CYBERPSYCHOLOGY, BEHAVIOR, AND SOCIAL NETWORKING
Volume 17, Number 10, 2014

DOI: 10.1089/cyber.2013.0585

ORIGINAL ARTICLE

Transparency of Intentions Decreases Privacy Concerns in Ubiquitous Surveillance

Antti Oulasvirta, PhD,[1,2,3] Tiia Suomalainen, MSc,[1] Juho Hamari, MSc,[1,4,5]
Airi Lampinen, PhD,[1] and Kristiina Karvonen, PhD[1]

Abstract

An online experiment ($n = 1,897$) was carried out to understand how data disclosure practices in ubiquitous surveillance affect users' privacy concerns. Information about the identity and intentions of a data collector was manipulated in hypothetical surveillance scenarios. Privacy concerns were found to differ across the scenarios and moderated by knowledge about the collector's identity and intentions. Knowledge about intentions exhibited a stronger effect. When no information about intentions was disclosed, the respondents postulated negative intentions. A positive effect was found for disclosing neutral intentions of an organization or unknown data collector, but not for a private data collector. The findings underline the importance of disclosing intentions of data use to users in an easily understandable manner.

Introduction

UBIQUITOUS SURVEILLANCE REFERS to the increasing penetration of computerized data capture in everyday life.[1–4] Credit card companies track consumer behavior, security companies access live video feeds from homes, employers read employees' e-mails, governments tap communications, sports companies store exercise data, media companies store digital TV usage, health records are distributed among healthcare service providers, public spaces are under CCTV surveillance, and social media companies capitalize on data on their customers' social behavior. The recent uproar triggered by the National Security Agency whistleblower Edward Snowden suggests that a key contributor to the negative perception of ubiquitous surveillance is the lack of transparency.

In this paper, ''transparency'' denotes any piece of information available to the person being surveilled that concerns the identity, purposes, or practices of the involved data collectors. Often such pieces of information, like terms of service (ToS) and control settings, are too complex, and users do not understand or use them.[5–8] These developments call for research on privacy concerns under uncertain and incomplete information.

Positive effects of transparency have been previously reported in many domains of the information society: online marketing,[9,10] job applications,[11] work performance monitoring,[12] monitoring by government,[13] and Internet use and online shopping.[14–17] Disclosing the uses of personal data also reduces concerns about personality tests[18] and employment applications.[19] In online behavior, transparency increases willingness to disclose personal information for marketing as well as trust in companies who gather personal information.[9,17] In contrast, opaqueness decreases customer retention in Web services.[20] Oftentimes, transparency is only partial, and users base their decisions on limited signals of the service provider.[21] However, the questions remain of whether the effects of transparency apply across different domains of ubiquitous surveillance and how different levels of transparency affect privacy concerns.

To understand transparency in ubiquitous surveillance better, the online experiment reported here ($n = 1,897$) investigates nine ubiquitous surveillance scenarios within a single study. The scenarios cover many recently debated privacy issues, ranging from health records to sports tracking and smartphone logging. We focus on the *a*symmetric surveillance case where data are not voluntarily disclosed by the person being surveilled but captured by a data collector—here, an organization or an individual. There are forms of surveillance (e.g., Internet services and loyalty cards) where disclosure is a part of using a service.

Our primary goal is to shed light on a pragmatically important question concerning transparency: what should the data collector disclose and bring to the attention of the users? Basing on previous work, we hypothesize that any information disclosed to people being surveilled has the potential to indicate a risk of a harmful outcome for the individual.[10,22,23] Therefore, particularly useful cues should be those that

[1]Helsinki Institute for Information Technology HIIT, Aalto University, Helsinki, Finland.
[2]Max Planck Institute for Informatics, Saarbruecken, Germany.
[3]Cluster of Excellence on Multimodal Computing and Interaction, Saarland University, Saarbruecken, Germany.
[4]Department of Information and Service Economy, Aalto University School of Business, Helsinki, Finland.
[5]Game Research Lab, School of Information Sciences, University of Tampere, Tampere, Finland.

decrease the expected level of harm. Such cues are many, but we chose to focus on two universally applicable cues that could also be easily disclosed in marketing, ToS, and user interfaces: the identity and intention of the data collector.

