International Journal of Human–Computer Interaction

ISSN: 1044-7318 (Print) 1532-7590 (Online) Journal homepage: www.tandfonline.com/journals/hihc20

Online Privacy Breaches, Offline Consequences: Construction and Validation of the Concerns with the Protection of Informational Privacy Scale

Eric Durnell, Karynna Okabe-Miyamoto, Ryan T. Howell & Martin Zizi

To cite this article: Eric Durnell, Karynna Okabe-Miyamoto, Ryan T. Howell & Martin Zizi (2020) Online Privacy Breaches, Offline Consequences: Construction and Validation of the Concerns with the Protection of Informational Privacy Scale, International Journal of Human–Computer Interaction, 36:19, 1834-1848, DOI: 10.1080/10447318.2020.1794626

To link to this article: https://doi.org/10.1080/10447318.2020.1794626

INTERNATIONAL JOURNAL OF HUMAN–COMPUTER INTERACTION
2020, VOL. 36, NO. 19, 1834–1848
https://doi.org/10.1080/10447318.2020.1794626

Taylor & Francis
Taylor & Francis Group

Online Privacy Breaches, Offline Consequences: Construction and Validation of the Concerns with the Protection of Informational Privacy Scale

Eric Durnell[a], Karynna Okabe-Miyamoto[b], Ryan T. Howell[c], and Martin Zizi[a]

[a]Aerendir Social Research, Aerendir, Mountain View, CA, USA; [b]Department of Psychology, University of California, Riverside, CA, USA; [c]San Department of Psychology, San Francisco State, California State University, San Francisco, CA, USA

ABSTRACT

Concerns with protecting privacy, especially of online data, has been a goal of privacy scholarship for years. Because most data are transferred online, many instruments focus on online environments. However, when privacy is invaded and data mishandled, the consequences, including the emotional ramifications, extend beyond the online space and into the offline world. Thus, we developed the CPIP, a measure of privacy concern. We were able to (1) determine the top four domains for informational privacy and (2) correlate that concern with emotional outcomes showing people with high concerns felt less calm, less at ease, and angrier, after reading prompts about the right to privacy protection. The CPIP predicts who experiences an emotional reaction to a loss of privacy and steps for Internet providers collecting data online to create a better balance for users and their privacy. This alignment (or misalignment) of attitudes and behaviors challenge the privacy paradox.

Over 30 years ago, Mason (1986) voiced ethical concerns over the protection of informational privacy, or "*the ability of the individual to personally control information about one's self*" (Stone et al., 1983), calling it one of the four ethical issues of the information age. Since the 1980s, scholars have remained concerned about informational privacy, especially given that trillions of gigabytes of data are collected online (Beke et al., 2018). Every *minute* in 2019, Americans used an estimated 4,416,720 GB of Internet data and users performed 4,497,420 Google searches (Domo, 2019). Given the staggering amount of private information shared online, much of the research on informational privacy, not surprisingly, focuses on the Internet. However, when data are mishandled online, the consequences of privacy breaches extend beyond the online environment. In essence, invasions of online privacy jeopardize offline privacy, as one cannot protect their offline privacy if their online privacy is not protected.

Many people express concerns about privacy (Jupiter, 2002) and, specifically, a desire to control how personal information is obtained and used by companies (Castañeda & Montoro, 2007). Yet demographic differences exist. Females, compared to males, tend to report higher privacy concerns (Fogel & Nehmad, 2009; Hoy & Milne, 2010; Mohamed & Ahmad, 2012). Older adults tend to be more concerned about their privacy than younger adults (Paine et al., 2007), possibly because younger adults feel more knowledgeable about their online privacy options. In contrast, older adults are less aware of protection strategies, especially on Facebook (Brandtzæg et al., 2010).

The widespread nature of privacy concerns has prompted researchers to examine whether such concerns may correlate with adverse emotional outcomes. For example, greater concern over whether websites track Internet activity associates with more anxiety and less happiness (Pappas et al., 2013). And yet, individuals continue to share personal information freely online (Brandtzæg et al., 2010). Recent scholarship has examined this apparent paradox of people expressing privacy concerns while continuing to engage in online behaviors that compromise that privacy. One explanation states that individuals may feel helpless about their privacy or think that protecting their privacy is futile (Xie et al., 2019). However, given that distress and lower levels of happiness are linked to harmful psychological outcomes, such as depression (Headey et al., 1993; Seligman & Diener, 2002), these findings highlight the need to more adequately understand and address the causal connection between privacy concerns and negative emotions, and expands the scope of the privacy issue into a new ethical dimension.

1. Privacy

Privacy is a human right. Human rights were first guaranteed in 1215 with the Magna Carta (e.g., the right to inherit property and the limitation of taxes), and centuries later, privacy was described by Warren and Brandeis (1890) as the right of the individual to be free from intrusion (i.e., "*to be let alone*"). Later, others argued that privacy includes the protection of one's autonomy and freedom from surveillance (e.g., physical, psychological, and data surveillance or observation; see Westin, 1967). Then in 2007, after reviewing various philosophical and legal theories, Tavani argued that privacy includes numerous attributes (e.g., nonintrusion, seclusion, limitation, and control of information about the self) and developed the restricted access/

CONTACT Eric Durnell edurnell1700@gmail.com Aerendir Social Research, Aerendir, Mountain View, CA, USA

limited control theory of privacy. Tavani defined privacy as a situation in which one has protection from intrusion and can control one's information by restricting others' access to it. Stone et al.'s (Stone et al., 1983) definition of informational privacy was similar: "*The ability of the individual to personally control information about one's self.*"

1.1. Measuring concerns for privacy online

The Internet is the primary environment for informational privacy, as this is where most information is transferred, collected, and stored. Privacy concerns are inherent to the process of using the Internet because users' personal information is continuously shared, both passively and actively, as users browse. For example, automated recommender systems, or cookies, are designed for tracking and recording frequently visited websites. That information is typically used to generate suggested search results and can be sold to corporations for creating targeted ads. But the same data can also be easily accessed or even hacked when a breach of security occurs. Because of the ubiquity of online data-sharing, most research around privacy concerns has tended to focus on users' attitudes about how their personal information is acquired, stored, and used by companies and organizations (Wang et al., 2020). As a result, extensive measures, including legislation, have been undertaken to protect private information, such as the California Consumer Privacy Act (CCPA) and the General Data Protection Regulation (GDPR). Ultimately, as Proctor et al. (2008) argue, "*issues relating to consumer privacy and the privacy policies of organizations are of vital concern to persons interacting with the Web.*"

Much of the foundational research, dating back to the 1990s, has involved creating measures that focus on concerns over data privacy and protection on computer systems. For example, Smith, Milberg, and Burke's (Smith et al., 1996) Concern for Informational Privacy scale contains 15 items measuring concern in four dimensions of online organizational information privacy practices: collection (i.e., whether extensive identifiable data is being collected and stored); errors (e.g., inadequate protection against errors); unauthorized secondary use (e.g., whether and how data are collected for additional purposes such as disclosure to a third party); and improper access (i.e., access to personal data by unauthorized individuals). Although the original scale was reliable, valid, generalizable, and adequately demonstrated that privacy concerns emerge as a latent variable from other concerns, Steward and Segars (2002) argued only six years later that, given recent changes to organizational practices, the items needed to be reevaluated.

In the 2000s, Malhotra et al. (2004) developed the Internet Users' Informational Privacy Concerns (IUIPC) scale, which measures three factors: collection (i.e., the benefits accrued from giving up personal information); control (i.e., whether individuals have control over their personal information); and awareness (i.e., of organizations' information-privacy practices). All of these factors are related to privacy on the Internet. Buchanan et al. (2007) measured privacy concerns and attitudes as well as privacy-protection safeguards and behaviors using a single composite measure. The Measure of Online Privacy Concern and Protection for Use on the Internet examines three facets: privacy concerns (i.e., about data misuse, misrepresentation, and online fraud), general caution, and technical protection (the last two being behavioral measures). These facets were distinct from those measured within the Westin Privacy Segmentation Scale (Harris and Associates Inc & Westin, 1998) and IUIPC Scale. However, again, this measure was limited to concerns about online privacy.

More recently, Baruh and Cemalcilar (2014) developed a multidimensional privacy-orientation scale that included four factors: (1) privacy as a right; (2) concerns about one's own informational privacy; (3) other-contingent privacy; and (4) concern about the privacy of others. Although the four factors effectively predicted privacy-protective behaviors, the authors developed the scale particularly to measure the privacy attitudes of social network site (SNS) users. While this is not a comprehensive list of measures assessing privacy in the literature, an overwhelming majority have been created specifically to focus on privacy in an online environment.

Other researchers have measured privacy concerns without undertaking to explicitly develop and validate a scale, but many still focus on the online environment. For example, Sheehan and Hoy (2000) had 889 online users rate their levels of concern with various privacy-invasive marketing practices. Overall, the participants were most concerned with practices that threatened the control of information (e.g., "Information about you is sold to another company") and were less concerned with organizational practices deriving from established relationships (e.g., "You receive an e-mail from a company you currently do business with"). Additionally, researchers have evaluated how concerned individuals are about their privacy when using the Internet, demonstrating increased concern with age. For example, 80% of participants over the age of 40 were concerned about privacy, whereas only 45% of those age 20 and younger were concerned (Paine et al., 2007). Dinev and Hart (2003) measured privacy concern by having 369 respondents complete a 13-item survey as part of a larger research project. They found that trust in the Internet and privacy concerns mediated the relationship between vulnerability and perceived control in Internet usage. The researchers also concluded that privacy concerns were detrimental to e-commerce transactions. In a similar vein, Earp et al. (2005) had respondents complete a 36-item survey to measure what Internet users valued within privacy policies. They compared the results to the privacy policies on various organizations' websites and found that, in contrast to the companies' posted policies, Internet users were most concerned about their information being provided to other companies.

