concerns (Metzger, 2004). This proposition is consistent with Trepte's (2021) social media privacy model, which suggests that trust, together with interpersonal communication and norms, can substitute for the desire for control in social media use.

Empirical evidence on the effect of trust on privacy concerns is conflicting. Notably, Chen, Beaudoin, and Hong (2016) reported no significant association between trust and online privacy concerns in a sample of adolescents, while Bergström (2015) found trust in people to be "the single most important factor explaining privacy concerns among people using digital media and applications" (p. 425). Turow and Hennessy (2007) found that general trust in the Internet is associated with beliefs that institutions are more likely to help users protect their privacy and less likely to disclose sensitive information against users' will. Männiste and Masso (2018) reported that trust in government, state, and media institutions significantly reduces concerns about institutional privacy violations. Reviewing this literature confirms that more research is needed on the effect of trust on online privacy concerns.

The present study models trust as a direct predictor of online privacy concerns to measure its empirical performance. As several theoretical approaches link trust to privacy concerns (see a review by Rohunen, 2020), the present empirical assessment can serve as a reference for studies that test theories of this nature, as well as in the overall assessment of the role of trust in privacy-related beliefs, attitudes, and behaviors.

Social Capital

The concept of social capital is also not new. According to Portes (1998), the notion that group participation can be beneficial for both the individual and the community dates back to "Durkheim's emphasis on group life as an antidote to anomie and self-destruction and to Marx's distinction between an atomized class-in-itself and a mobilized and effective class-for-itself" (p. 2). Since the late 20th century, conceptual discussions and empirical studies of social capital have flourished at all levels of analysis (Coleman, 1988; Granovetter, 1973; Putnam, 2000). With the advent of online social networking, the concept has gone through further theoretical development, as different forms of online participation can have different effects on different forms of social capital (Shane-Simpson, Manago, Gaggi, & Gillespie-Lynch, 2018).

For the current discussion, social capital refers to the actual or potential resources available to individuals through social networks. At the individual level, higher levels of social capital are associated with higher levels of safety, support, opportunities, and overall well-being. According to Urwin, Di Pietro, Sturgis, and Jack's (2008) categorization, which is based on Granovetter (1973) and Putnam (2000), there are three dimensions of social capital. *Bonding social capital* refers to strong ties among members of exclusive and relatively homogenous networks, such as families and groups of close friends. *Bridging social capital* refers to weak ties among members of more extended groups, such as groups of colleagues or associates or occupational or professional networks. Finally, *linking social capital* refers to relationships "between individuals and institutions or groups in various social strata" (Urwin et al., 2008, p. 946). To study the full spectrum of social capital dimensions, it is necessary to look at both offline and online networks. Offline networks are social capital by definition. Online networks, too, as repeatedly confirmed, are associated with increased levels of social capital (Ahn, 2012; Shane-Simpson et al., 2018; Valenzuela, Park, & Kee, 2009).

Digital Literacy

Digital literacy refers to skills related to digital communication. In a typology presented by Friemel and Signer (2010), Web 2.0 literacy comes in four types: receptive knowledge, productive knowledge, receptive use, and productive use. Studies have detected associations between aspects of literacy, privacy concerns, and privacy-protective behaviors. Yao, Rice, and Wallis (2007) showed that Internet use fluency increases privacy concerns indirectly through beliefs in privacy rights. Park (2013) reported a positive effect of three dimensions of digital literacy on information-control behavior. Bartsch and Dienlin (2016) reported a positive association between privacy literacy and perceived privacy safety. These findings justify the inclusion of digital literacy as a control variable in models of online privacy concerns.

Length of Internet Use

The length of Internet use is related to privacy concerns in at least three ways. First, the longer individuals use the Internet, the more aware they are expected to be about privacy-related issues. More experienced users have different attitudes compared with less experienced users, typically, but not always, in the direction of being less concerned (Metzger, 2004). Second, the longer individuals use the Internet, the more literate they are expected to be about privacy-protective knowledge and skills (Park, 2013). Finally, the length of Internet use may simply correlate with age; thus, its effect on privacy concerns may be spurious. Yet, such a correlation should not be assumed. Kezer, Sevi, Cemalcilar, and Baruh (2016) reported that the average number of years of Internet use in a sample of 600 users aged 18–85 was about the same (between 8 and 9 years) for all age groups. Thus, it is safer to model age and length of Internet use as separate predictors.

Privacy Violation Experience

A consistent finding in the literature is that experience with online privacy violations increases online privacy concerns (Li, 2011), especially when the violation victimizes users themselves, rather than other users (Baek, Kim, & Bae, 2014; Debatin et al., 2009). Recently, Masur and Trepte (2021) reported mild effects of privacy violation experiences on privacy concerns cross-sectionally and small effects longitudinally. These findings justify controlling for privacy violation experience when studying privacy concerns as the outcome variable.