To understand these phenomena, the disclosure of the data collector's identity and intentions is controlled, enabling us to gauge the overall effect, as well as provide a breakdown per cue type. We further add a blind (hidden) condition where such information is not disclosed. This emulates the nondisclosure—or unattendance by users—to these pieces of information.

Our study follows a $9 \times 3 \times 3$ (scenario × intention × identity) design. It is an online experiment in which the content of a data collection scenario is manipulated, and respondents rate their concern for privacy. Two variables are manipulated in each scenario: (a) identity, or what is said about the identity of the data-collecting actor in the scenario, and (b) intention, or what is said of the intention that underlies data collecting. The experiment examines transparency by breaking down both variables into three levels. For identity, these are private, organization, and hidden; for intention, these are negative, neutral, and hidden. To study the effect of uncertainty, we ''sandwich'' the hidden condition between negative and neutral intentions, which allows us to learn whether people by default assume that intentions are closer to neutral or negative. Positive intentions were not included in the study because they are of secondary importance in the study of privacy concerns related to ubiquitous surveillance and because previous work has overwhelmingly showed the benefit of disclosing positive intentions.

This design allows us to address the following research questions related to the effect of transparency:

RQ1: Is there an effect of transparency on privacy concerns, and is it universal across domains of ubiquitous surveillance?

Based on previous work, we expect that transparency should generally support users' ability to draw factually correct inferences about the collection and use of personal data and, by that, help them to regulate their behavior and alleviate their concerns.[22,24]

However, this may not occur universally across the diverse scenarios we include in the study. There are at least three theoretically motivated predictions for a null effect. First, it has been argued that people underestimate the impact of privacy loss because it arises only later, in an abstract future, while the utility of the service might manifest itself instantly.[22,25,26] Second, the cost of reasoning is relatively high in comparison to the gains and losses that are believed to be related to the decision of divulging information—a phenomenon also known as rational ignorance.[27,28] Finally, the gratifications associated with the received benefits from different services may be perceived greater than any privacy threat.[29] We thus predict that large differences can be expected among scenarios of different kinds.

RQ2: Is the effect of transparency on privacy concerns dependent on the type of information disclosed about the data collector? In particular, does knowledge of the identity versus intentions affect the effect differentially?

Previous findings support the conjecture that both identity and intention should affect privacy concerns: First, employees have been found to be concerned not so much about the nature of the data collected on them, but about the individuals or groups who can access these data (identity).[30] Second, trust toward online vendors is affected by the perception that the vendor has nothing to gain by cheating (intention).[15] However, previous work provides no clues on which of the factors has a larger effect size and if these effects generalize.

We hypothesize that the data collector's intention is a direct cue suggesting the probability of privacy loss, and identity is an indirect cue suggesting the entity's capacity to realize those intentions. An organization should, other things being equal, be perceived as more capable in realizing potential threats than an individual. The government is a very powerful actor, but its capacity is of little concern unless it harbors negative intentions. This effect could interact with scenario because capacity can be expected to be case specific.

RQ3: Is uncertainty over the data collector's intentions worse for privacy concerns than knowing that the intentions are neutral?

Our two transparency variables—identity and intention—both include a condition where this information is not closed. In real world contexts of use, ambiguity can pose a rather different outcome. One possibility is that the perceived high risks make people exhibit what is known as risk aversion. Furthermore, not knowing identity and intentions can create a situation where the decision maker is unable to assess accurately the probabilities of different possible outcomes and might thus exhibit what is known as ambiguity aversion.[31–33] Another possibility is that people construct imaginary threat scenarios wherein their details are accessed and used by others, in which case privacy concerns amid uncertainty should be closer to the level of concern arising when data collectors' intentions are known to be negative. Such effect could be bolstered by the negative reporting of ubiquitous surveillance in the media. Due to case-specific differences, this effect could also differ among scenarios.

Understanding the effect of uncertainty on privacy concerns is also relevant to existing models of privacy concerns. For example, the concern for information privacy (CFIP) model[9,34] predicts privacy concerns as a function of four beliefs: collection of data, errors in the data, secondary use of data, and improper access. A recent review models privacy concerns as the consequence of privacy experiences, privacy awareness, personality differences, demographic differences, and culture.[35] Concerns are also linked to regulation, trust, risks/costs, and behavioral reactions. Trust is modeled as affected by institution-based structural assurances, calculation, institution-based normality, and knowledge-based familiarity.[15] To our knowledge, none of the models specifies uncertainty as a factor.

