Journal of the American Medical Informatics Association, 26(7), 2019, 610–619
doi: 10.1093/jamia/ocz010
Advance Access Publication Date: 2 April 2019
Research and Applications

Research and Applications

Disposition toward privacy and information disclosure in the context of emerging health technologies

Cynthia E Schairer,[1] Cynthia Cheung,[2] Caryn Kseniya Rubanovich,[3] Mildred Cho,[4] Lorrie Faith Cranor,[5,6] and Cinnamon S Bloss[1,2,7]

[1]Department of Psychiatry, School of Medicine, University of California, San Diego, San Diego, La Jolla, California, USA, [2]Center for Wireless and Population Health Systems, California Institute for Telecommunications and Technology, University of California, San Diego, San Diego, La Jolla, California, USA, [3]Clinical Psychology Joint Doctoral Program, San Diego State University/University of California, San Diego, San Diego, California, USA, [4]Department of Pediatrics, Center for Biomedical Ethics, Stanford University, Stanford, California, USA, [5]Institute for Software Research, School of Computer Science, Carnegie Mellon University, Pittsburgh, Pennsylvania, USA, [6]Engineering & Public Policy Department, College of Engineering, Carnegie Mellon University, Pittsburgh, Pennsylvania, USA, and [7]Department of Family Medicine and Public Health, School of Medicine, University of California, San Diego, San Diego, La Jolla, California, USA

Corresponding Author: Cinnamon S. Bloss, PhD, The Qualcomm Institute of Calit2, 9500 Gilman Drive, La Jolla, California 92093-0811, USA (cbloss@eng.ucsd.edu)

Received 16 November 2018; Revised 4 January 2019; Editorial Decision 9 January 2019; Accepted 14 January 2019

ABSTRACT

Objective: We sought to present a model of privacy disposition and its development based on qualitative research on privacy considerations in the context of emerging health technologies.
Materials and Methods: We spoke to 108 participants across 44 interviews and 9 focus groups to understand the range of ways in which individuals value (or do not value) control over their health information. Transcripts of interviews and focus groups were systematically coded and analyzed in ATLAS.ti for privacy considerations expressed by respondents.
Results: Three key findings from the qualitative data suggest a model of privacy disposition. First, participants described privacy related behavior as both contextual and habitual. Second, there are motivations for and deterrents to sharing personal information that do not fit into the analytical categories of risks and benefits. Third, philosophies of privacy, often described as attitudes toward privacy, should be classified as a subtype of motivation or deterrent.
Discussion: This qualitative analysis suggests a simple but potentially powerful conceptual model of privacy disposition, or what makes a person more or less private. Components of privacy disposition are identifiable and measurable through self-report and therefore amenable to operationalization and further quantitative inquiry.
Conclusions: We propose this model as the basis for a psychometric instrument that can be used to identify types of privacy dispositions, with potential applications in research, clinical practice, system design, and policy.

Key words: privacy, confidentiality, patient data privacy, disclosure, social values

INTRODUCTION

Information technologies for moving, copying, and storing personal information electronically are increasingly ubiquitous in American life. The associated rapid movement of personal information allows us to stay in touch with more people than ever before, facilitates the efficient purchasing and distribution of goods, saves lives through

© The Author(s) 2019. Published by Oxford University Press on behalf of the American Medical Informatics Association.
This is an Open Access article distributed under the terms of the Creative Commons Attribution-NonCommercial-NoDerivs licence (http://creativecommons.org/licenses/by-nc-nd/4.0/), which permits non-commercial reproduction and distribution of the work, in any medium, provided the original work is not altered or transformed in any way, and that the work is properly cited. For commercial re-use, please contactjournals.permissions@oup.com