1.2. Offline privacy in an online world: The psychological impact of privacy concerns

As a body of scholarship, the privacy literature to date has focused almost exclusively on privacy in an online environment. Yet, online privacy captures only a fraction of the universe of informational privacy and seems to underappreciate the fact that when privacy is invaded the ramifications extend into the offline world. For example, in 2014, the iCloud accounts of countless celebrities were hacked, leaking private and lewd

images onto the Internet for public viewing. In 2017, Equifax, one of the largest credit reporting agencies, was hacked, revealing the personal data of nearly 143 million customers, including social security numbers, home addresses, and birth dates. An even more well-documented breach of privacy, which led to a publicized scandal, occurred in 2018 with Cambridge Analytica. The political consulting firm reportedly harvested data from nearly 87 million Facebook users (and their non-consenting friends) to gain psychological insights to sway political campaigns across the globe. Online invasions of privacy impact the offline world, whether they be violations of one's intimate (e.g., personal photos), financial (e.g., credit data), or social privacy (e.g., Facebook data of non-consenting friends). Thus, understanding the general domains (including online) in which people want their privacy protected will allow researchers to bridge the gap and understand how people feel about their privacy both online and offline.

Another important ethical dimension of privacy that must be understood is the emotional consequences of online to offline privacy spillovers. Few researchers have explored the link between privacy and emotions but the scant literature on this topic suggests that privacy concerns correlate negatively with happiness and positively with anxiety (Pappas et al., 2013). Past research has demonstrated that lower levels of happiness and higher levels of anxiety affect psychological and physiological health, such as lower satisfaction with life and increased depression (Seligman & Diener, 2002). Indeed, many individuals adopt a fatalistic outlook when it comes to controlling and their protecting privacy (Xie et al., 2019), and similar losses of control have been linked to depressive tendencies (Mirowsky & Ross, 1996).

2. Current study

Nearly all validated scales that measure concern about the violation of informational privacy have focused on online privacy and have not investigated the well-being of the user. And while these measures lay a vital foundation for understanding perceptions of privacy online, which is valuable in the current age of information, we must expand that understanding by investigating how concern over online privacy impacts people offline as well. Of particular interest are the various *domains* in which people want certain information to be kept private (e.g., financial, health, technological, etc.) and how concern over the invasion of one's privacy affects emotional well-being. As such, the goal of this current research is to create a measure of informational privacy concern. Moreover, our study will investigate the negative emotional ramifications of having privacy concerns across different domains. We hypothesize that respondents will (1) express high concern about their privacy; (2) more highly value the protection of their privacy in certain domains over others; and (3) report more negative emotionality when they have greater concerns over privacy and feel information they consider to be private is compromised.

Across two pilot studies and three survey studies, we sought to (1) determine which domains of informational privacy were most important to users (Pilot Studies 1 & 2); (2) develop scale items for the CPIP (Study 1); (3) examine the factor structure of the CPIP (Study 2); (4) test the utility of the CPIP (Study 2); (5) test the reliability of the CPIP (Study 3a); and (6) test the validity of the CPIP (Study 3b). The authors declare that they have no conflicts of interest. All procedures performed in studies involving human participants were in accordance with the ethical standards of the academic institution. Informed consent was obtained from all individual participants involved in the study. Importantly, data from the first survey (Study 1) were collected and analyzed prior to Facebook's CEO, Mark Zuckerberg, testimony to Congress (April 11th, 2018) about the social media giant's collection and storage of users' private information. Given that this case was one of the first highly public cases that garnered attention worldwide regarding the protection of users' private information, we suspect these results provide a conservative snapshot of how people viewed their privacy prior to Zuckerberg's testimony and can be taken as a baseline for future studies examining privacy concerns.

3. Pilot 1: Open-ended list of information people want protected

A goal of the two pilot studies was to identify the domains people rated as most important for privacy protection. Our findings would inform our development of the Concerns with the Protection of Informational Privacy Scale (CPIP). We used an open-ended survey format to elicit responses from participants.

3.1. Participants

We recruited 130 U.S. adults through Amazon's Mechanical Turk (MTurk; see Buhrmester et al., 2011; Paolacci et al., 2010, for justification for employing MTurk participants in research), an online service in which people can sign up as "workers" and receive payment for completing surveys. Our Mturk announcement invited people to participate in a human intelligence task (HIT) entitled "What part of your life do you consider private?" Using an open-ended response format, participants listed the types of information they considered private and were paid 0.20 USD each to complete the survey. We did not collect demographic information.

3.2. Method and results

Participants read the following instructions:

> The goal of the current study is to better understand the types of information you consider to be private. While privacy is an important part of life, historically, describing privacy has been difficult because there are so many definitions of it. We feel that there are many domains of privacy that must be examined and understood to better understand what information you consider to be private. What are the different parts of your life you are protective of and would like to be considered private? Please type as many single-word or short phrases describing the different areas of your life where you feel that information is private.

Participants listed up to 10 areas of life where they wanted information kept private, and the open-ended responses were coded. For example, responses of "bank account information,"

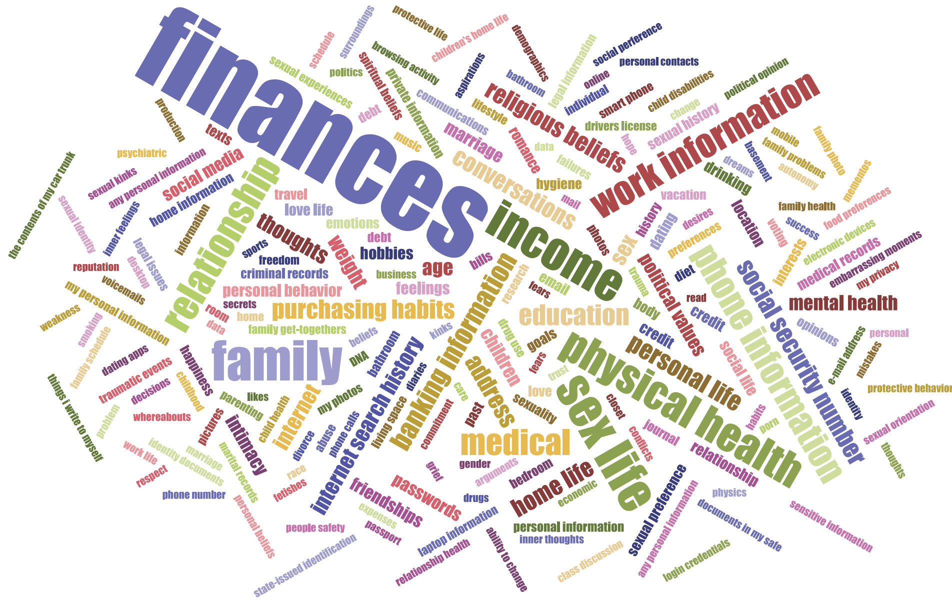

Figure 1. A word cloud of individual responses indicating the areas of life people want protected.

"credit," "income," and "salary" were coded into the category "financial information." The responses "social security number," "phone number," "personally identifying information," and "personal thoughts" were coded as "personal information." Words and phrases such as "conversation(s)," "work information," "communication(s)," and "children" were coded as "confidential information." All 945 coded responses (an average of 7.27 per participant) were used to create a word cloud to reveal the most commonly mentioned categories (see Figure 1). Financial information mentioned by 18.5% of the sample, followed by personal information (17.6%), and confidential information (6.6%).

A total of 26 unique privacy domains emerged from the coding task: (listed in alphabetical order with examples): behavioral (drinking, smoking, hygiene); confidential (workplace, disabilities, social security number); document (marriage and medical records, passports); educational (grades, school ranking, educational background); emotional (emotional state, traumatic events, grief); family (names, photos, schedules); financial (bank accounts, debt history, income); health (current health, health history, medications); individual (age, gender, ethnicity); legal (criminal history, legal problems, communication with lawyers); locating (current location, where you can be found); mail (what you mail and when); hobbies (leisure activities and interests, amateur interests); personal (thoughts, struggles, work life); physical (diet, weight, DNA, body type); political (voting history, political party affiliation); purchasing habits (spending, shopping, food purchases); relationships (dating history, current status or details); religious beliefs (views on religion, style of worship); safe space information (what you say in a classroom or workplace); sex life and sexual behavior (fetishes, sexual activity, sexual desires); sexual orientation (sexual preference, sexuality, sexual identity); social (activities, acquaintances, conversations); spatial orientation (GPS location monitoring); spiritual (beliefs, spirituality); and technical (search or web history, e-mail address, text messages, social media).

4. Pilot 2: Measuring the most valued domains of privacy

In the second pilot study, we used the 26 categories identified in the first pilot study to measure and identify the most important domains of privacy to include in the CPIP.