RQ4: Are there large individual differences?

Given that individuals differ in their attitudes toward and prior knowledge about the different scenarios, we expect to find large individual differences. To learn if they can be attributed to more stable individual factors, we administered the Behavioral Inhibition/Approach Scale (BIS/BAS),[36] hypothesizing that individuals high in BIS will respond more negatively to potential privacy loss than respondents lower in

BIS. According to the theory, BAS regulates motives in which the goal is to move toward something desired, such as the benefits of the services in a ubiquitous surveillance scenario. The BIS system, on the other hand, regulates aversive motives in which the goal is to move away from something unpleasant, such as privacy loss.

Method

An online questionnaire with nine scenarios was designed for the study (Table 1).

Participants

In all, 1,911 Finnish-speaking respondents filled in the online questionnaire. The sample was a nonrandom convenience sample. Sampling was carried out by means of advertisements in Finnish student organizations' e-mail mailing lists, online mailing lists, Web sites of professional organizations, and discussion forums of hobbyists targeting different age groups.

The respondents were predominantly female (67.8%). The mean age was 36.35 years ($SD = 13.96$ years; range 14–80 years). Eighteen percent had a university-level education. Comparing against the demographics of the Finnish population (Statistics Finland 2014), our sample was somewhat younger (population average 42 years), better educated (population average 9% university education), and it included more females (population average 51%).

Five respondents were randomly chosen and awarded a small prize (two movie tickets worth €20 in total), but no other participation fees were paid.

Fourteen blank answer sheets caused by a technical error in the service were excluded from the final sample.

Design

The experimental design was a $9 \times 3 \times 3$ design (scenario × identity: private individual vs. organization vs. hidden × intention: negative vs. neutral vs. hidden). Intention and identity refer to what information was disclosed about the entity accessing or using the data collected, with ''hidden'' denoting that information was not provided.

With nine scenarios and nine experimental conditions, 81 sets were created. The order of scenarios was counterbalanced by rotation. Each respondent was randomly assigned to a set by a server-side script. Every participant completed nine scenarios.

Table 1. Summaries of the Data Collection Scenarios with Identities and Intentions

1. Your only computer has a device that logs everything typed on the computer's keyboard	
Organization: employer	Private: roommate
Neutral: logging only, not examining	Neutral: logging only, not examining
Negative: investigate if guilty of espionage	Negative: seeing if you are hiding something
2. You wear a body sensor measuring pulse, body temperature, EKG trace, and respiration	
Organization: employer	Private: a relative
Neutral: checking your medical health	Neutral: reacting quick in case of emergency
Negative: sending you home if sick	Negative: checking if you are sick
3. You have a Facebook account	
Organization: insurance company	Private: acquaintance
Neutral: collects data but not using it	Neutral: watching your profile
Negative: inspecting insurance fraud	Negative: identity fraud
4. Every room in your house is subject to recording by video cameras around the clock	
Organization: security company	Private: neighbor
Neutral: security monitoring	Neutral: no watching, just recording
Negative: watching clips on coffee breaks	Negative: blackmail with video clips
5. All of your health records are in one central register	
Organization: hospital	Private: spouse
Neutral: diagnosis and treatment	Neutral: use in case of accident
Negative: check if you have been lying	Negative: check if you have been lying
6. Your phone records all communication (calls and text messaging)	
Organization: telecom company	Private: unknown individual
Neutral: stored; used only in emergency	Neutral: not interested in you
Negative: finding interesting materials	Negative: finding interesting materials
7. Your credit card transactions are recorded in a database	
Organization: bank	Private: acquaintance
Neutral: survey of card use in your district	Neutral: report if credit card data stolen
Negative: following your money use	Negative: following your money use
8. Your phone determines your location to an accuracy of 50 meters	
Organization: state	Private: good friend
Neutral: warning in case of natural disaster	Neutral: call you up if close by
Negative: check if your self-report holds	Negative: check if you are where you told to be
9. Cameras record people in public places	
Organization: researchers at a university	Private: work colleague
Neutral: study crowd behavior	Neutral: follow interesting events in the city
Negative: report if you have secret goings	Negative: see how you behave outside work