more informed and timely healthcare delivery, and supports the development and testing of new innovations.[1,2] Along with these benefits, information technologies also cause disruptions and create new problems. In addition to presenting new sources of data security risks, information technologies have created, and will continue to create, new social situations in which our assumptions about privacy and confidentiality will be challenged, inevitably leading to feelings of discomfort, threat, and mistrust.[2–5] In efforts to mitigate these effects, scholars and professionals concerned with electronic data sharing have sought to understand and characterize attitudes and values of consumers and the general public.[6] The resulting literature shows how challenging it has been to develop measures that meaningfully capture attitudes toward privacy.[6,7] As the impacts of information technologies intensify and current events create more public awareness and anxiety about privacy, increasing numbers of stakeholders across disciplines and industries will find a need for tools that identify and characterize attitudes and values regarding data sharing. Here, we present a model of disposition toward privacy, or privacy disposition, focused on the context of health, healthcare, and emerging technologies in the United States. Our privacy disposition model is based on qualitative research and will serve as the basis for a quantitative psychometric instrument that measures individuals' sensitivity to disclosure of personal health information. The model has the potential to be used to develop measures for other specific contexts such as disclosure of financial information or sharing via social media.

BACKGROUND AND SIGNIFICANCE

The ambiguity of "privacy" has inspired many scholars across diverse fields to define, operationalize, or measure it. Existing scholarship on privacy addresses many facets of the concept, from privacy as a legal concept[8] to the kinds of social and psychological factors that contribute to privacy-related attitudes and behaviors.[9,10] Nissenbaum[11] suggests that disparate descriptions of privacy can be understood as a whole by considering privacy as a product of "contextual integrity" in which information flows conform to expectations and norms regarding disclosure of information. Thus, the theory of contextual integrity suggests that privacy is a feature of sociotechnical systems navigated and understood by individuals according to shared norms as well as personal expectations.[11–13]

Drawing on Nissenbaum's notion of privacy, our study was designed to identify the diversity of personal expectations and values regarding the flow of health information. Connecting this idea to the existing literature on attitudes toward privacy requires theorizing and operationalizing the concept of "private-ness" or "how private you are," colloquially treated much like a personality trait. Westin and colleagues developed one of the most well-known attempts to operationalize and measure such a concept, and between 1978 and 2004 created an index of "privacy concern" (eg, fundamentalist, pragmatist, unconcerned) based on a short questionnaire.[7,14,15] Others have suggested expanding Westin's three clusters of privacy concern into four[16] or five[17] privacy *personas*. Internet Users' Information Privacy Concerns[18] scale has emerged as a validated and widely used privacy scale, which is based on a longer questionnaire. Preibusch[6] reviewed the Internet Users' Information Privacy Concerns and about a half dozen other validity-tested privacy scales[19–24] and discussed the benefits and limitations of their use.

Many of these measures have been shown to be poor predictors of behavior,[3,25,26] pointing to a phenomenon called the "privacy paradox,"[27,28] in which reported attitudes toward privacy are found to be inconsistent with privacy-related behavior. The model of "privacy calculus" is one way that scholars have sought to make sense of the privacy paradox. Theories of privacy calculus describe behaviors related to privacy as the outcome of how individuals weigh costs and benefits of disclosing information or using privacy settings.[29] Some scholars have suggested modifications to this model, such as "privacy cynicism,"[30] "privacy fatigue,"[31] and "psychological ownership."[32] The privacy calculus approach has also been criticized for being based on an assumption of rational action that is not borne out in empirical studies.[33]

In addition to low predictive validity, these models of privacy have been limited in the extent to which they integrate context as a factor in privacy-related behaviors. Some privacy attitude scales have been adapted to refer directly to certain information-sharing scenarios[34,35] while the "privacy calculus" approach incorporates context insofar as individuals are theorized to weigh specific risks and benefits. Researchers and scholars have adapted these theories and measures of privacy attitudes and behaviors to particular technological contexts, such as self-disclosure on social media,[36–38] use of GPS-enabled apps,[39,40] and use of electronic health records.[41] These studies provide insight into individuals' attitudes and behavior in certain contexts. However, the expanding data ecosystem raises the question of how individuals conceptualize and protect information privacy across a variety of contexts.