4.1. Participants

Our sample consisted of 405 U.S. adults recruited from MTurk (*M*age = 38.00, *SD* = 12.90, range = 18–76; 56% female; 73% Caucasian/White; 53% reported incomes higher than 50,000 USD; 52% with a bachelor's degree or higher; 77% working for pay or self-employed). The participants were geographically diverse, representing 42 of 50 states. Our MTurk announcement invited people to participate in a HIT focused on identifying the domains of their lives they wanted to keep private. We used TurkPrime (Litman et al., 2017) to exclude participants who took part in Pilot Study 1, to verify geographic locations, and to minimize the probability of compromised data. Participants were paid 0.15 USD to complete this task.

4.2. Method

The participants read the same passage about privacy as in Pilot Study 1. Then they read the following instructions:

> Please read each of the following areas of your life that you may want to be free from unauthorized observation, viewing, or intrusion. Select at least 5, but no more than 10, domains of your life you strongly believe must be kept private.

Participants then selected the privacy domains they considered most important to protect, using the 26 categories extracted from the first pilot study.

4.3. Results and brief discussion

Overall, Pilot Study 2 revealed that respondents were concerned with the protection of various kinds of personal information. Table 1 shows the percentage of participants who selected each domain. The top domain respondents believed must be kept private was financial information (73%). In contrast, only 4% of people believed that spiritual information was important to protect. To ensure an adequate but non-exhaustive number of domains, we combined some categories to create larger domains. Ultimately, four overarching domains emerged: financial information (e.g., bank account data, spending habits); social and psychological information (e.g., sexual preferences, religious beliefs); legal information (e.g., social security number, criminal history); and technological information (e.g., online information like social media or GPS location).

5. Study 1: Scale development

The goal of Study 1 was to develop the CPIP with items that measure individual differences in concerns about privacy protection – namely the four informational privacy domains that emerged in Pilot Study 2: Financial, social/psychological, legal, and technological. Our aim was to determine whether these proposed domains were distinct enough to be measured as separate constructs on the CPIP.

5.1. Method

5.1.1. Participants and procedure

We recruited 335 community members (34.3% 18–25 years old, 2% older than 66; 53% female; 17% Caucasian) from three proximal geographic locations (San Francisco, Oakland, and San Jose, CA) to complete a 10-page survey that took approximately 10 minutes. The survey was described as measuring their attitudes concerning privacy. Each participant was compensated with a 10.00 USD gift card.

The survey had four sections: (1) a demographic questionnaire (e.g., gender, age, marital status, number of children), (2) items measuring attitudes toward privacy, (3) items measuring usage of electronic devices (smartphone, desktop, laptop, or tablet) for banking or social media use via the internet. For the purposes of Study 1, we only analyzed the items measuring attitudes toward privacy.

5.1.2. Item development

All items were written without any references to current privacy or data-protection practices to ensure a timeless measurement that could stay relevant with changing technology. Participants were instructed to answer the questions as honestly as possible by rating their agreement with each statement on a scale from 1 (strongly disagree) to 5 (strongly agree). Seventeen items were used to measure attitudes and actions taken to protect social and psychological privacy, legal privacy, financial privacy, and technological privacy.

5.2. Results

Table 1 shows the means, standard deviations, and intercorrelations of all attitudes toward the information privacy domains for Study 1. First, consistent with a number of previous studies (Jupiter, 2002), participants overwhelmingly felt that all information privacy domains were important to protect. For example, 90% agreed that protecting technological privacy was important. Further, the overall means for the concern for privacy among all domains were very high (> 4.00 on a 5-point Likert scale). Specifically, the average concern for the protection of these four domains was significantly greater

Table 1. Percentage of participants from pilot study 2 selecting each life domain as one they wanted protected.

Domain of Privacy (examples)	Percentage
Financial information (bank account data, debt history, income)	73
Confidential information (workplace, disabilities, social security number)	68
Sex life and sexual behavior (fetishes, sexual activity, sexual desires)	60
Health information (current health, healthy history, medications)	51
Locating information (current location, where you can be found)	50
Legal information (criminal history, legal problems, communication with lawyers)	49
Technical information (e-mail address, text messages, social media)	46
Document information (marriage and medical records, passports)	43
Personal information (personal thoughts, struggles, work life)	42
Physical information (diet, weight, DNA, body type)	33
Family information (names, family photos, family schedule)	32
Emotional information (emotional state, traumatic events, grief)	30
Mail (what you mail and when)	26
Behavioral information (drinking, smoking, hygiene)	22
Relationships (dating history, current relationship status or details)	20
Purchasing habits (spending, shopping, food purchases)	19
Political information (voting history, party affiliation)	17
social information (social activities, conversations with friends)	17
Spatial orientation (where you travel, where you go).	15
Sexual orientation (sexual preference, sexuality, sexual identity)	15
Safe space information (what you say in a classroom or workplace)	15
Individual information (age, gender, ethnicity)	13
Religious beliefs (views on religion, style of worship)	10
Education information (grades, school ranking, educational background)	8
Personal hobbies (leisure activities and interests, amateur interests)	5
Spiritual information (spiritual beliefs, spirituality)	4

Participants were instructed to select 5–10 domains of privacy they wanted protected.

Table 2. Study 1 descriptive statistics, internal consistency, and correlations for domains of the informational privacy variables.

	M	*SD*	1	2	3	4
1. Social and Psychological	4.09	.61	–			
2. Legal	4.07	.74	.65**	–		
3. Financial	4.41	1.33	.42**	.30**	–	
4. Technology	4.40	.82	.55**	.48**	.18**	–

N = 335. The technology construct was measured with a single item.
* p <.05; ** p <.01

than 3.00, signifying that, on average, people were concerned across various privacy domains (all p-values <.001; all d-effect sizes > 1.06). These results support Hypothesis 1 and Hypothesis 2, demonstrating that participants value their privacy regardless of the domain, but some domains were felt to be more important than others.

Next, the intercorrelations were moderately high for the separate domains (See Table 2 for all intercorrelations, means, and standard deviations). Specifically, concern for social/psychological information privacy correlated highly with both concern for legal information privacy, r (333) = .65, p < .001, explaining 42% of the variance, and with concern for technological information privacy, r (333) = .55, p < .001, explaining 30% of the variance. However, the correlation between concern for financial and technological information privacy was comparatively weak, r (333) = .18, p < .001, explaining only 3% of the variance. Given that the variance *unexplained* by our domains range from 97% to 58%, each domain measures a unique facet of privacy and each domain is a separate construct.

6. Brief discussion

The results of Study 1 address some of the fundamental questions about individual differences in concern over the protection of personal information in specific domains. First, we found that people felt that the protection of personal information was important in all four domains. This is consistent with previous results showing that individuals are generally concerned with violations of information privacy when online (Harris, 2004; Harris & Westin, 1998; Jupiter, 2002). Importantly, although the average level of concern was high for each domain, the correlations between the domains were relatively weak. Thus, each domain represents a unique facet of informational privacy concern and it remains necessary to measure all four specific domains in order to gain a fuller understanding of individual privacy concern.

7. Study 2: Factor analysis and utility analysis

In Study 1 we determined that the four information privacy domains were indeed unique and separate constructs. Thus, in Study 2, we tested the reliability of the domain measurement along with a general concern for privacy by creating the Concerns with the Protection of Informational Privacy Scale (CPIP). We also wanted to diversify our sample beyond the Bay Area to determine whether the scale could be generalized across diverse populations. Finally, given the emotional repercussions of a perceived loss of informational privacy, Study 2 also aimed to examine the utility of the CPIP in predicting discrete changes in mood. As such, we had participants read various domestic and foreign documents (e.g., 1st Amendment of the Constitution) that highlight one's current guaranteed right to privacy. We hypothesized that the strongest emotional reactions would be experienced by people with the highest scores on the CPIP: General scale.

7.1. Method

7.1.1. Participants

We recruited participants via an MTurk announcement inviting people to complete a 20-minute online survey. This survey was described as identifying people's attitudes toward the protection of their privacy and actions they might take to protect their privacy. To recruit an international sample, we posted country-specific HITs with the goal of drawing participants from outside the United States and India (the two largest participant pools on MTurk). We used TurkPrime (Litman et al., 2017) to exclude participants who responded to any of our previous studies, to verify locations, and to minimize the probability of compromised data. Participants were paid 0.50 USD to complete the task. We recruited 593 adult respondents and purged data from 56 who failed to follow or understand the instructions. Our final sample of 537 participants (50% 26–35 years old, >1% older than 66; 39% female; 56% Caucasian) came from numerous countries.

7.1.2. Procedure

To better understand how to measure concerns about informational privacy protection, we wrote a number of new items. This allowed us to examine the factor structure, internal consistency, and utility of our newly constructed general measure as well as our four domains of information privacy. Thus, the survey in Study 2 included a total of 107 items, about 15 to 20 randomized items per domain/block. Participants rated their agreement on a Likert scale from 1 (strongly disagree) to 5 (strongly agree) for all items, which were administered in five separated and randomized blocks based on domain. At the beginning of each block, we operationally defined the domain and asked participants to acknowledge that they understood the operational definition. For example, if a participant was randomly assigned to begin with legal information in the first block, the operational definition of "legal information" would appear and participants would be asked if they understood the definition.