Materials

Table 1 presents the nine data collection scenarios. Each scenario was a textual description of a sensor that collects data, the identity of the data collector with access to the data, and the believed collector's intention. To make the scenarios realistic, we perused newspaper articles dealing with surveillance and also interviewed our colleagues informally. The following scenario for a PC describes a public institution with a negative intention:

> Your only computer has a device that logs everything typed on the computer's keyboard to a file. You know it is possible for your employer [IDENTITY] to view the file. You find it likely that the employer wants to monitor whether you are sharing confidential information regarding your job with non-employees [INTENTION].

In the case where identity and/or intention were hidden, the corresponding sentences marked in brackets above were not displayed.

The questionnaire was implemented via the e-Lomake service, a service that is used for creating, launching, and administering Web-format questionnaire-based studies. Radio buttons (HTML) were provided as a means for entering ratings. All content was in Finnish.

Measurements

We constructed a questionnaire with 12 Likert-scale items measuring privacy concerns. It was administered after every scenario. The 12 items center on privacy concerns, and they have some overlap with items in CFIP.[9,34] In particular, the items cover (a) a general concern for privacy, (b) concern for the particular data exposed, (c) experiential states (frustration, anxiety), and (d) and behavioral responses (inhibition of regular behavior). Two negative questions were included. The aggregate score was used for analysis.

Post-treatment check of the negative items exposed no significant response bias. A two-tailed one-sample t test was not significant, $t(1886) = 1.127$, $p = 0.26$.

The BIS/BAS scale with five items was administered at the beginning of each questionnaire.

Procedure

After supplying basic background information (gender, age, etc.), the respondent was assigned to a condition within the set of 81 questionnaires. One scenario with the questionnaire was presented at a time. After pressing the ''Continue'' button, the next scenario was loaded. The questionnaire took about 15 minutes to complete.

Results

On account of the fact that the appropriateness of responses could only be checked after the study and not during the random assignment phase, cell sizes were not equal across the nine sets created to counterbalance for the order of scenarios. However, thanks to the sample size, this inequality had no biasing effect. The smallest of the counterbalancing sets had $n = 187$ and the largest $n = 236$. There was no significant effect of the set on the dependent variable, $F(8) = 0.66$, $p = 0.73$. For statistical testing, we use an alpha value of 0.05 as a threshold.

Table 2. Results of Statistical Testing—Effects of Experimental Factors on Privacy Concerns

Factor	F	*df*	*MS*	p
Intention	72.43	2	33,376.0	<0.001*
Identity	7.81	2	3,644.2	<0.001*
Scenario	1.56	71	1,224.9	0.002*
Identity × intention	3.43	4	1,565.2	0.008*
Intention × scenario	3.096	142	1,426.7	<0.001*
Identity × scenario	3.263	142	1,522.4	<0.001*
Identity × intention × scenario	3.302	284	1,509.3	<0.001*

*Statistically significant at $p < 0.05$.

Main factors and interactions

Table 2 presents results from statistical testing with a mixed model analysis of variance. Table 2 shows that the three main factors—scenario, identity, and intention—and their interaction effects were statistically significant.

The main effect of scenario was significant, as expected. Table 3 reports privacy concerns measured in each of the nine scenarios, ranked per severity of concern. Table 3 shows that privacy concerns were relatively high on average, with four scenarios scoring an average concern greater than 30 (out of 48), and all except one scoring more than 25. Domestic video surveillance was closest to the ceiling ($M = 41.15$) and centralized health records lowest. As Table 2 shows, scenario also had a significant interaction effect with both identity and intention.

Identity had a significant main effect. A post hoc test (Bonferroni) exposed that the mean of privacy concern in scenarios involving a private data collector was higher than in those involving a public organization ($p = 0.009$). When information about identity was not provided (i.e., was hidden), privacy concern was lowest. The difference with organization was not significant, but with private it was significant ($p < 0.001$).

Intention also had a significant main effect. Post hoc tests (Bonferroni) showed that all differences among the levels were significant ($p < 0.001$).