Demographics

About *gender*, women are generally more concerned about online privacy (Baruh et al., 2017; Tifferet, 2019). Still, some studies report no gender effect (Paine et al., 2007; Yao et al., 2007). Research on the effect of *age* on privacy concerns has also produced mixed results (Li, 2011). Some studies show that concerns increase with age (Kezer et al., 2016; Paine et al., 2007). Männiste and Masso (2018) found that younger users are more concerned about online privacy violations by individuals but not by institutions. Miltgen and Peyrat-Guillard's (2014) analysis of focus group data in seven European countries shows that younger individuals are less worried about privacy than older individuals, as they feel safer concerning legal protection and more confident in their self-protection skills. Findings on the effects of *education* on privacy concerns or related constructs are mixed. Education was found to be positively associated with concerns about institutional privacy violations by Männiste and Masso (2018). Park (2013), on the other hand, found no effect of education on skills of information control on the Internet. Finally, about *income*, Baek, Kim, and Bae (2014) found no effect on perceived online risks and privacy-protective behaviors, Männiste and Masso (2018) reported no effect on privacy concerns, and Park (2013) found no effect on skills of information control on the Internet. Yet, in a U.S. survey (Madden & Rainie, 2015), respondents from the highest-income households were slightly more likely than respondents from lowest-income households to believe that there are sufficient limits on what data the government collects through surveillance of electronic communications.

Conceptualization and Hypotheses

The present study models online privacy concerns as the dependent variable. Measures of concern about online privacy violations by individuals, corporations, and governments are first modeled separately. Then, a privacy concerns construct, which combines the three measures of concern, is modeled as a single outcome.

The focal predictor is trust. Two conceptual points must be stressed. First, trust, as conceptualized here, refers to *general* trust, a general expectation that the community and its members are trustworthy (Fukuyama, 1995). This is conceptually different from *specific* trust, which refers to perceived trustworthiness of specific organizations (Beldad, de Jong, & Steehouder, 2011), online social network providers or other users (Krasnova, Spiekermann, Koroleva, & Hildebrand, 2010), or firms in the context of e-commerce (Malhotra, Kim, & Agarwal, 2004). In those contexts, trust is a function of concern: the more concerned individuals are about privacy violations, the more skeptical they are expected to be in trusting specific entities. In the present study, concern is a function of trust: the more individuals believe that other people and institutions can, in general, be trusted, the less concerned they are expected to be about their privacy being violated by such entities.

Second, a distinction between trust and social capital is of critical importance. In most conceptualizations (Bourdieu, 1986; Coleman, 1988; Putnam, 2000), trust is a component of individual social capital: by virtue of trust, other people and institutional structures are resources for individuals to promote their well-being and personal development. Consistently, empirical studies typically model trust as a dimension of social capital (Scheufele & Shah, 2000; Valenzuela et al., 2009). The approach of the present study is to model trust as a separate variable. Methodologically, this allows estimating the independent effect of trust on privacy concerns over and above the effects of social capital. This approach is justified in substantive terms as well, as it applies an analytical separation of structural and individual components. By excluding trust from the social capital construct, what stays is the structural component, that is, resources and relationships that individuals can use to promote their well-being. These *objective* measures of social capital are independent of individual beliefs. Trust is a *subjective* measure, an individual belief, and it is as such that it is expected to affect privacy concerns, as hypothesized.

In social psychological terms, trust is an element of the social bond to significant and generalized others. Putnam (2000) termed these two types *thick* and *thin* trust, respectively. The latter type is what the present study models as a predictor of online privacy concerns. Following Fukuyama (1995), who defined trust as "the expectation that arises within a community of regular, honest, and cooperative behavior, based on commonly shared norms, on the part of other members of that community" (p. 26), *trust in people* is defined here as the expectation that other people will tend to honor rather than violate norms of reciprocity: they will be honest, fair, and helpful. It follows that people who tend to trust others will tend to feel less threatened by others; thus, the first hypothesis of the study is:

H1: Trust in people reduces concerns about online privacy violations by other people.

Consistently, *trust in institutions* is the expectation that institutions will tend to honor rather than violate norms governing their operation and it follows that the more people trust institutions, the less threatened by institutional entities they will feel. This leads to the next two hypotheses:

H2: Trust in institutions reduces concerns about online privacy violations by corporations.

H3: Trust in institutions reduces concerns about online privacy violations by governments.

Finally, the three sources of concern (individuals, corporations, and governments), which are the outcomes in the first three hypotheses, are merged into a single construct of overall privacy concerns, leading to two more hypotheses:

H4: Trust in people reduces overall concerns about online privacy violations.

H5: Trust in institutions reduces overall concerns about online privacy violations.

Following the literature on the etiology of online privacy concerns, all models include dimensions of social capital, digital literacy, length of Internet use, privacy violation experience, gender, age, education, income, and residence area type as control variables. As the focus of the study is on trust, the effects of these variables are not evaluated in separate hypotheses. These effects are controlled for by using multiple regression analysis. The purpose of the study is better served by this approach, as the analysis is more sharply focused on trust without compromising internal validity.

Operationalization

Online Privacy Concerns

To measure online privacy concerns, the present study's questionnaire included three statements, each followed by a 5-point Likert scale, from *strongly agree* to *strongly disagree*, coded from 1 to 5, with higher values standing for more agreement:[1]

[1] For a discussion about the operationalization of privacy concerns, see Preibusch (2013).

> I am concerned other people are violating my privacy online.
>
> I am concerned corporations are violating my privacy online.
>
> I am concerned governments are violating my privacy online.

The statements specify the source of concern (individuals, corporations, and governments) and measure exactly what is under study as a dependent variable, that is, concerns.

Trust

Trust in people was measured with three items, which, since their introduction by Rosenberg (1956), have been used widely (Putnam, 2000). The items on the questionnaire were phrased as follows:

> Generally speaking, would you say that most people can be trusted or that you can't be too careful in dealing with people? Please tell me on a scale of 0–10, where 0 means you can't be too careful and 10 means that most people can be trusted.
>
> Do you think that most people would try to take advantage of you if they got the chance, or would they try to be fair? Please tell me on a scale of 0–10, where 0 means most people would try to take advantage of you and 10 means that most people would try to be fair.
>
> Would you say that, most of the time, people try to be helpful or that they are mostly looking out for themselves? Please tell me on a scale of 0–10, where 0 means people mostly look out for themselves and 10 means that people mostly try to be helpful.