To demonstrate the utility of the CPIP, we used an ABA design to measure people's emotions before and after they read text about privacy rights. These texts related to how various domestic and foreign documents addressed the right to privacy (e.g., the 1st, 4th, 6th, and 9th Amendments of the U.S. Constitution, the Right to be Forgotten, and the Health Insurance Portability and Accountability Act [HIPPA]; see Appendix A), and were intended to make salient people's right to privacy. The participants first rated their current emotions using the PANAS-X (Watson, 1988). Next, they read about how the various documents guaranteed a right to

privacy. This allowed us to measure how participants felt about a loss of privacy. Then they rated their current emotions again using the same PANAS-X survey. We were particularly interested in the change in emotions among those who scored high and low on a general concern for the protection of informational privacy.

7.1.3. Item creation

Not only did we measure attitudes about protecting privacy in specific domains of privacy, we also included 17 items to measure general attitudes toward protecting information privacy (e.g., "*I feel that it is important to keep personally identifiable information private*"). For each of the four domains we created items to measure attitudes and specific actions taken to protect that domain of privacy: social and psychological privacy (18 items; e.g., "*I feel that the state or condition of being free from being disturbed by other entities is important*"); legal privacy (27 items; e.g., "*I feel that the ability to prevent the nonconsensual disclosure of sensitive information is a right for all people that are currently involved in any form of civil litigation*"); financial privacy (25 items; e.g., "*I feel that it is important to prohibit the unwanted access of your financial data to third parties without your authorization.*"); and technological privacy (20 items; e.g., "*I feel that online activities should be conducted without intrusions from corporations*").

7.2. Results

7.2.1. The factor structure of the CPIP: General concern

We first performed an exploratory principal component analysis (PCA) on the 17 items measuring general concern with protection of informational privacy. The number of components was always determined by a parallel analysis. We found that seven general items loaded onto a single component with loadings greater than .60. We removed the 10 items with low loadings and conducted a second PCA. For this PCA, we extracted components. The same seven items formed a single component. However, because two were semantically very similar, we dropped the one with the lower loading. The remaining six items were internally consistent (α = .84), so we retained them as our scale to measure attitudes toward the protection of informational privacy (see Appendix B for all items retained in the CPIP).

Because we collected an international sample, our first goal was to compare the standardized root mean square residuals (SRMRs) as a measure of fit across the five geographic locations to ensure the factor structure was similar. First, the SRMR for each culture indicated good fit. Second, we examined whether attitudes toward the protection of informational privacy differed between the five countries (see Figure 2). The only difference was that participants in India had significantly lower attitudes about the protection of informational privacy (all *p*s < .002), however they did, on average, still care about privacy. Thus, because of the similar factor structure and average importance of protecting informational privacy, we decided to conduct all subsequent analyses on the full sample.

7.2.2. The factor structure of the CPIP: Concern with particular domains

We performed a second exploratory PCA with a promax rotation on the 90 items measuring concern with privacy in our four domains. Again, we retained items with loadings greater than .60. Interestingly, only 18 items had a loading less than this, and only a single item had a cross loading. These 19 items were removed from further analyses. Because many items had strong semantic similarity, similar items with lower loadings were dropped, which resulted in constructs with eight or nine items each. We then conducted the second PCA. We achieved a simple structure, in that each item loaded strongly (>.50) onto exactly one of four distinct components (all cross-loadings were <.25). The means, standard deviations, and inter-correlations of these four components are shown in Table 3.

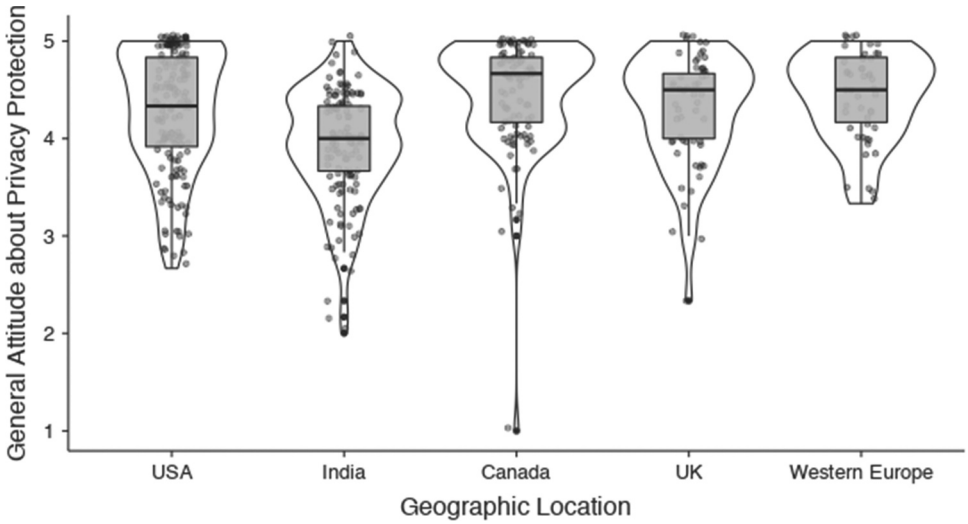

Figure 2. Violin plots of attitudes about general privacy protection across our five geographic locations. Higher scores indicate greater agreement with the need for privacy protection. The only significant difference is that the participants from India had significantly lower attitudes about privacy protection (all *p*-values <.002) than people from other areas.

Table 3. Study 2 descriptive statistics, internal consistency, and correlations for domain specific attitudes about privacy protection.

	M	*SD*	α	1	2	3	4
1. Legal	3.80	.72	.89	–			
2. Psychological	3.86	.72	.89	.36**	–		
3. Financial	3.94	.78	.93	.41**	.42**	–	
4. Technological	4.23	.69	.91	.43**	.41**	.45**	–

N = 495–517 (sample sizes differed because some respondents did not answer all questions). See the method section for demographic characteristics.
* p <.05; ** p <.01

Next, we explored the correlations among the four domains. First, even though we used a promax rotation to determine the structure of the survey, which allows constructs to be correlated, all correlations among the domains were moderate. For example, the strongest correlation was between financial and technological privacy (r = .45), while the weakest was between legal and psychological privacy (r = .36). As expected, each domain was also internally consistent (α = .89 – .91). Also, the means of each domain indicated that most participants were concerned with the protection of personal information in every domain. Finally, we performed regression analysis to better understand how the four domains predicted general concern with privacy protection. Although each domain was a significant positive predictor of increased concern for privacy protection in general, concern with the protection of technological privacy was overwhelmingly the strongest predictor (F(1,419) = 190.38, p < .001), uniquely explaining 21% of the variance in general privacy concerns.

7.2.3. Utility analysis

After completing the CPIP items, participants completed the full PANAS-X, which includes 60 discrete emotions (e.g., cheerful, angry, surprised) to rate their own emotional states at that moment ($\alpha_{\text{Pre-PA}}$ = .96; $\alpha_{\text{Pre-NA}}$ = .98). They then read the governmental documents granting individual rights to privacy (again, see Appendix A). Finally, they completed the full PANAS-X again ($\alpha_{\text{Post-PA}}$ = .96; $\alpha_{\text{Post-NA}}$ = .98).

As we expected, numerous discrete emotions changed after reading the privacy rights documents. For example, participants reported being less cheerful (t[525] = – 7.07, p < .001, d_z = – .31), calm (t[522] = – 6.51, p < .001, d_z = – .28), happy (t[524] = – 6.44, p < .001, d_z = – .28), relaxed (t[522] = – 5.54, p < .001, d_z = – .24), and joyful (t[523] = – 4.69, p < .001, d_z = – .20), and being more surprised (t[525] = 5.33, p < .001, d_z = .23), angry (t[524] = 3.46, p < .001, d_z = .15), astonished (t[525] = 2.87, p = .004, d_z = .13), hostile (t[521] = 2.70, p = .007, d_z = .12), and disgusted (t[525] = 2.79, p = .005, d_z = .12) after reading about rights to privacy. These changes were consistent regardless of geographic location. Interestingly, some specific emotions did not change, including nervousness (t[524] = .26, p = .799, d_z = – .01), anger at oneself (t[522] = .15, p = .877, d_z = – .01), and feeling blue (t[522] = – .05, p = .96, d_z = .00), sheepish (t[522] = 0.00, p = 1.00, d_z = .00), or guilty (t[525] = .19, p = .853, d_z = .01).

To demonstrate the utility of the CPIP, we examined whether a general concern for protecting informational privacy moderated the emotional changes observed after participants read the privacy rights laws (Appendix A). Overall, people who were, in general, highly concerned with informational privacy protection had stronger emotional reactions than those who were not as concerned, supporting Hypothesis 3. The interaction between change in emotions and general concern for privacy was significant for decreased sluggishness (F(1,506) = 4.83, p = .028), calmness (F(1,504) = 11.46, p < .001), ease (F(1,500) = 4.15, p = .042), and enthusiasm (F(1,506) = 5.03, p = .024). The interaction was also significant for increased surprise (F(1,507) = 13.63, p < .001), amazement (F(1,505) = 6.09, p = .014), and nervousness (F(1,506) = 6.97, p = .009). In each of these models, post-hoc comparisons (with Tukey corrections) between the slopes in cases of high and low concern for privacy revealed that the strongest emotional reactions for participants with the greatest concern for privacy protection were steeper (see Figure 3 for a comparison of changes in calmness and surprise by concern for protection of informational privacy). Thus, the CPIP explained who had the strongest emotional reactions to being reminded of their right to privacy.