Finally, the interaction effect of identity × intention was significant. Figure 1 presents an overview with the means from all 3×3 conditions, pointing out that intention had a greater and less variable effect than identity. A positive effect of transparency was found for disclosing neutral intentions of a public data or an unknown data collector. Post hoc tests

Table 3. The Nine Scenarios Ranked per Mean Privacy Concern (Maximum Score 48)

Data collection scenario	M	SD
Domestic video surveillance	41.15	6.24
Communications recording	36.41	9.49
Keylogging on a personal computer	34.07	10.64
Facebook monitoring	30.83	11.13
Exercise data monitoring	30.41	11.58
Credit card logging	29.19	11.27
Smartphone location tracking	28.97	11.39
Public place video surveillance	27.46	11.73
Centralized health records	22.73	11.93

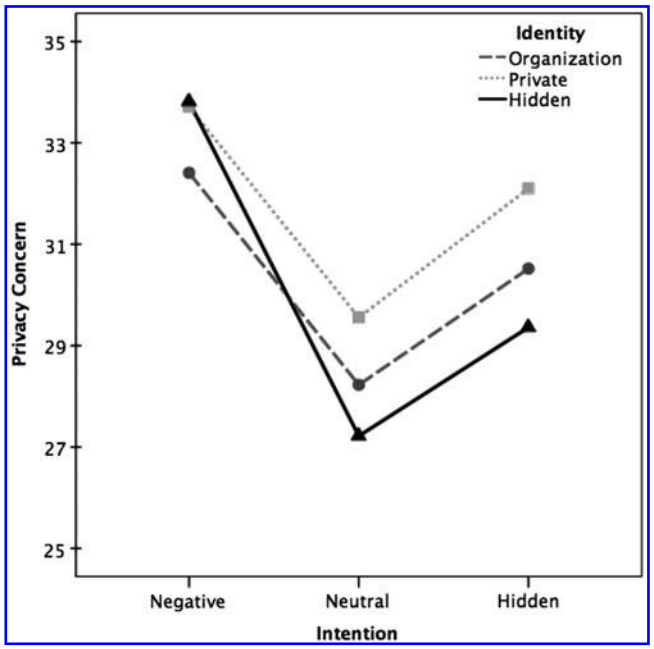

FIG. 1. Privacy concerns with a breakdown by the type of information provided about the data collector.

(Bonferroni) expose three patterns. First, there were no significant differences in the intention conditions within a given identity condition, except for the condition intention = neutral, where the sub-conditions identity = private and identity = hidden differed from each other ($p = 0.03$). Second, privacy concern in the condition intention = hidden and identity = private was not statistically different from the conditions were intention was negative ($p > 0.99$), and it was higher than in the conditions where intention = neutral and identity = organization/hidden. Third, the intention = negative condition was different from other conditions ($p < 0.004$), except the condition where intention was hidden and identity private.

Individual differences

To understand the effect of BIS/BAS traits, statistical testing was carried out using general linear model (GLM) with intention and identity as within-subjects factors and BIS/BAS as continuous predictors (BAS Drive, BAS Fun Seeking, BAS Reward Responsiveness, and BIS).

Table 4 reports the effects of BIS/BAS variables. BIS had a significant main effect on privacy concern. Not surprisingly, respondents scoring high in BIS had higher privacy concerns overall. Only one of the BAS variables (BAS-Fun) had a main effect.

TABLE 4. INDIVIDUAL DIFFERENCES: THE EFFECTS OF BIS/BAS COMPONENTS ON CONCERN FOR PRIVACY

Factor	*df*	*MS*	F	p
BAS-Drive	1	1,193.7	1.503	0.220
BAS-Reward	1	361.1	0.455	0.500
BAS-Fun	1	1,354.7	1.706	0.001*
BIS	1	15,071.9	18.978	< 0.001*

*Statistically significant at $p < 0.05$.

Discussion

The high level of concern measured over the nine scenarios confirms that people perceive ubiquitous surveillance negatively, and this motivates the need for studying privacy concerns. To our knowledge, this is the first time the effect of transparency has been studied across a large set of surveillance scenarios.