For trust in institutions, participants were asked to say, on a scale from 0 (*absolutely*) to 10 (*not at all*), to what degree they trust each of five major institutions: the parliament, public administration, political parties, the police, and the media.

Other Variables

Offline bonding social capital was operationalized in terms of frequency of spending time with close relatives (parents, siblings, spouse or partner, and children), other relatives, and friends or acquaintances. The answers (*daily or almost daily*, *a few times a week*, *a few times a month*, *a few times a year*, and *never or almost never*) were coded from 1 to 5, with higher values corresponding to higher frequencies. Offline bridging social capital was operationalized in a question about the frequency of spending time with colleagues outside the work environment, with the same answer options and coding. Offline linking social capital was measured in terms of membership (*yes*/*no*) in each of the seven types of organized groups (cultural, religious, professional, political, environmental, sport or recreation, and charity). For online social capital, respondents were asked to say to what extent they use the Internet for each of 10 online networking activities (presented later in the Analysis and Findings section), with 5-point answer options ranging from *to a great extent* to *not at all*, coded from 1 to 5, with higher values standing for more use.

Digital literacy was measured with respect to Friemel and Signer's (2010) Web 2.0 receptive and productive knowledge literacies. Participants were asked about their knowledge of five specific Internet use tasks ("I know how to open downloaded files, I find it easy to decide on the best keywords for online search, I know how to change who I share content with, I know how to create and upload content," and "I know how to download apps to a mobile device") on a 5-point Likert scale, from 1 (*strongly disagree*) to 5 (*strongly agree*). The length of Internet use was measured with the question "How many years have you used the Internet?" with answers coded 1 (0–4 years), 2 (5–9 years), 3 (10–14 years), 4 (15–19 years), and 5 (20 or more years).

Gender was coded 1 for male and 0 for female. Age was computed from the participant's year of birth. Education was recorded on a 6-level ordinal scale: *primary school or lower*, *secondary school/middle school*, *attending high school*, *high school graduate/vocational school*, *attending or attended university*, and *college or university degree or higher*. For income, participants were asked about the gross monthly income of their households (for young students, this was the parents' households even if they lived apart). Answer options ranged from *0 to 1,000 euros* (ordinal level 0) to *more than 10,000 euros* (ordinal level 10). Finally, participants were asked whether their areas of residence were urban (coded 1) or rural (coded 0).

Sampling and Measurement

The data were collected through a national telephone survey of individuals 15 years old or older in a Mediterranean society. The survey was conducted as part of the *World Internet Project*, an ongoing international survey project on Internet use, directed by the Annenberg School for Communication and Journalism at the University of Southern California. The instrument used included core items required by the project and additional items, including measures of trust and social capital. The survey was implemented in the society of reference in late 2016 by a research team of graduate and undergraduate communication students trained by the author.

The representativeness of the sample was a priority. This is an important feature of the present investigation, as studies of Internet use and related issues often compromise external validity for convenience (hence, the use of student- or online-recruited samples in most otherwise well-designed published studies). The sample was obtained by a two-stage random process. First, telephone numbers (corresponding to households) were selected by systematic random sampling from the print version of the national telephone directory.[2] Once communication was established with a selected household, one household member was selected for participation by simple random sampling, using a random number

[2] The print version of the directory is a continuous list of landline numbers organized by residential entity (by city for the urban areas and by town/village for the rural areas) and then alphabetically. Applying systematic random sampling on such a list returns a random sample proportionately stratified by residential entity, as the number of times that the sampling interval fits in each entity is proportional to the entity's population size.

generator and the age order of the residents. The cooperation rate (number of successful interviews as a percentage of successful communications) was 26.7%. To correct for group differences in cooperation rates, the final data set (*N* = 926) was postweighted by gender, age, and level of education.

Only Internet users (*N* = 655) are included in the present analysis. The final sample composition is as follows: gender: 49.7% women; area of residence: 36.6% rural; age: mean 37.12 years, *SD* = 15.85 years; education: mean 4.85 (ordinal scale of 1–6), *SD* = 1.24; income: mean 1.94 (ordinal scale of 0–10), *SD* = 1.57.[3]

Analysis and Findings

Variable Profiles

Table 1 shows information about the dependent variables: the three empirical measures (Y_1, Y_2, and Y_3) and the Privacy Concerns Index (Y_4), which was obtained by addition of the empirical variables. All variables behave well in terms of distribution and reliability.

Table 1. Online Privacy Concerns Variables.

Variables	Min	Max	Mean	*SD*	Skewness	Kurtosis	Cronbach's α	Valid *N*
Concern about privacy violations by other people (Y_1)	1	5	3.30	1.08	−.32	−1.11		649
Concern about privacy violations by corporations (Y_2)	1	5	3.30	1.09	−.25	−1.18		649
Concern about privacy violations by governments (Y_3)	1	5	3.13	1.12	−.01	−1.30		650
Privacy Concerns Index (Y_4)	3	15	9.73	2.75	−.22	−.62	.785	647

[3] All cases were valid on the demographic variables, except for areas of residence (valid *N* = 644) and income (valid *N* = 374). The consequences of the low response rate on income were examined. First, participants who did not answer the question were compared to those who did on all other variables. The key finding was that the two groups did not differ on the dependent variable. Second, a binary logistic model was estimated, with an income-respondent/income-nonrespondent binary as the dependent variable and all other variables as predictors. The coefficient for the Privacy Concerns Index was not significant. These two analyses confirm that answering the income question is not related to the dependent variable; thus, the missing values can be said to be missing at random (MAR). Finally, the equations of the present analysis were reestimated with mean-substituted missing values. All trials yielded nonsignificant coefficients for the missing-substituted income variable and a lower R^2 compared to the reported models.