8. Brief discussion

The results of Study 2 strengthened the support of the CPIP as a reliable measure of concern for informational privacy. Importantly, we examined the descriptive statistics and psychometric properties in cultures outside of the U.S. to increase the generalizability of our results. That is, to address some of our fundamental questions we recruited an international sample which consisted of 33% from the U.S., 27% from India, 19% from Canada, 12% from the United Kingdom, and 10% from other Western European countries. The results from these cultures we consistent with the past literature. For example, while CPIP when administered in the U.S. indicated good fit (standardized root mean square residuals = .04) and the SRMS demonstrated good fit for other cultures as well (e.g., India = .05; Canada = .03; U.K. = .07; Western Europe = .06). Interestingly, though the factor structure was similar across cultures, there were cultural differences in the concern for protecting informational privacy. For example, while 84% overall reported being concerned with technological privacy protection, concern was highest in Canada 93% and in the U.K. (88%), but was lowest in the U.S. (80%) and India (72%). Thus, the results from Study 2 can be reliability administered across various cultures.

9. Study 3: Reliability and validation of the CPIP

The goal of Study 3a was to examine the internal consistency and test-retest reliability of the CPIP. We used the reliability analyses to reduce the number of items for both the general scale and the four information privacy domain scales, such that only items that maximized the reliability coefficients were retained. The goal of Study 3b was to further demonstrate the construct validity of the CPIP. In Study 3b, we established the validity of the CPIP by correlating the general and domain

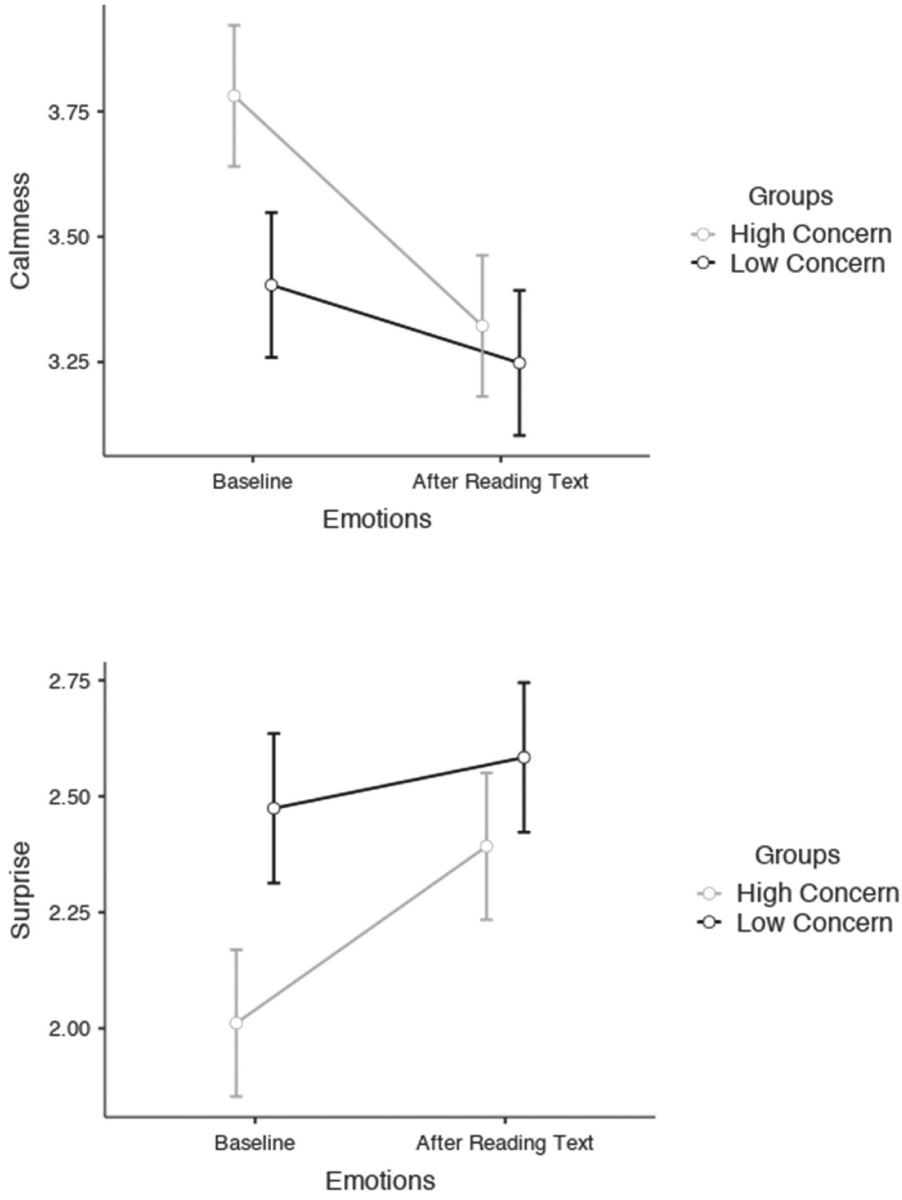

Figure 3. People with a high concern for privacy protection had a significant drop in calmness (M_D = –.46; SE_D =.07; t [504] = 6.81, p <.001); those with a low concern did not (M_D = –.16; SE_D =.08; t [504] = 2.07, p =.166). Those with a high concern also had a significant increase in surprise (M_D =.38; SE_D =.07; t [504] = 5.82, p <.001); those with a low concern did not (M_D =.11; SE_D =.07; t [504] = 1.51, p =.433).

scales with previously established demographic predictors of concern with informational privacy.

10. Study 3a: Reliability of the CPIP

10.1. Method

10.1.1. Participants

To establish the reliability of the CPIP and each of the four domains, we recruited participants from Amazon's Mechanical Turk to complete the CPIP once and then again 14 days later. Both surveys included all items retained in the surveys used for Study 1 and Study 2, as well as demographic questions. A total of 261 participants (M_{age} = 43.07, *SD* = 13.56, *range* = 18–76; 57.1% female; 81.6% Caucasian) completed both surveys and met all criteria to be included in all analyses. Participants were paid .50 USD for each survey they completed.

10.1.2. Procedure

Participants were informed that we would be asking questions about their feelings of privacy and their buying behaviors. They were also told that the study was a two-week study. Participants who (1) completed the first survey, (2) had a mobile device (e.g., a smartphone, tablet, or laptop), and (3) passed three attention checks were invited to take the second survey two weeks later. Those participants who completed the second survey and passed three more attention check were used in the final analyses.

10.2. Results

10.2.1. Internal consistency and temporal stability of the CPIP

First, we assessed the internal consistency and temporal stability of the general concern with informational privacy as well as the concern with each of our four domains. While assessing these reliability coefficients, we dropped items that did not contribute to improved internal consistency or temporal stability. Ultimately, we determined that all six of the items for the general concern with informational privacy contributed to the internal consistency and temporal stability of the scale. However, for each of the four domains the internal consistency and temporal stability was improved by retaining only four items each (see Appendix C for the final items retained for the CPIP).

Overall, the reliability coefficients from time 1 and time 2 for both the general scale and the four information privacy domains demonstrated good internal consistency. Also, the test-retest Pearson correlations for both the general scale and the four domains were statistically significant (all p's < .001). For example, the reliability coefficients demonstrated the reliability of: (1) the general concern with informational privacy scale (Time 1: M = 6.32, SD = .69, α = .88; Time 2: M = 6.32, SD = .68, α = .90; test-retest Pearson correlation: r (259) = .71, p < .001), (2) the concern with technological information privacy domain scale (Time 1: M = 6.35, SD = .74, α = .88; Time 2: M = 6.32, SD = .68, α = .90; test-retest Pearson correlation: r (259) = .70, p < .001), (3) the concern with financial information privacy domain scale (Time 1: M = 5.75, SD = 1.17, α = .91; M = 5.89, SD = 1.02, α = .88; test-retest Pearson correlation: r (259) = .59, p < .001), (4) the concern with psychological and social information privacy domain scale (Time 1: M = 5.52, SD = 1.05, α = .88; M = 5.59, SD = .99, α = .88; test-retest Pearson correlation: r (259) = .51, p < .001), and (5) the concern with legal information privacy domain scale (Time 1: M = 5.44, SD = 1.23, α = .92, M = 5.44, SD = 1.22, α = .92; test-retest Pearson correlation: r (259) = .36, p < .001).

11. Study 3b: Validity of the CPIP

11.1. Participants and procedure

to establish the validity of the CPIP and each of the four domains, we recruited participants from Amazon's Mechanical Turk to complete the CPIP and answer questions about how much they trusted mobile transactions and corporations to protect their privacy. At the end of the survey participants answered numerous demographic questions. Those participants who completed the survey and passed four attention checks were used in the final analyses. A total of 367 participants (M_{age} = 38.19, SD = 12.85, *range* = 18–74; 50.5% female; 64.9% Caucasian; 51.9% married; 51.6% living without children in the household) met all our criteria to be included in all analyzes. Participants were paid .50 USD for completing the survey.

11.2. Results

11.2.1. Validity of the CPIP

We assessed the validity of the CPIP by examining the correlation with age and gender to identify differences in concerns with informational privacy. Previous research has found that concern with information privacy is positively correlated with age (Paine et al., 2007) and that females are more concerned with informational privacy than males (Hoy & Milne, 2010). Additionally, we examined if those who were more concerned with the protection of their information privacy had less trust of m-commerce security as well as the security of specific corporations (i.e., Facebook and Amazon). We considered negative correlations between trust and concern with information privacy as support for the validity of the CPIP. We also examined the correlation with age and gender on the general scale and across all four domains.