Our findings indicate that transparency decreases the level of concern.[1,9,18,20,22] We found that the effect is moderated in an expectable way by the other variables manipulated in the experiment. First, we found that the nine scenarios differ in terms of the effect of transparency (RQ1). We found a significant main effect of scenario, as well as significant interactions with the transparency-related factors identity and intention.

Two other findings allow further insight into this effect. First, although knowledge about the data collector's identity moderates privacy concerns, knowledge of intentions has a far stronger effect on privacy concerns (RQ2). Not surprisingly, we found that neutral intentions of the data collector decrease the level of concern, and negative ones increase it. The highest level of concern is associated with scenarios with negative intentions, and knowledge about who is accessing data lowers concerns if the intentions are known to be not antagonistic.

Second, when the data collector's intention is unknown, privacy concerns are elevated (RQ3). People do not assume a priori that data collectors have neutral intentions; rather, they postulate negative intentions, although they are not as negative as the ones used in our scenarios.

Moreover, we found that respondents scoring higher in BIS are relatively more alarmed when they know that the data collector's intentions are against them (RQ4).

These findings call for more research to provide exact models that link disclosed information with privacy concerns. With regard to previous models that consider risks/gains in threat scenarios,[35] the believed intentions of the data collector seem to be critical because they indicate the probability of harm and thereby raise concerns. On the other hand, believed identity has a secondary effect as an indicator of the capacity to inflict actual harm. Both might be modeled in terms of expected harm. Moreover, we found evidence of pessimism: when it comes to surveillance, by default people tend to expect high harm in the face of uncertainty rather than ignore possible threats.

These findings also point toward the question of how to implement usable transparency. Recent work in human–computer interaction has started to examine usable ''privacy nutrition labels,'' descriptions that employ a standard set of categories and symbols to communicate privacy practices and are used for many types of services.[8,17,37] Widespread adoption of such standardization could revolutionize the field similarly to how Creative Commons licensing has revolutionized copyright management on the Internet. The present findings underline that both the data collector's identity and intention should be disclosed in such privacy nutrition labels. Furthermore, while exposing the two factors (identity and intention) will be beneficial, directing the user's attention to the data collector's intention will have a stronger effect than would drawing attention to identity alone. We hope that the benefit conveyed by the present data will fuel serious efforts in this direction.

Author Disclosure Statement

No competing financial interests exist.