Information about the variables representing trust in people is presented in Table 2. The three empirical measures were combined in a Trust in People Index (*X_1*) by simple addition.

Table 2. Trust in People Variables.

Variables	Min	Max	Mean	*SD*	Skewness	Kurtosis	Cronbach's α	Valid *N*
Most people can be trusted	0	10	3.97	2.23	−.17	−.42		634
Most people would try to be fair	0	10	4.24	2.28	−.06	.02		634
Most of the time people try to be helpful	0	10	3.66	2.38	.06	−.39		635
Trust in People Index (X_1)	0	30	11.87	5.35	−.19	.04	.672	634

Information about the variables representing trust in institutions is presented in Table 3. The five empirical measures were combined in a Trust in Institutions Index (X_2) by simple addition.

Table 3. Trust in Institutions Variables.

Variables	Min	Max	Mean	*SD*	Skewness	Kurtosis	Cronbach's α	Valid *N*
Trust in the parliament	0	10	3.51	2.40	−.05	−.97		621
Trust in public administration	0	10	3.95	2.28	−.19	−.50		619
Trust in political parties	0	10	2.62	2.27	.44	−.57		609
Trust in the police	0	10	4.99	2.45	−.35	−.40		626
Trust in the media	0	10	4.37	2.51	−.27	−.65		630
Trust in Institutions Index (X_2)	0	50	19.25	9.47	−.07	−.63	.857	600

Offline social capital variables are presented in Table 4. Three empirical measures operationalizing offline bonding social capital (spending time with close relatives, other relatives, and friends or acquaintances) were added up in an Offline Bonding Social Capital Index. Offline bridging social capital is presented as operationalized (spending time with colleagues outside the work environment).[4] The empirical variables measuring offline linking social capital produced skewed results, as only small percentages in the sample reported membership in organizations or organized groups (11.7% cultural, 4.3% religious, 13.1% professional,

[4] The four variables measuring time spent with other people (close relatives, other relatives, friends or acquaintances, and colleagues) were also factor analyzed. As expected, the first three loaded on one factor (eigenvalue 1.42; loadings .79, .72, and .53, respectively) and the fourth on a second factor (eigenvalue 1.12). Still, as the reliability of the three-item index was low, the underlying structure of the data was not as clear as desired. To secure that the predictive power of these items was not compromised by data reduction, all equations were reestimated with the three empirical items as separate predictors. The results were the same in terms of direction and statistical significance and similar in terms of R^2. Thus, the three-item index was preferred.

6.5% political, 6.1% environmental, 15.0% sport or recreation, and 15.8% charity). Thus, the seven binaries were merged into a ratio variable representing the number of memberships (61.1% of valid cases had zero memberships, 22.3% one, 8.2% two, 4.2% three, 1.7% four, 1.7% five, and 0.8% had six memberships).

Table 4. Offline Social Capital Variables.

Variables	Min	Max	Mean	*SD*	Skewness	Kurtosis	Cronbach's α	Valid *N*
Offline Bonding Social Capital Index	3	15	12.18	1.73	−1.01	1.74	.444	640
Offline Bridging Social Capital	1	5	2.41	1.30	0.35	−1.10		631
Offline Linking Social Capital	0	7	0.72	1.19	2.16	4.88		637

Online social capital was measured with 10 items. An exploratory factor analysis yielded three factors with eigenvalues greater than one that correspond well to the three dimensions of online social capital: bonding social capital (using the Internet "to conserve existing relationships with your family" and "to conserve and maintain relationships with your friends"), bridging social capital (using the Internet "to expand your professional and occupational ties, to meet people who are different from you, such as people from other occupations or people of different social status," and "to meet people who are different from you, such as people of a different lifestyle or people from other cultures"), and linking social capital (using the Internet "to connect with political parties locally or internationally"; "to connect with local or international nongovernmental organizations"; "to connect with public officials"; and "to join protest or other social movements").[5] Based on these results, three indices were constructed by addition of the empirical variables loading on each factor (presented in Table 5).

Table 5*. *Online Social Capital Variables.

Variables	Min	Max	Mean	*SD*	Skewness	Kurtosis	Cronbach's α	Valid *N*
Online Bonding Social Capital Index	2	10	6.45	2.31	−.320	−.756	.670	650
Online Bridging Social Capital Index	3	15	6.21	3.10	.684	−.532	.729	650
Online Linking Social Capital Index	4	20	5.78	2.94	1.95	3.25	.834	648

For digital literacy, the five empirical variables were added together to form a Digital Literacy Index (ranging from 5 to 25, mean = 20.55, *SD* = 4.34, valid *N* = 645, Cronbach's α = .845). The length of Internet use is distributed as follows: 0–4 years, 12.4%; 5–9 years, 28.9%; 10–14 years, 31.0%; 15–19 years, 15.3%; and, 20 or more years, 12.3%. For privacy violation experience, 6.2% of the sample responded affirmatively. A binary variable, coded 1 for violation and 0 for no violation, was used in the equations.