First, we examined the descriptive statistics for the CPIP. As expected, the general scale as well as all four domains were significantly negatively skewed. Therefore, to assess the associations with age, gender, and trust, we report nonparametric correlations (specifically, Spearman's rho [r_s]). As expected, there was a positive association between age and a general concern with the protections of informational privacy (r_s [365] = .24, p < .001). Also, there were significant positive correlations with the domains of technological privacy protection (r_s [365] = .24, p < .001) and financial privacy protection (r_s [365] = .13, p = .012); however, age was not associated with concerns over the protection of psychological and social privacy (r_s [365] = − .08, p = .151) nor legal privacy (r_s [365] = .03, p = .560). Also, as expected, females were more concerned with the protection of information privacy in general (r_s [365] = .19, p < .001) and were specifically concerned with the domain of technological privacy protection (r_s [365] = .14, p = .009); however, there was no gender difference when assessing the domains of financial privacy protection (r_s [365] = .09, p = .865), psychological and social privacy protection (r_s [365] = − .04, p = .491), or legal privacy protection (r_s [365] = − .09, p = .100). Finally, as expected, there was a negative association with general concern with the protection of informational privacy and trust in: (1) data security when making purchases on a mobile device (r_s [365] = − .14, p = .007), (2) privacy protections on Facebook (r_s [365] = − .25, p < .001) or Amazon (r_s [365] = − .27, p < .001), and (3) online clothing retailers to protect privacy (r_s [365] = − .18, p < .001). The pattern of these results was only consistent with a concern over technological privacy.

12. Discussion

The primary goal of our research was to create a measure of privacy concern across general domains of information privacy, which will help bridge the gap between online and offline privacy. Moreover, we also aimed to identify the specific emotional outcomes of having high concerns for privacy. First, overwhelmingly, participants were concerned for their information privacy, replicating past research (Jupiter, 2002).

Second, across two pilot studies and three survey studies with a cross-cultural sample, we developed a highly reliable and valid measure of privacy concerns in four participant-driven and replicated information domains: technological, financial, social/psychological, and legal. Third, as expected, people were more concerned for their privacy in certain domains over others, with financial privacy being most highly valued. Fourth, demonstrating the validity of the scale, we also identified that those who expressed greatest concern with their information privacy also experienced fewer positive emotional outcomes (e.g., feeling less cheerful, less happy, less calm) and more negative emotions (e.g., anger and hostility) after reading excepts from government documents regarding individual privacy rights. Finally, demonstrating the predictive validity of the CPIP, when we examined which domain of informational privacy was the best predictor of more general concern for informational privacy, we found that concern for technological privacy substantially predicted general concern better than any other domain, even though the domains were only modestly inter-correlated. Thus, people who are highly concerned with technological privacy are the most likely to be concerned with informational privacy in general.

The privacy paradox suggests that there is a disconnect between people's attitudes and behaviors when it comes to information privacy. That is, while people express strong concern over their information privacy, they often act in ways that could jeopardize that privacy. For example, research has shown that increased perceived privacy risks (a correlate of privacy concerns) was not associated with reduced intention to use mobile social networking apps (Qin et al., 2018), signaling that although people may find a social networking app to be risky, this does not impact their intention to use the app. Importantly, meta-analyses have found that results related to the privacy paradox are mixed (Kokolakis, 2015). One explanation for why the privacy paradox emerges inconsistently relates to rational fatalism ideologies. Feelings of helplessness regarding control over one's privacy make individuals less likely to protect themselves as they feel any efforts to do so would be futile (Xie et al., 2019). These findings shed light on a deeper and more troubling social issue, that people do indeed care about their privacy but feel they have no volitional control. This could also be why researchers have found that strong privacy concerns are related to less happiness and more anxiety (Pappas et al., 2013).

Researchers have addressed the growing body of literature supporting the link between privacy and feelings of helplessness by calling on companies to have a better balance in power when it comes to users and their privacy (Draper & Turow, 2019; Hochheiser & Lazar, 2007). This is a critical point, as there are few alternatives to using many of services (e.g., search engines) that strip people of their privacy. Similarly, given that social media frequency leads to stronger social connections, and ultimately well-being (Roberts & David, 2020), quitting social media may lead to a cut in ties with friends and loved ones, especially those who are physically distant, and ultimately reduce well-being. Given the lack of options when it comes to Web-based services, it is no wonder that privacy paradox findings emerge.

While the privacy paradox may not provide actionable information for researchers and businesses, it is crucial to remember that these concerns are linked to negative psychological outcomes. Just after reading a short excerpt outlining current governmental privacy rights, participants in our study reported feeling greater negative emotions, such as hostility, disgust, and anger, and also reported fewer positive emotions, such as cheerfulness, calmness, and happiness (with large effect sizes). Moreover, those with the highest concerns about privacy reported the greatest emotional reactions after reading about their rights to privacy. Importantly, geographic location did not moderate the participants' emotional changes. If these emotional outcomes were induced (1) in an online survey and (2) after reading a short privacy excerpt, a notably conservative provocation of privacy concern, then the emotional ramifications of having one's privacy actually violated (e.g., having personal photos leaked, or an e-mail account hacked) are far graver than researchers currently estimate and warrant further investigation and action.

Another key issue, raised by Kokolakis (2015), is the diversity of measures used to assess the privacy paradox (e.g., surveys, experiments), which lead to varied results. Further, there is little nuance around how privacy attitudes are measured, leading to imprecise generalizations of attitudes and subsequent behaviors. Our measure, the CPIP, attempts to address these problems by disentangling privacy concerns into the domains of technology, finances, social/psychological, and legal information. For example, someone who takes the CPIP and reports high concern over financial information privacy and lower concern over legal information privacy may be more willing to engage in behaviors that would compromise legal privacy but less willing (or more reluctant) to jeopardize financial privacy. With the CPIP, researchers can parse where the privacy paradox holds and where it does not, perhaps leading to more precise observations of the privacy paradox.

12.1. Future directions

The results of our pilot studies and survey demonstrate the CPIP is a reliable and valid psychological measurement of privacy attitudes, in both online and offline contexts, across four important domains. Also, given that many of the scales in the privacy literature are specific to an online environment, the CPIP provides the field with a psychometrically sound measure of privacy attitudes that consider real-world implications. While the results from Study 2 suggested that the CPIP can be administered in different cultural contexts, it is important to recognize the key role culture plays in privacy concerns (Milberg et al., 2000) and be mindful of these differences when administering and interpreting the CPIP in different cultures. For example, those who live in an individualist culture, or a low-context culture (e.g., the United States, Western Europe, etc.), value autonomy and privacy; however, those who live in a collectivist culture, or a high-context culture (e.g., Asia, Latin America, etc.), value cohesion and trust (Bandyopadhyay, 2009). As such, previous research has demonstrated that those who live in

individualistic and low-context cultures tend to be more concerned with protecting their privacy, similar to the results we found.

For example, research in India has demonstrated that privacy is thought of as a spatial concept, rather than an informational one (Bellman et al., 2004). This is perhaps why previous research (Kumaraguru & Cranor, 2005) demonstrates that participants from India also report relatively lower concerns for their privacy – consistent with our results in Study 2. Moreover, it is important to keep in mind the relationship between cultural values and privacy regulation, as the former often shapes the latter (Milberg et al., 1995). Taken together, culture plays a key role in shaping privacy concerns and research should continue to unpack this relationship further, especially when examining the specific facets (e.g., legal, social/psychological) in which different cultures may place value in their privacy. In sum, while our data suggest a broad general phenomenon, we are careful to generalize our results to all cultures and recognize that privacy is deeply culturally-defined.

13. Conclusion

Today's globally networked society places great demands on the collection and sharing of person-specific data for many new uses. Entities that serve as data holders (or service providers), such as a hospitals, banks, and social networking sites, often describe the need to share person-specific records in such a way that the identities of their subjects can be determined. These ways are described as beneficial or at least non-intrusive to the individual because (a) the data are collected in large quantities and analyzed in aggregate, and (b) the private data being analyzed on an individual basis are deemed necessary to provide a customized or personalized experience when engaging the Internet of Things on various platforms.

Websites typically communicate privacy practices through terms and usage agreements that are intended to "*reduce the trade-off between personalization and privacy*" (Preibusch, 2006). However, when different types of data are bound together, they can provide a "detailed picture of each customer" (Resnick & Montana, 2003). This digital profile is as identifying and personal as a fingerprint, even when the information contains no explicit identifiers such as names or phone numbers. Also, as Mark Zuckerberg's Congressional on April 11th, 2018 highlighted, the near-complete erosion of information privacy is the new reality – one that angers and frustrates many consumers. Therefore, privacy is personal. But personalization without the full disclosure of potential loss of privacy brings a voice to a different conversation, one that speaks to why it is important to measure how people feel about their privacy (in all important domains) and the protection of it. This is why reliable scales like the CPIP are necessary.

While people are not often aware of how their data are stored and managed (Visinescu et al., 2016), research has demonstrated that people in general are willing to forgo some protection of their private information, whether in aggregate or individually, if they stand to benefit from it (see Dinev & Hart, 2003). With the CPIP, researchers can now (1) measure how people feel about privacy protection in general, and (2) understand the different information privacy domains people most want to protect – psychological, technological, legal, and financial – to see where and why people may be willing to sacrifice their privacy. As such, we can better understand who wants specific privacy protections and whether the benefits gained to offset the sacrifice of privacy vary among individuals. By understanding individuals' concerns over privacy protection in general and in specific domains, we can come to a better understanding of the actions needed to protect privacy.