The emergence of data-generating health technologies, such as direct-to-consumer genetic testing,[42] mobile health apps,[43] and wearable devices[44] that capture granular-level data, coupled with large-scale precision medicine initiatives, such as the *All of Us* research study,[45] further highlight the importance of understanding the intersection of privacy, emerging technologies, and health information sharing. At the same time, consumer privacy regulations, such as the European Union's General Data Protection Regulation,[46] have raised awareness and anxiety about the movement of personal information. Together, these factors create a pressing need to understand and respond to public attitudes toward sharing personal health information when deploying new data-generating health technologies. Thus, our qualitative study was designed to query individual perspectives on health information disclosure, specifically in the context of emerging health technologies. Here, we present our qualitative findings and conceptual model of privacy disposition that emerged from our analysis, which serves as the basis for a psychometric assessment tool currently in development.

MATERIALS AND METHODS

Participants of this study (1) completed either a focus group or individual interview, (2) provided demographic information, and (3) completed a companion survey comprising various measures related to health information and privacy (survey data not reported here). All recruitment procedures and study measures were reviewed and approved by the Institutional Review Board at the University of California, San Diego (protocol #160156).

Sampling

Our prior work on privacy attitudes, combined with a review of the existing privacy literature, suggested that new and changing attitudes may be developing around health privacy with regard to mobile devices, online and social media environments, genetic testing, biobanking, and other emerging health technology contexts. As such, our sampling frame was theoretically driven rather than

focused on statistical generalizability.[47] Specifically, we sought to capture a wide spectrum of experiences, expectations, and understandings of privacy.

We recruited individuals for focus groups and interviews from a number of sources to provide a broad sample for the study. These groups included several patient cohorts, including a breast health research network, an adult HIV research network, pediatric chronic disease patients from a children's hospital, and members of an online patient social network. We also recruited from community groups, including a Pacific Islander community organization, a legal advocacy organization for disadvantaged workers, a church, a charter middle school, and a leadership and academic support organization for disadvantaged adolescents. These groups were chosen because of an expectation that individuals in these cohorts would likely have had experience with these new forms of data or that they may have had specific experiences with and concerns about health privacy. For example, chronic disease patients might have specialized experience with emerging technologies such as genetic or genomic testing, members of historically underrepresented or underserved groups may have distinct concerns about disclosure of information, and school-aged adolescents are likely to have exposure to online and social media environments.

Measures

Interview and focus group protocols were developed based on results of a comprehensive review of literature on health privacy and reanalysis of data from 2 previous studies that addressed expectations about the privacy of health-related information.[2,48] Two pilot focus group sessions were conducted with undergraduate students to further refine the protocol. The final semistructured protocol probed participant attitudes about several types of health and personal information and their privacy beliefs and behaviors in relation to those types of information. While separate versions of the protocol were developed for focus groups and individual interviews, both versions covered the same topics, albeit with differences in phrasing and procedure to account for the format of administration. Example items from the protocol can be found in Supplementary Appendix 1.

Data collection

Contact information for interested individuals was provided to study investigators from site-specific cohort liaisons. Potential participants were either recruited by the site-specific cohort liaison (a nonstudy team member who contacted participants and coordinated their participation) or by a study team member for those cohorts that did not have a dedicated liaison. Our sample, therefore, comprises a series of 6 convenience samples, in which recruitment was conducted with assistance from these liaisons.

Focus groups and interviews took place between June 2016 and April 2017. Seven of 9 focus groups were conducted before the interviews to inform development of the interview guides. Two focus groups with individuals living with HIV were conducted later in the study to capture unique insights about health information privacy offered by these individuals. Focus groups were 90 minutes in length and took place at the University of California, San Diego, or a community location in San Diego County appropriate to the cohort. Focus groups were conducted by 1 of 4 facilitators. All participants provided written consent before the start of the study or signed parental consent and assent if the participant was an adolescent. All focus groups were audio and video recorded except the HIV cohorts, which were only audio recorded.