[5] One item, "using the Internet to maintain relationships with people who share your political views," loaded on two factors and was excluded from further analysis.

Test Results

To test the five hypotheses, OLS regression equations were estimated for each dependent variable. All predictors were entered together and kept in each equation. Collinearity diagnostics did not reveal any variance inflation issues in any of the equations. Statistical significance is applied for hypothesis testing, with $p < .05$ allowing rejection of the null hypothesis. Substantive significance is examined by looking at the size of each statistically significant effect. For this purpose, both unstandardized and standardized regression coefficients are reported for each predictor. The coefficient of determination (R^2) for each equation is reported with and without the two trust variables (X_1 and X_2). The improvement in R^2 because of the inclusion of X_1 and X_2 is assessed by an F_{change} test. The results are presented in Table 6.

Table 6. Unstandardized and (Standardized) OLS Regression Coefficients for the Effects of Independent Variables on Privacy Concerns.

	Dependent Variables (Privacy Concerns)			
	Equation 1	Equation 2	Equation 3	Equation 4
	Other People	Corporations	Governments	All Concerns
Independent Variables	(Y_1)	(Y_2)	(Y_3)	(Y_4)
Gender (male)	−.014 (−.006)	.253 (.113)*	.141 (.062)	.380 (.068)
Age	−.006 (−.085)	−.004 (−.053)	−.004 (−.054)	−.014 (−.077)
Education	−.023 (−.024)	.030 (.033)	−.037 (−.040)	−.030 (−.013)
Income	−.002 (−.003)	.029 (.040)	−.009 (−.012)	.018 (.010)
Residence area type (urban)	.051 (.022)	−.170 (−.072)	−.135 (−.057)	−.254 (−.043)
Digital literacy	−.035 (−.138)*	−.009 (−.038)	−.037 (−.144)*	−.081 (−.129)*
Length of Internet use	−.010 (−.010)	−.044 (−.047)	−.001 (−.001)	−.055 (−.023)
Privacy violation experience	.490 (.112)*	.124 (.029)	.615 (.140)*	1.229 (.113)*
Offline bonding social capital	−.088 (−.127)*	−.149 (−.218)**	−.087 (−.125)*	−.324 (−.189)**
Offline bridging social capital	.177 (.198)**	.084 (.096)	.106 (.118)*	.367 (.166)**
Offline linking social capital	.066 (.077)	.061 (.072)	.085 (.099)	.211 (.100)
Online bonding social capital	.037 (.077)	−.023 (−.048)	.023 (.047)	.037 (.031)
Online bridging social capital	−.006 (−.017)	.040 (.116)	.016 (.046)	.051 (.058)
Online linking social capital	.024 (.066)	.015 (.041)	.060 (.166)*	.098 (.110)
Trust in people (X_1)	−.027 (−.130)*	−.019 (−.091)	−.015 (−.071)	−.061 (−.117)*
Trust in institutions (X_2)	−.010 (−.089)	−.013 (−.115)*	−.015 (−.132)*	−.039 (−.135)*
R^2 without X_1 and X_2	.094	.101	.140	.134
R^2 with X_1 and X_2	.124	.127	.167	.173
F_{change}	5.268**	4.685*	4.991**	7.400**

Note. Valid *N* (all equations) = 331. Statistical significance reference: * $p < .05$, ** $p < .01$

Equation 1 corresponds to H1 ($X_1 \longrightarrow Y_1$). The coefficient for X_1 is negative and statistically significant; thus, H1 is supported. The size of the standardized coefficient (−.130) shows a mild effect. The actual substantive effect is given by the unstandardized coefficient with respect to the units of measurement: ceteris paribus, one unit increase in X_1 causes .027 of a unit decrease in Y_1. Given that X_1 has a theoretical range of 30 units (see Table 2) and Y_1 a theoretical range of four units (see Table 1), the effect is mild.[6] These results support that trust in people mildly reduces concerns about online privacy violations by other people.

Equation 2 corresponds to H2 ($X_2 \longrightarrow Y_2$). The coefficient for X_2 is negative and statistically significant; thus, H2 is also supported. The standardized coefficient (−.115) shows a mild effect. This means that trust in institutions mildly reduces concerns about online privacy violations by corporations.

The analysis also supports H3 ($X_2 \longrightarrow Y_3$), as the coefficient for X_2 in Equation 3 is negative and statistically significant. Again, a mild effect is observed (the size of the standardized coefficient is −.132). The conclusion is that trust in institutions mildly reduces concerns about online privacy violations by governments.

Finally, Equation 4 corresponds to H4 ($X_1 \longrightarrow Y_4$) and H5 ($X_2 \longrightarrow Y_4$). The coefficients for both X_1 and X_2 are negative and statistically significant; thus, both H4 and H5 are supported. Both effects are mild, as the standardized coefficients are, respectively, −.117 and −.135. These results support that both trust in people and trust in institutions mildly reduce overall online privacy concerns.

The contribution of trust in explaining variation in the dependent variables was also examined. The improvement in R^2 because of the inclusion of the two trust variables (X_1 and X_2) is given by the F_{change} statistic, which corresponds to the null hypothesis that the inclusion of X_1 and X_2 does not improve the model in this respect. As shown in Table 6, F_{change} is statistically significant in all equations. This confirms that trust significantly helps explain variation in online privacy concerns.