References

1. Agre PE. Surveillance and capture: two models of privacy. The Information Society 1994; 10:101–127.
2. Barnes SB. A privacy paradox: social networking in the United States. First Monday 2006; 11:11–15.
3. Brin D. (1998) *The transparent society*. Reading, MA: Addison-Wesley Longman, Inc.
4. Lyon D. Facing the future: seeking ethics for everyday surveillance. Ethics & Information Technology 2001; 3:171–181.
5. Muise CE, Desmarais S. Information disclosure and control on Facebook: are they two sides of the same coin or two different processes? CyberPsychology & Behavior 2009; 12:341–345.
6. Jensen C, Potts C, Jensen C. Privacy practices of Internet users: self-reports versus observed behavior. International Journal of Human–Computer Studies 2004; 63:203–227.
7. Leon PG, Ur B, Balebako R, et al. (2011) Why Johnny can't opt out: a usability evaluation of tools to limit online behavioral advertising. Carnegie Mellon University CyLab Technical Report 11-017. www.cylab.cmu.edu/research/techreports/2011/tr_cylab11017.html (accessed April 4, 2014).
8. Kelley PG, Bresee J, Reeder RW, et al. (2009) Design of a privacy label. Symposium on Usable Privacy and Security SOUPS, Mountain View, CA.
9. Malhotra NK, Kim SS, Agarwal J. Internet users' information privacy concerns (IUIPC): the construct, the scale, and a causal model. Information Systems Research 2004; 15:336–355.
10. Culnan M. ''How did they get my name?'': an exploratory investigation of consumer attitudes toward secondary information use. MIS Quarterly 1993; 17:341–363.
11. Bauer TN, Truxillo DM, Tucker JS, et al. Selection in the information age: the impact of privacy concerns and computer experience on applicant reactions. Journal of Management 2006; 32:601–621.
12. Chen J, Ross W. Individual differences and electronic monitoring at work. Information, Communication & Society 2007;10:488–505.
13. Dinev T, Hart P, Mullen MR. Internet privacy concerns and beliefs about government surveillance—an empirical investigation. The Journal of Strategic Information Systems 2008; 17:214–233.
14. Dinev T, Hart P. Internet privacy concerns and their antecedents—measurement validity and a regression model. Behaviour & Information Technology 2004; 23:413–422.
15. Gefen D, Karahanna E, Straub D. Trust and TAM in online shopping: an integrated model. MIS Quarterly 2003; 27:51–90.
16. Xu H, Dinev T, Smith HJ, et al. (2008) Examining the formation of individual's privacy concerns: toward an integrative view. Proceedings of 29th Annual International Conference on Information Systems (ICIS), Paris, France.
17. Hui K-L, Teo H, Lee S-Y. The value of privacy assurance: an exploratory field experiment. MIS Quarterly 2007; 31:19–33.
18. Fink AM, Butcher JN. Reducing objections to personality inventories with special instructions. Educational & Psychological Measurement 1972; 32:631–639.
19. Fusilier MR, Hoyer WD. Variables affecting perceptions of invasion of privacy in a personnel selection situation. Journal of Applied Psychology 1980; 65:623–626.
20. Riegelsberger J, Sasse MA, McCarthy J. The researcher's dilemma: evaluating trust in computer-mediated communication. International Journal of Human Computer Studies 2003; 58:759–781.
21. Chen YH, Chien SH, Wu JJ, et al. Impact of signals and experience on trust and trusting behavior. Cyberpsychology, Behavior, & Social Networking 2010; 13:539–546.
22. Acquisti A, Grossklags J. (2005) Uncertainty, ambiguity and privacy. 4th Workshop on the Economics of Information Security (WEIS), Cambridge, MA.
23. Paradise A, Sullivan M. (In) visible threats? The third-person effect in perceptions of the influence of Facebook. Cyberpsychology, Behavior, & Social Networking 2012; 15:55–60.
24. Acquisti A, Gross R. Imagined communities: awareness, information sharing, and privacy on the Facebook. Privacy Enhancing Technologies 2006; 4258:36–58.
25. Ainslie G. Specious reward: a behavioral theory of impulsiveness and impulse control. Psychological Bulletin 1975; 82:463–496.
26. Thaler R. Some empirical evidence on dynamic inconsistency. Economics Letters 1981; 8:201–207.
27. Caplan B. Rational ignorance versus rational irrationality. KYKLOS 2001; 54:3–26.
28. Downs A. (1957) *An economics theory of democracy*. New York: Harper.
29. Chen HT, Kim Y. Problematic use of social network sites: the interactive relationship between gratifications sought and privacy concerns. Cyberpsychology, Behavior, & Social Networking 2013; 16:806–812.
30. Taylor GS, Davis JS. Individual privacy and computer-based human resources systems. Journal of Business Ethics 1989; 8:596–576.
31. Camerer CF, Weber M. Recent developments in modelling preferences: uncertainty and ambiguity. Journal of Risk & Uncertainty 1992; 5:325–370.
32. Ellsberg D. Risk, ambiguity, and the savage axioms. Quarterly Journal of Economics 1961; 75:643–699.
33. Fox CR, Tversky A. Ambiguity aversion and comparative ignorance. Quarterly Journal of Economics 1995; 110:585–603.
34. Smith HJ, Milberg SJ, Burke SJ. Information privacy: measuring individuals' concerns about organizational practices. MIS Quarterly 1996; 20:167–196.
35. Smith HJ, Dinev T, Xu H. Information privacy research: an interdisciplinary review. MIS Quarterly 2011; 35:989–1015.
36. Carver CS, White TL. Behavioral inhibition, behavioral activation, and affective responses to impending reward and punishment: the BIS/BAS scales. Journal of Personality & Social Psychology 1994; 67:319–333.
37. Tsai J, Egelman S, Cranor L, et al. (2007) The effect of online privacy information on purchasing behavior: an experimental study. 6th Workshop on the Economics of Information Security (WEIS), Pittsburgh, PA.

Address correspondence to:
Prof. Antti Oulasvirta
Department of Communications and Networking
School of Electrical Engineering
Aalto University
Otakaari 5
13000 Aalto University
Helsinki, Finland

E-mail: antti.oulasvirta@gmail.com