Interviews were up to 60 minutes in length and were conducted in person or over the phone by 1 of 3 interviewers. All participants provided either oral consent or written parental consent and oral assent (if the participant was an adolescent) before participation. All interviews were audio recorded.

Qualitative coding and analysis

Audio and video recordings were professionally transcribed. Transcripts were reviewed by members of the study team to ensure accuracy of the transcription and to redact any personally identifiable information.

To develop the code book, 7 independent coders were assigned to independently review 2 transcripts each (~25% of the corpus). Coders were instructed to highlight passages that suggest a privacy-influencing factor or any reason that an informant provided for making a decision about privacy. The coders collectively analyzed these factors and 27 thematic codes were identified. These codes and 8 section codes made up the codebook (Supplementary Appendix 2).

Three independent coders completed the systematic coding of the corpus according to the codebook. Each week during the coding period, 3 interviews were assigned to 2 coders who met to go over and come to consensus on the coding. This consensus coding helped to maintain consistency among coders and over time.[49] A total of 10 (19%) transcripts were consensus coded. Because coders must come to agreement in the process of consensus coding, we did not calculate intercoder reliability for these transcripts.

RESULTS

A total of 108 individuals participated across 9 focus groups and 44 interviews. The sample was predominantly female (60.2%) and participants ranged in age from 13 to 82 years old (SD = 20.0). See Table 1 for further sociodemographic characterization of the participants.

The results reported here are based on an analysis of the 10 codes most relevant to when, how, and why respondents disclose health information. These codes were named *access control*, *consequences of disclosure*, *institutional mechanisms*, *privacy practices*, *reasons to share–altruistic*, *reasons to share–personal*, *safe/unsafe*, *sensitive info–health*, *stigmatized*, and *TMI* (too much information). The working definitions of these codes are listed in Table 2. Quotes associated with these codes were further sorted according to concurrent coding with codes named interpersonal relations and institutional relations. Ultimately, we grouped the content of these codes into 4 broad categories that form the foundation of our model of privacy disposition: (1) reasons for sharing, (2) reasons against sharing, (3) interpersonal habits, and (4) institutional habits.

Contextual disclosure habits

The categories we named interpersonal habits and institutional habits include reported behavior, practices, or rules of thumb for when and how to share personal health information. Interpersonal habits encompasses the ways in which people share information with people they know personally or encounter in person. Some interpersonal habits were mentioned in the context of a conversation about what it means to be "a private person" and therefore directly reflected perceptions of "private-ness" as a personality characteristic. For example, one man described himself as "not private" because, he said, "I'm more about trying to address [an issue] than hide it or be ashamed of it or whatever. I'm pretty much an open

Table 1. Sample demographics (N = 108)

Participation type	
Focus group	64 (59.3)
Interview	44 (40.7)
Female	65 (60.2)
Age, y	40.35 ± 20.0 (13-82)
Hispanic/Latino[a]	28 (26.2)
Race[b]	
American Indian/Alaska Native	3 (3.2)
Asian	10 (10.6)
Black or African American	8 (8.5)
Native Hawaiian or Other Pacific Islander	8 (8.5)
White	63 (67.0)
Mixed/more than 1 race	2 (2.1)
Marital status[a]	
Single	62 (57.9)
Married/in a domestic partnership	36 (33.6)
Divorced/widowed	9 (8.1)
Highest education[a]	
Completed 11 or fewer years (majority adolescents still in school)	29 (27.1)
Graduated from high school or GED completed	12 (11.2)
Graduated from 2-year college	13 (12.1)
Graduated from 4-year college	21 (19.6)
Some postcollege education	11 (10.3)
Master's degree	17 (15.9)
Professional degree or PhD	4 (3.7)
Approximate annual household income[c]	
Under $25 000	28 (29.2)
$25 000-$49 999	20 (20.8)
$50 000-$99 999	22 (22.9)
$100 000-$149 999	12 (12.5)
$150 000+	14 (14.5)
Self-reported health status	
Very good	24 (22.2)
Good	52 (48.1)
Average	26 (24.1)
Poor	6 (5.6)
Very Poor	0 (0.0)