About the control variables, the overall absence of statistically significant effects of social capital variables shows that social capital, per se, is less important, if important at all, in explaining privacy concerns (offline bonding social capital is the only dimension that significantly reduces privacy concerns in all models). Digital literacy, as expected, significantly affects privacy concerns in the expected direction, with effect sizes comparable to those of the main predictors in three of the four equations. The more digitally literate Internet users are, the less concerned they are about online privacy violations by other people, governments, and overall. Privacy violation experience also has statistically significant effects in the expected direction, with effect sizes comparable to those of the main predictors in three of the four equations. Users who experienced privacy violations are more concerned about privacy violations by other people, governments, and overall. Length of Internet use is not a statistically significant predictor of privacy concerns. Finally, demographic characteristics do not seem to affect privacy concerns, except for gender in Equation 2, where men are significantly more concerned (by .253 of a unit on Y_2) than women about corporations violating their privacy online.

[6] Substantive effects analysis is not repeated for the remaining hypotheses; it can be obtained from the unstandardized coefficients (reported in Table 6) and the theoretical ranges (max–min) of the variables (reported in the Variable Profiles section).

Conclusion and Discussion

The study concludes that trust reduces online privacy concerns. Specifically, trust in people reduces concerns that other individuals are violating Internet users' privacy online; trust in institutions reduces concerns that corporations and governments are violating Internet users' privacy online; and both trust in people and trust in institutions reduce overall online privacy concerns. The effects are mild but consistent across the five models. These results side with studies reporting influence of trust on privacy concerns or information disclosure practices (Bergström, 2015; Metzger, 2004; Turow & Hennessy, 2007), adding evidence of negative direct effects of trust on online privacy concerns. This evidence is of theoretical interest as the construct of trust is present in several theoretical approaches and in various causal roles. The study supports that general trust is an important predictor in modeling the causes of online privacy concerns.

The study also presents evidence that the effect of trust on privacy concerns is independent of structural dimensions of social capital. It supports that it is the subjective feeling of trust in other people and institutions, not participation in social networks, per se, that makes Internet users less concerned about online privacy violations, and this applies to both offline and online social capital. Only one dimension, offline bonding social capital, evades this conclusion. This is reasonable under the present conceptualization, given that, in Putnam's (2000) terms, the study has modeled *thin* trust (trust to generalized others and institutions) leaving thick trust out; thus, the amount of variance in privacy concerns that thick trust would account for has been allowed to be mathematically credited to offline bonding social capital (bond to significant others).

Certain limitations apply. Concerning internal validity, one limitation is the use of nonexperimental cross-sectional data to test causal hypotheses. In such cases, the causal order can only be theoretically justified but not empirically confirmed. A second limitation concerning internal validity is that, even though the study has modeled privacy concerns as a function of several established predictors, it could have included more, such as ideology, political orientation, and belief in privacy rights (see Yao et al., 2007), or personality traits (Smith et al., 2011; Tang et al., 2021). This is a limitation of the data, as concerns of respondent fatigue prevented the inclusion of more items in the questionnaire. Finally, concerning external validity, the conclusions of the study are strictly generalizable only to the reference society.

Four directions for future research can be outlined. First, in the historical direction, we need continuous monitoring of the relationship between trust, privacy, and other related variables, preferably through longitudinal designs. Research can also move forward in the comparative direction to reveal how privacy concerns, trust, and other variables are related in different cultural contexts. In this respect, Miltgen and Peyrat-Guillard (2014) and Trepte et al. (2017) have made considerable contributions and the paths they have paved could be followed. Third, research can focus on how privacy concerns and privacy-related problems are conditioned by social inequality, by studying, for example, to what extent disadvantaged groups, such as the poor, are disproportionately affected by privacy violations and mass surveillance (Madden, Gilman, Levy, & Marwick, 2017) and to what extent these consequences influence privacy concerns and attitudes. Finally, this area of research can benefit from more qualitative inquiries. These will produce more detailed and in-depth accounts of Internet users' perceptions, emotions, beliefs, and concerns.

The use of supplementary interviews (e.g., Debatin et al., 2009) or focus groups (e.g., Marwick & Hargittai, 2019; Miltgen & Peyrat-Guillard, 2014) are good examples of such investigations. Heikkilä (2020) further recommends the use of the life-story method, supporting this recommendation with a commentary on Snowden (2019). Qualitative and mixed research designs, together with purely quantitative contributions, such as the present, will further enhance our understanding of online privacy concerns, will go deeper into subjective and experiential components of privacy, and will promote awareness and privacy protection on the Internet.

References

Ahn, J. (2012). Teenagers' experiences with social network sites: Relationships to bridging and bonding social capital. *The Information Society, 28*(2), 99–109. doi:10.1080/01972243.2011.649394

Baek, Y. M., Kim, E. M., & Bae, Y. (2014). My privacy is okay, but theirs is endangered: Why comparative optimism matters in online privacy concerns. *Computers in Human Behavior, 31*, 48–56. doi:10.1016/j.chb.2013.10.010

Barnes, S. B. (2006). A privacy paradox: Social networking in the United States. *First Monday, 11*(9). doi:10.5210/fm.v11i9.1394

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

Bartol, J., Vehovar, V., & Petrovčič, A. (2021). Should we be concerned about how information privacy concerns are measured in online contexts? A systematic review of survey scale development studies. *Informatics, 8*(2), 31. doi:10.3390/informatics8020031

Bartsch, M., & Dienlin, T. (2016). Control your Facebook: An analysis of online privacy literacy. *Computers in Human Behavior, 56*, 147–154. doi:10.1016/j.chb.2015.11.022