References

Bandyopadhyay, S. (2009). Antecedents and consequences of consumers' online privacy concerns. *Journal of Business & Economics Research*, *7*(3), 41–48. https://doi.org/10.19030/jber.v7i3.2269

Baruh, L., & Cemalcilar, Z. (2014). It is more than personal: Development and validation of a multidimensional privacy orientation scale. *Personality and Individual Differences*, *70*, 165–170. https://doi.org/10.1016/j.paid.2014.06.042

Beke, F. T., Eggers, F., & Verhoef, P. C. (2018). Consumer informational privacy: Current knowledge and research directions. *Foundations and Trends in Marketing*, *11*(1), 1–71. https://doi.org/10.1561/1700000057

Bellman, S., Johnson, E. J., Kobrin, S. J., & Lohse, G. L. (2004). International differences in information privacy concerns: A global survey of consumers. *The Information Society: An International Journal*, *20*(5), 313–324. https://doi.org/10.1080/01972240490507956

Brandtzæg, P. B., Lüders, M., & Skjetne, J. H. (2010). Too many Facebook "friends"? Content sharing and sociability versus the need for privacy in social network sites. *International Journal of Human-computer Interaction*, *26*(11–12), 1006–1030. https://doi.org/10.1080/10447318.2010.516719

Buchanan, T., Paine, C., Joinson, A. N., & Reips, U. D. (2007). Development of measures of online privacy concern and protection for use on the Internet. *Journal of the American Society for Information Science and Technology*, *58*(2), 157–165. https://doi.org/10.1002/asi.20459

Buhrmester, M., Kwang, T., & Gosling, S. S. (2011). Amazon's mechanical turk: A new source of inexpensive yet high quality data? *Perspectives on Psychological Science*, *6*(1), 3–5. https://doi.org/10.1177/1745691610393980

Castañeda, J. A., & Montoro, F. J. (2007). The effect of Internet general privacy concern on customer behavior. *Electronic Commerce Research*, *7*(2), 117–141. https://doi.org/10.1007/s10660-007-9000-y

Dinev, T., & Hart, P. (2003). *Privacy concerns and Internet-use: A model of trade-off factors* [Paper presentation]. Academy of management, Briarcliff Manor, NY.

Domo. (2019). *Data never sleeps 7.0*. https://www.domo.com/learn/data-never-sleeps-7

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

Earp, J. B., Antón, A. I., Aiman-Smith, L., & Stufflebeam, W. H. (2005). Examining Internet privacy policies within the context of user privacy values. *IEEE Transactions on Engineering Management*, *52*(2), 227–237. https://doi.org/10.1109/TEM.2005.844927

Fogel, J., & Nehmad, E. (2009). Internet social network communities: Risk taking, trust, and privacy concerns. *Computers in Human Behavior*, *25*(1), 153–160. https://doi.org/10.1016/j.chb.2008.08.006

Harris. (2004). *National survey on consumer privacy attitudes*. http://www.epic.org/privacy/survey/

Harris, & Westin, A. (1998). *E-commerce and privacy: What net users want*. Privacy & American Business and PricewaterhouseCoopers.

Headey, B., Kelley, J., & Wearing, A. (1993). Dimensions of mental health: Life satisfaction, positive affect, anxiety, and depression. *Social Indicators Research*, *29*(1), 63–82. https://doi.org/10.1007/BF01136197

Hochheiser, H., & Lazar, J. (2007). HCI and societal issues: A framework for engagement. *International Journal of Human and Computer Interaction*, *23*(3), 339–374. https://doi.org/10.1080/10447310701702717
Hoy, M. G., & Milne, G. (2010). Gender differences in privacy-related measures for young adult Facebook users. *Journal of Interactive Advertising*, *10*(2), 28–45. https://doi.org/10.1080/15252019.2010.10722168
Jupiter. (2002). *Security and privacy data* [Paper presentation]. Washington, DC: Federal trade commission consumer information security workshop.
Kokolakis, S. (2015). Privacy attitudes and privacy behavior: A review of current research on the privacy paradox phenomenon. *Computers & Security*, *64*, 122–134. https://doi.org/10.1016/j.cose.2015.07.002
Kumaraguru, P., & Cranor, L. F. (2005). *Privacy indexes: A survey of Westin's studies*. Institute for Software Research International.
Litman, L., Robinson, J., & Abberbock, T. (2017). TurkPrime.com: A versatile crowdsourcing data acquisition platform for the behavioral sciences. *Behavior Research Methods*, *49*(2), 433–442. https://doi.org/10.3758/s13428-016-0727-z
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. https://doi.org/10.1287/isre.1040.0032
Mason, R. O. (1986). Four ethical issues of the information age. *MIS Quarterly*, *10*(1), 5–12. https://doi.org/10.2307/248873
Milberg, S. J., Burke, S. J., Smith, H. J., & Kallman, E. A. (1995). Values, personal information privacy, and regulatory approaches. *Communications of the ACM*, *38*(12), 65–74. https://doi.org/10.1145/219663.219683
Milberg, S. J., Smith, H. J., & Burke, S. J. (2000). Information privacy: Corporate management and national regulation. *Organization Science*, *11*(1), 35–57. https://doi.org/10.1287/orsc.11.1.35.12567
Mirowsky, J., & Ross, C. E. (1996). Fundamental analysis in research on well-being: Distress and the sense of control. *The Gerontologist*, *26*(5), 584–594. https://doi.org/10.1093/geront/36.5.584
Mohamed, N., & Ahmad, I. H. (2012). Information privacy concerns, antecedents and privacy measure use in social networking sites: Evidence from Malaysia. *Computers in Human Behavior*, *28*(6), 2366–2375. https://doi.org/10.1016/j.chb.2012.07.008
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. https://doi.org/10.1016/j.ijhcs.2006.12.001
Paolacci, G., Chandler, J., & Ipeirotis, P. G. (2010). Running experiments on Amazon Mechanical Turk. *Judgment and Decision Making*, *5*(5), 411–419. https://ssrn.com/abstract=1626226
Pappas, I. O., Giannakos, M. N., Kourouthanassis, P. E., & Chrissikopoulos, V. (2013). Assessing emotions related to privacy and trust in personalized services. *Conference on e-Business, e-Services and e-Societ* (pp. 38–49).
Preibusch, S. (2006). *Implementing privacy negotiations in E- commerce*. In X. Zhou, J. Li, H. T. Shen, M. Kitsuregawa, Y. Zhang (Eds.), *Frontiers of WWW Research and Development - APWeb 2006. APWeb 2006. Lecture Notes in Computer Science, vol. 3841*. Berlin, Heidelberg: Springer. https://doi.org/10.1007/11610113_53
Proctor, R. W., Ali, M. A., & Vu, K. P. L. (2008). Examining usability of web privacy policies. *International Journal of Human-computer Interaction*, *24*(3), 307–328. https://doi.org/10.1080/10447310801937999
Qin, L., Kim, Y., & Tan, X. (2018). Understanding the intention of using mobile social networking apps across cultures. *International Journal of Human-computer Interaction*, *34*(12), 1183–1193. https://doi.org/10.1080/10447318.2018.1428262
Resnick, M. L., & Montana, R. (2003). Perceptions of customer service, information privacy, and product quality from semiotic design features in an online web store. *International Journal of Human-computer Interaction*, *16*(2), 211–234. https://doi.org/10.1207/S15327590IJHC1602_05
Roberts, J. A., & David, M. E. (2020). The social media party: Fear of missing out (FoMO), social media intensity, connection, and well-being. *International Journal of Human-computer Interaction*, *36*(4), 386–392. https://doi.org/10.1080/10447318.2019.1646517
Seligman, M., & Diener, E. (2002). Very happy people. *Psychological Science*, *13*(1), 81–84. https://doi.org/10.1111/1467-9280.00415
Sheehan, K. B., & Hoy, M. G. (2000). Dimensions of privacy concern among online consumers. *Journal of Public Policy & Marketing*, *19*(1), 62–73. https://doi.org/10.1509/jppm.19.1.62.16949
Smith, H., Milberg, S., & Burke, S. (1996). Information privacy: Measuring individuals' concerns about organizational practices. *MIS Quarterly*, *20*(2), 167–196. https://doi.org/10.2307/249477
Stewart, K. A., & Segars, A. H. (2002). An empirical examination of the concern for information privacy instrument. *Information Systems Research*, *13*(1), 36–49. https://doi.org/10.1287/isre.13.1.36.97
Stone, E. F., Gueutal, H. G., Gardner, D. G., & McClure, S. (1983). A field experiment comparing information-privacy values, beliefs, and attitudes across several types of organizations. *Journal of Applied Psychology*, *68*(3), 459–468. https://doi.org/10.1037/0021-9010.68.3.459
Tavani, H. T. (2007). Philosophical theories of privacy: Implications for an adequate online privacy policy. *Metaphilosophy*, *38*(1), 1–22. https://doi.org/10.1111/j.1467-9973.2006.00474.x
Visinescu, L. L., Azogu, O., Ryan, S. D., Wu, Y. A., & Kim, D. J. (2016). Better safe than sorry: A study of investigating individuals' protection of privacy in the use of storage as a cloud computing service. *International Journal of Human-computer Interaction*, *32*(11), 885–900. https://doi.org/10.1080/10447318.2016.1204838
Wang, Y., Genc, E., & Peng, G. (2020). Aiming the mobile targets in a cross-cultural context: Effects of trust, privacy concerns, and attitude. *International Journal of Human-computer Interaction*, *36*(3), 227–238. https://doi.org/10.1080/10447318.2019.1625571
Warren, S., & Brandeis, L. (1890). The right to privacy. *Harvard Law Review*, *45*(5), 193–220. https://doi.org/10.2307/1321160
Watson, D. (1988). Intraindividual and inter individual analyses of positive and negative affect: Their relation to health complains, perceived stress, and daily activities. *Journal of Personality and Social Psychology*, *54*(6), 1020–1030. https://doi.org/10.1037/0022-3514.54.6.1020
Harris and Associates Inc, Westin, A. (1998). *E-commerce and privacy: What net users want*. Privacy & American Business and PricewaterhouseCoopers.
Westin, A. F. (1967). *Privacy and Freedom*. Antheneum, NY.
Xie, W., Fowler-Dawson, A., & Tvauri, A. (2019). Revealing the relationship between rational fatalism and the online privacy paradox. *Behavior & Information Technology*, *38*(7), 742–759. https://doi.org/10.1080/0144929X.2018.1552717

About the Authors

Eric Durnell is the Social Research and Outreach Manager at Aerendir Mobile Inc. He leads a team of researchers where their primary aim is to understand how people's concerns for privacy can determine how people interact socially, particularly in an online environment.