Values are n (%) or mean ± SD (range).
[a]Missing data for 1 participant.
[b]Missing data for 14 participants.
[c]Missing data for 12 participants.

book" (CG-003). In contrast, another interviewee described herself as private, explaining, "I just tend not to share everything personal with a lot of people. I keep things to myself" (CG-004). Other interpersonal habits were specific statements about how and when respondents communicated health information with other individuals. For example, one man stated, "It's right in my [dating] profile, I've been [HIV] positive for 36 years. That's my health information," (FG-P4). Another kind of response focused on who the respondent did or did not share information with, like the woman who reported, "Nobody around me knows what's going on with my health, just my mom" (CG-048).

Institutional habits include reported behavior, practices, or rules of thumb used in situations in which disclosed information may be recorded and used by institutions. For example, one patient group member told us, "I have no compunctions about either withholding information, or just flat out lying, because [insurance agents] will misuse the information if I give it to them" (PT-028). Some of these practices were specific to medical information. For example, one respondent who was highly familiar with biobanking described the information she has asked for before donating blood for research, commenting, "Deidentification is very important, number one, I think. I would like to know how long the sample's going to be stored, who has access to the sample, actually even how it's going to be stored. Is it whole blood or [are] they thinning down or getting plasma, all that stuff." (PT-023) However, many behaviors mentioned were examples of cautionary steps taken with digital data in general, such as the man who reported, "I'm very conscious about turning location off, not just on my devices, but different members of my family, their devices" (PT-051). Table 3 presents a list of specific behaviors we collected from comments like these.

Some respondents who described themselves as "very private" in interpersonal contexts also reported conservative or closed habits with respect to disclosing information in institutional settings. However, self-description as "private" or "not so private" did not always match the behaviors they reported in institutional contexts, which was not necessarily a contradiction. For example, when asked if he thought of himself as a private person, one respondent said, "Not really [. . .because] I'm social. People know about me and everything. I'm not scared to know what people know about me" (PT-025). Yet, he also reported keeping his Facebook account private and sometimes reading the terms and conditions for apps. In contrast, a mother of a chronically ill child described herself as private and reported cautious privacy practices in most settings, except when it came to sharing medical information about her child, commenting, "We really wouldn't [share his medical information] if we had a choice, but because we're in this circumstance, we're giving up a little bit of risk to hopefully benefit at the end of it" (PT-050). These examples suggest that, for some individuals, interpersonal and institutional information habits can vary independently.

Reasons for and against sharing

When discussing decisions about when and how to disclose personal information, respondents referred to not only familiar benefits and risks or adverse consequences, but also ideas about privacy, emotional responses, and other motivations and deterrents. For example, respondents did not necessarily connect annoyance with personalized online advertisements with a direct threat to privacy, but this annoyance was noted as a deterrent to sharing. Conversely, benefits of sharing, such as helping others with similar conditions, did not need to be direct or guaranteed to be mentioned several times as reasons to disclose health information. Conceptualizing benefits as "reasons to share" in our coding process helped us to attend to a more inclusive set of motivations whether or not they were easily understood as benefits. As we sorted through the many deterrents coded with *access control*, *consequences of disclosure*, *safe/unsafe*, *stigmatized*, and *TMI*, we saw that the same logic could be applied. Therefore, we included a wide selection of reasons for sharing and reasons against sharing in our lists (outlined in Table 4), encompassing: (1) reasons conventionally described as "risks and benefits" that have clear and generally agreed-upon impacts on the individual, (2) feelings and subjective experiences that impact decisions about disclosure, and (3) philosophies of privacy that imply support for sharing or reticence. The types of reasons we collected reflect the emphasis in our interview guide on disclosure of health information.