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

Bélanger, F., & Crossler, R. E. (2011). Privacy in the digital age: A review of information privacy research in information systems. *MIS Quarterly, 35*(4), 1017–1041. doi:10.2307/41409971

Beldad, A., de Jong, M., & Steehouder, M. (2011). A comprehensive theoretical framework for personal information-related behaviors on the internet. *The Information Society, 27*(4), 220–232. doi:10.1080/01972243.2011.583802

Bergström, A. (2015). Online privacy concerns: A broad approach to understanding the concerns of different groups for different uses. *Computers in Human Behavior, 53*, 419–426. doi:10.1016/j.chb.2015.07.025

Blank, G. & Dutton, W. H., & Lefkowitz, J. (2019). Perceived threats to privacy online: The Internet in Britain. Oxford Internet Survey 2019. Oxford Internet Institute, University of Oxford. Retrieved from https://oxis.oii.ox.ac.uk/wp-content/uploads/sites/16/2019/09/OxIS-report-2019-final-digital-PDFA.pdf.

Bourdieu, P. (1986). Forms of capital. In J. G. Richardson (Ed.), *Handbook of theory and research for the sociology of education* (pp. 241–258). Westport, CT: Greenwood Press.

Chen, H., Beaudoin, C. E., & Hong, T. (2016). Teen online information disclosure: Empirical testing of a protection motivation and social capital model. *Journal of the Association for Information Science and Technology, 67*(12), 2871–2881. doi:10.1002/asi.23567

Coleman, J. S. (1988). Social capital in the creation of human capital. *American Journal of Sociology, 94*(Suppl.), S95–S120. doi:10.1086/228943

Cook, K. S., & Rice, E. (2003). Social exchange theory. In J. Delamater (Ed.), *Handbook of social psychology* (pp. 53–76). New York, NY: Kluwer Academic/Plenum Publishers.

Debatin, B., Lovejoy, J. P., Horn, A. K., & Hughes, B. N. (2009). Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Journal of Computer-mediated Communication, 15*(1), 83–108. doi:10.1111/j.1083-6101.2009.01494.x

Dienlin, T., Masur, P. K., & Trepte, S. (2023). A longitudinal analysis of the privacy paradox. *New Media & Society, 25*(5), 1043–1064. doi:10.1177/14614448211016316

Fukuyama, F. (1995). *Trust: The social virtues and the creation of prosperity*. New York, NY: Free Press.

Granovetter, M. S. (1973). The strength of weak ties. *American Journal of Sociology, 78*(6), 1360–1380. doi:10.1086/225469

Friemel, T. N., & Signer, S. (2010). Web 2.0 literacy: Four aspects of the second-level digital divide. *Studies in Communication Sciences, 10*(2), 143–166. doi.org/10.5167/uzh-44984

Heikkilä, H. (2020). Beyond moral coupling: Analysing politics of privacy in the era of surveillance. *Media and Communication, 8*(2), 248–257. doi:10.17645/mac.v8i2.2875

Homans, G. C. (1961). *Human behavior: Its elementary forms*. New York, NY: Harcourt, Brace.

Jardine, E. (2018). Tor, what is it good for? Political repression and the use of online anonymity-granting technologies. *New Media & Society, 20*(2), 435–452. doi:10.1177/1461444816639976

Jia, H., & Xu, H. (2016). Measuring individuals' concerns over collective privacy on social networking sites. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 10*(1), Article 4. doi:10.5817/CP2016-1-4

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

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

Krasnova, H., Spiekermann, S., Koroleva, K., & Hildebrand, T. (2010). Online social networks: Why we disclose. *Journal of Information Technology, 25*(2), 109–125. doi:10.1057/jit.2010.6

Li, Y. (2011). Empirical studies on online information privacy concerns: Literature review and an integrative framework. *Communications of the Association for Information Systems, 28*(1), Article 28. doi:10.17705/1CAIS.02828

Lindner, A. M., & Xiao, T. (2020). Subverting surveillance or accessing the Dark Web? Interest in the Tor anonymity network in U.S. states, 2006–2015. *Social Currents*, *7*(4), 352–370. doi:10.1177/2329496520919165

Lutz, C., Hoffmann, C. P., & Ranzini, G. (2020). Data capitalism and the user: An exploration of privacy cynicism in Germany. *New Media & Society, 22*(7), 1168–1187. doi:10.1177/1461444820912544

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

Madden, M., & Rainie, L. (2015, May 20). *Americans' attitudes about privacy, security and surveillance*. Pew Research Center. Retrieved from http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research, 15*(4), 336–355. doi:10.1287/isre.1040.0032

Männiste, M., & Masso, A. (2018). The role of institutional trust in Estonians' privacy concerns. *Studies of Transition States and Societies, 10*(2), 22–39.