Karynna Okabe-Miyamoto is a graduate student at the University of California, Riverside pursuing her doctorate degree in Social/Personality Psychology. She researches the science of well-being, specifically the antecedents of well-being such as social connection.

Ryan T. Howell is a Full Professor at San Francisco State University (SFSU). He is the director of The Personality and Well-being Lab at SFSU where their primary aim is to communicate to scientists and society about the motivation of purchasing habits.

Martin Zizi is the founder and CEO of Aerendir Mobile Inc. and is the inventor of the Nuero Print®, a biometric technology for authentication, identification, and encryption. He received his degree from Université Catholique de Louvain Medical School and postdoctorate at the Walter Reed Army Institute of Research.

Appendix A

Instructions: *Please take the time to read the following. It is meant for the sole purpose of passing on information about current legislation, both domestic and foreign, regarding privacy rights. It is to be considered only*

as a tool to pass on information, nothing more and nothing less. Please take the time to read ***all*** *the following information.*

The First Amendment assures particular freedoms regarding religion, expression, assembly, and the right to petition. It forbids Congress from either promoting one religion over another or restricting a person's religious practices. It further assures the freedom of expression by asserting the prohibition of Congress from restricting the press or the rights of United States citizens to speak freely. The right of citizens to assemble peaceably and to petition their government is also covered in the First Amendment.

The Fourth Amendment of the United States Constitution provides the right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures. It continues that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

The Sixth Amendment assures the rights of criminal defendants. This includes the right to a public trial without unnecessary delay, the right to a lawyer, the right to an impartial jury, and the right to know who your accusers are and the nature of the charges and evidence brought against you.

The Ninth Amendment of the United States Constitution states that there may exist rights other than those explicitly mentioned. So even though they are not listed, it does not mean that they can be violated.

The Right to be Forgotten is a concept put into practice in the European Union (EU) and Argentina since 2006. It addresses individuals' right to "determine the development of their life in an autonomous way, without being perpetually or periodically stigmatized as a consequence of a specific action performed in the past."

The Health Insurance Portability and Accountability Act (HIPPA) of 1996 created requirements for health care providers to protect the privacy and security of health information. As a result of HIPPA, on November 3, 1999, in-depth and detailed regulations were designed to protect the privacy of individually identifiable health information. [**Right to privacy of health information**]

Appendix B

Items used in Concern for Informational Privacy Scale

Items used to measure General Privacy Concern

(1) I feel that the state or condition of being free from being disturbed by other entities is important.
(2) I feel that people's right to be free from being disturbed by others should be respected.
(3) I feel that it is important to keep personally identifiable information private.
(4) I feel that it is important to keep sensitive information private.
(5) I feel that it is important to keep information that can be used to identify me as a person private.
(6) I feel that it is important to keep information that can be used to locate me private.

Items used to measure Financial Privacy Concern

(1) I feel that it is important to keep your unemployment wage(s) private.
(2) I feel that it is important to keep the income received while on medical disability private.
(3) I feel that it is important to keep your retirement income private.
(4) I feel that it is important to keep the funds you receive from a pension private.
(5) I feel that it is important to keep the wages received from worker's compensation private.
(6) I feel that it is important to keep the amount received from your social security income (SSI) private.
(7) I feel that it is important to keep the amount(s) of money received from the state government private.
(8) I feel that it is important to keep the amount(s) of money received from memberships private.
(9) I feel that it is important to keep the amount(s) of money received from a partnership private.

Items used to measure Social/Psychological Privacy Concern

(1) I make it a practice to take action at work to protect my right to maintain my personal and cultural values, such as cultural beliefs.
(2) I make it a practice to take action when it comes to protecting my personal and cultural values, such as inner thoughts.
(3) I make it a practice to take action when it comes to protecting my personal and cultural values, such as inner feelings.
(4) I make it a practice to take action when it comes to protecting my personal and cultural values, such as religious practices.
(5) I make it a practice to take action at home to protect my personal and cultural values, such as cultural beliefs.
(6) I make it a practice to take action in public to protect my personal and cultural values, such as inner thoughts.
(7) I make it a practice to take action in public to protect my personal and cultural values, such as inner feelings.
(8) I make it a practice to take action in public to protect my personal and cultural values, such as cultural beliefs.

Items used to measure Legal Privacy Concern

(1) I feel that the ability to prevent the nonconsensual disclosure of confidential information is a right for all people that were previously involved in any form of criminal litigation.
(2) I feel that the ability to prevent the nonconsensual disclosure of discrediting information is a right for all people that were previously involved in any form of criminal litigation.
(3) I feel that the prevention of nonconsensual disclosure of sensitive information is a right for all people that are currently involved in an arbitration judgment.
(4) I feel that the ability to prevent the nonconsensual disclosure of discrediting information is a right for all people that were previously involved in an arbitration judgment.
(5) I feel that the ability to prevent the nonconsensual disclosure of sensitive information is a right for all people that are currently involved in any form of civil litigation.
(6) I feel that the ability to prevent the nonconsensual disclosure of confidential information is a right for all people that are currently involved in any form of civil litigation.
(7) I feel that the ability to prevent the nonconsensual disclosure of discrediting information is a right for all people that are currently involved in any form of civil litigation.
(8) I feel that the ability to prevent the nonconsensual disclosure of sensitive information is a right for all people that are currently involved in any form of court-ordered decision(s).
(9) I feel that the ability to prevent the nonconsensual disclosure of confidential information is a right for all people that are currently involved in any form of court-ordered decision(s).

Items used to measure Technological Privacy Concern

(1) I feel that digital activities should be conducted without intrusions from corporations.
(2) I feel that all my electronic information should be protected.
(3) I believe that privacy is important when sending information using a laptop.
(4) I believe that privacy is important when sending information using a desktop.
(5) I believe that privacy is important when sending information using a tablet.
(6) I believe that my browsing history and web sites I visit should be kept private on all devices I own.
(7) I believe that my browsing history and web sites I visit should be kept private on all devices I own.

Appendix C

Final Items in CPIP (General and Facets)

CPIP: General Concern With Privacy

Please answer the following questions about yourself (1 = strongly disagree; 7 = strongly agree).

I feel that …

(1) The state or condition of being free from being disturbed by other entities is important.
(2) People's right to be free from being disturbed by others should be respected.
(3) It is important to keep personally identifiable information private.
(4) It is important to keep sensitive information private.
(5) It is important to keep information that can be used to identify me as a person private.
(6) It is important to keep information that can be used to locate me private.

CPIP: Concerns for Technological Privacy

Please answer the following questions about yourself (1 = strongly disagree; 7 = strongly agree)

I feel that …

(1) Digital activities should be conducted without intrusions from corporations.
(2) All my electronic information should be protected.
(3) Privacy is important when sending information using a laptop.
(4) Privacy is important when sending information using a desktop.

CPIP: Concerns for Financial Privacy

Please answer the following questions about yourself (1 = strongly disagree; 7 = strongly agree)

I feel that it is important to …

(1) Keep your unemployment wage(s) private.
(2) Keep the funds you receive from a pension private.
(3) Keep the amount(s) of money received from memberships private.
(4) Keep your retirement income private.

CPIP: Social Psychological Privacy Concerns

Please answer the following questions about yourself (1 = strongly disagree; 7 = strongly agree)

I make it a practice to take action …

(1) At work to protect my right to maintain my personal and cultural values, such as cultural beliefs.
(2) When it comes to protecting my personal and cultural values, such as inner feelings.
(3) In public to protect my personal and cultural values, such as inner thoughts.
(4) In public to protect my personal and cultural values, such as cultural beliefs.

CPIP: Concern for Legal Privacy

Please answer the following questions about yourself (1 = strongly disagree; 7 = strongly agree)

I feel that the ability to prevent the nonconsensual disclosure of …

(1) Sensitive information is a right for all people that are currently involved in any form of civil litigation.
(2) Confidential information is a right for all people that are currently involved in any form of civil litigation.
(3) Sensitive information is a right for all people that are currently involved in any form of court-ordered decision(s).
(4) Confidential information is a right for all people that are currently involved in any form of court-ordered decision(s).