Marwick, A., & Hargittai, E. (2019). Nothing to hide, nothing to lose? Incentives and disincentives to sharing information with institutions online. *Information, Communication & Society, 22*(12), 1697–1713. doi:10.1080/1369118X.2018.1450432

Masur, P. K., & Trepte, S. (2021). Transformative or not? How privacy violation experiences influence online privacy concerns and online information disclosure. *Human Communication Research, 47*(1), 49–74. doi:10.1093/hcr/hqaa012

Metzger, M. J. (2004). Privacy, trust, and disclosure: Exploring barriers to electronic commerce. *Journal of Computer-mediated Communication, 9*(4). doi:10.1111/j.1083-6101.2004.tb00292.x

Miltgen, C. L., & Peyrat-Guillard, D. (2014). Cultural and generational influences on privacy concerns: A qualitative study in seven European countries. *European Journal of Information Systems, 23*(2), 103–125. doi:10.1057/ejis.2013.17

Misztal, B. A. (1992). The notion of trust in social theory. *Policy, Organisation and Society, 5*(1), 6–15. doi:10.1080/10349952.1992.11876774

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

Paine, C., Reips, U. D., Stieger, S., Joinson, A., & Buchanan, T. (2007). Internet users' perceptions of 'privacy concerns' and 'privacy actions.' *International Journal of Human-Computer Studies, 65*(6), 526–536. doi:10.1016/j.ijhcs.2006.12.001

Park, Y. J. (2013). Digital literacy and privacy behavior online. *Communication Research, 40*(2), 215–236. doi:10.1177/0093650211418338

Petronio, S. (2002). *Boundaries of privacy: Dialectics of disclosure.* Albany, NY: SUNY Press.

Portes, A. (1998). Social capital: Its origins and applications in modern sociology. *Annual Review of Sociology, 24*(1), 1–24. doi:10.1146/annurev.soc.24.1.1

Preibusch, S. (2013). Guide to measuring privacy concern: Review of survey and observational instruments. *International Journal of Human-Computer Studies, 71*(12), 1133–1143. doi:10.1016/j.ijhcs.2013.09.002

Preibusch, S. (2015). Privacy behaviors after Snowden. *Communications of the ACM, 58*(5), 48–55. doi:10.1145/2663341

Putnam, R. D. (2000). *Bowling alone: The collapse and revival of American community*. New York, NY: Simon and Schuster.

Rohunen, A., Markkula, J., Heikkilä, M., & Oivo, M. (2020). Explaining diversity and conflicts in privacy behavior models. *Journal of Computer Information Systems, 60*(4), 378–393. doi:10.1080/08874417.2018.1496804

Rosenberg, M. (1956). Misanthropy and political ideology. *American Sociological Review, 21*(6), 690–695. doi:10.2307/2088419

Scheufele, D. A., & Shah, D. V. (2000). Personality strength and social capital: The role of dispositional and informational variables in the production of civic participation. *Communication Research, 27*(2), 107–131. doi:10.1177/009365000027002001

Shane-Simpson, C., Manago, A., Gaggi, N., & Gillespie-Lynch, K. (2018). Why do college students prefer Facebook, Twitter, or Instagram? Site affordances, tensions between privacy and self-expression, and implications for social capital. *Computers in Human Behavior, 86*, 276–288. doi:10.1016/j.chb.2018.04.041

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly, 35*(4), 989–1015. doi:10.2307/41409970

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: Measuring individuals' concerns about organizational practices. *MIS Quarterly, 20*(2), 167–196. doi:10.2307/249477

Snowden, E. (2019). *Permanent record*. London, UK: Macmillan.

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. (2011, May 15). Why privacy matters even if you have "nothing to hide." *The Chronicle of Higher Education*. Retrieved from http://chronicle.com/article/Why-Privacy- Matters-Even-if/127461/

Stewart, K. A., & Segars, A. H. (2002). An empirical examination of the concern for information privacy instrument. *Information Systems Research, 13*(1), 36–49. doi:10.1287/isre.13.1.36.97

Tang, J., Akram, U., & Shi, W. (2021). Why people need privacy? The role of privacy fatigue in app users' intention to disclose privacy: Based on personality traits. *Journal of Enterprise Information Management, 34*(4), 1097–1120. doi:10.1108/JEIM-03-2020-0088

Tavani, H. T. (2007). Philosophical theories of privacy: Implications for an adequate online privacy policy. *Metaphilosophy, 38*(1), 1–22. doi:10.1111/j.1467-9973.2006.00474.x

Tifferet, S. (2019). Gender differences in privacy tendencies on social network sites: A meta-analysis. *Computers in Human Behavior, 93*, 1–12. doi:10.1016/j.chb.2018.11.046

Trepte, S. (2021). The social media privacy model: Privacy and communication in the light of social media affordances. *Communication Theory, 31*(4), 549–570. doi:10.1093/ct/qtz035

Trepte, S., Reinecke, L., Ellison, N. B., Quiring, O., Yao, M. Z., & Ziegele, M. (2017). A cross-cultural perspective on the privacy calculus. *Social Media + Society, 3*(1), 1–13. doi:10.1177/2056305116688035

Turow, J., & Hennessy, M. (2007). Internet privacy and institutional trust: Insights from a national survey. *New Media & Society, 9*(2), 300–318. doi:10.1177/1461444807072219

Urwin, P., Di Pietro, G., Sturgis, P., & Jack, G. (2008). Measuring the returns to networking and the accumulation of social capital: Any evidence of bonding, bridging, or linking? *American Journal of Economics and Sociology, 67*(5), 941–968. doi:10.1111/j.1536-7150.2008.00603.x

Valenzuela, S., Park, N., & Kee, K. F. (2009). Is there social capital in a social network site?: Facebook use and college students' life satisfaction, trust, and participation. *Journal of Computer-Mediated Communication, 14*(4), 875–901. doi:10.1111/j.1083-6101.2009.01474.x

Westin, A. F. (1967). *Privacy and freedom*. New York, NY: Atheneum.

Yao, M. Z., Rice, R. E., & Wallis, K. (2007). Predicting user concerns about online privacy. *Journal of the American Society for Information Science and Technology, 58*(5), 710–722. doi:10.1002/asi.20530