The ways in which respondents spoke about their reasons for sharing and reasons against sharing suggest an intuitive shorthand for characterizing contexts as private or not private in the face of uncertainty. We have come to think of this as a sort of privacy essentialism in which individuals appear to settle on static understandings

Table 2. Names and definitions of codes selected for incorporation into privacy disposition model

Thematic Code Name	Definition
Access control	Discussion of control over access to and content of electronic data. Includes discussion of who should or should not have access or the ability to change the content.
Consequences of disclosure	Discussion of potential negative outcomes of data sharing on self or others.
Institutional mechanisms	Discussion about regulations/infrastructure/policies/laws that exist to protect personal information and respondent's level of confidence in regulations or institutions. May be positive, negative, or neutral on the topic of whether such checks and balances are adequate. Include discussion of informed consent and de-identification procedures.
Institutional relations	Discussion of privacy and information sharing in the context of relationships with a company (for profit or nonprofit), health system, university, research institution, biobank, government, or other institutional entity. Include entities' motivations or willingness to protect privacy.
Interpersonal relations	Discussions of privacy or information sharing in the context of relationships with people (eg, friends, relatives, acquaintances, strangers).
Privacy practices	Discussion of intentional actions taken to protect privacy (eg, using privacy settings, private browsing, reading privacy statements, shredding documents, avoiding email for certain purposes, limits on what type of information is posted).
Reasons to share–personal	Discussion of personal benefits of sharing information. May include perceived or actual personal benefit (eg, to get better care, find others like me, learn more information).
Reasons to share–altruistic	Discussion of societal benefits of sharing information (altruistic or for a greater good). May include perceived or actual societal benefit (eg, contribute to better knowledge, help others, help my community).
Safe/unsafe	Discussions of feeling vulnerable or protected with respect to the movement of personal information.
Sensitive info–health	Discussions of health information and if it is sensitive relative to other types of information (eg, respondent may or may not feel health information is sensitive—need to capture discussions either way).
Stigmatized	Discussion about sharing or protecting potentially stigmatizing/ embarrassing information. Respondent must point to the stigmatizing potential of the information—coder should not infer. Includes acknowledgement of others' attitude toward this type of information, even if respondent does not agree.
TMI	Discussions about when too much electronic information is collected or requested.

TMI: too much information.

Table 3. Contextual disclosure habits

	Interpersonal Habits	Institutional Habits
Definition:	Behaviors, practices, or personal codes related to sharing or protecting information within interpersonal relationships	Behaviors, practices, or personal codes related to sharing or protecting information in institutional settings
Examples:	• Open with coworkers or acquaintances • Open with potential romantic partners • Open with people who see me (because I look sick) • Open with people who have conditions like mine • Talk about health with people who are seeking information • Talk about health only when it comes up in conversation • Talk about health only with people I trust • Disclose only select information with friends and family • Disclose only on a "need to know" basis • Lie to my friends about my chronic disease • Tell only my mom about my health • Discuss my health only with my doctor • More open with people online than in-person • Discuss condition with others (eg, friends) when it's serious or I know exactly what's going on	• Read terms and conditions or privacy policies • Lie or obfuscate information • Do not disclose health information with companies • Ask about how research information will be stored • Ask what research information is for • Deal only with credible health and research institutions • Bring physical copies of health records rather than sending electronically • Avoid certain search terms or posting about certain topics when online • Avoid online shopping or online banking • Avoid clicking on online ads • Clear online browsing history • Avoid disclosing sensitive information online • Disable features on apps • Delete apps that ask for too many permissions • Disable smartphone GPS

of circumstances as private or not private. For example, discussions about risks and consequences of disclosure often revolved around assumptions, generalized impressions, or secondhand stories that made no definitive statement about the likelihood of a bad outcome. One interviewee shared her general impression: "If my name's on it, it just feels like that information can be abused and then I directly take the hit for it, in some regard" (CG-058). Concerns about discrimination in insurance coverage were sometimes illustrated with stories like this one, offered by one focus group participant:

> I actually know a lot of younger people in their 20s and 30s who have a family history of polycystic kidney disease or whatever, and their parents have taken them to Mexico to be tested because they didn't want it in a database here in the US to basically tank their chances for insurance, for life insurance. I think you

Table 4. Reasons for and against sharing inclusive of benefits and risks, philosophies of privacy, and emotional factors

	Reasons for Sharing	Reasons Against Sharing
Conventional	• Receive better medical care • Gain or maintain employment • Gain or maintain insurance • Convenience • Receive social support • Legal requirement	• Avoid discrimination or loss of benefits • Avoid stigma or being treated differently • Prevent tracking, targeting, or information "used against me"
Emotional/Intangible	• Belief in research • Desire to help others • Feelings of safety (trust or familiarity; belief in anonymity, good information security and rules/regulations; sense of control) • Desire to demonstrate trustworthiness or other socially desirable trait • Desire to take a stand or "change the culture" • Build community	• Concerns about unspecified unintended consequences • Negative past experiences • High value on control of personal information • Negative or uncomfortable feeling when asked for too much or inappropriate information • Lack of trust in the commercial, political, or disrespectful motives of others • Protect others from worry or sadness • Uncertainty in what could happen with information • Fear of hacking
Philosophies of Privacy	• Conviction that privacy does not exist or cannot be maintained (fatalism) • Willingness to trade privacy for other benefits (tradeoff) • Assumption that privacy is not necessary if one has no secrets (nothing to hide)	• Conviction that privacy is a kind of human right or property right (moral right) • Conviction that maintaining privacy is an individual's responsibility (personal responsibility) • Assumption that privacy is necessary because the individual has a secret (something to hide)

> have to think about where that information is and what the end result could be when you decide to let people have access to it. (FG-P1)

This respondent demonstrates that the fears of her younger acquaintances resonate with her, first by making a very specific story sound like a notable trend in her social circle ("I know a lot of people who…") and then by concluding with a generalized moral about sharing information ("You have to think…"). At the same time, she does not address the issue of whether her friends' fears were well-founded. Indeed, her conclusion accounts for the difficulty of assessing risk—"you have to think about it"—but there is no clear action indicated one way or the other. Even firsthand stories about the consequences of disclosing information could be dominated by uncertainty. An interviewee discussed her experience of solicitations she suspects originated from her openness about her health online.

> But, I also know that I'm getting a lot of solicitations about do I want to try this drug? … stuff I've never heard of. Stuff that really did sound like "Acme" testing. I get a ton of stuff from Survey Monkey that I don't know. Sometimes I look at it and say, "Why would you even choose me?" It makes me think because of one little thing that I wrote or checked. (PT-018)

This respondent expresses her discomfort, but also does not have clear knowledge of what behavior allowed her information to be disclosed. Throughout the interview, she used the name "Acme" to denote a questionable or nonreputable institution. An experience like the one described previously could easily inspire a personal rule of thumb to never share health-related information via the internet, whether or not solicitation could be shown to be an outcome of such action. Another respondent expressed just such a conviction when he said, "If I don't know for a fact that I can trust them [companies that collect my information], then I'm going to think twice before I give them anything more" (PT-028).

Respondents discussed experiences as well as feelings (of trust and safety or mistrust and vulnerability) that might be overlooked by a narrow focus on risks and benefits. Discussions about personalized ads or communicating with insurance companies, for example, often brought up negative feelings, such as, "I don't like that. I feel like someone is watching me and watching what I'm doing" (PT-031), or, "I feel somewhat threatened, and I feel very adversarial with insurance companies. The less information they have, the better" (PT-047). This last respondent referred to her experience of suing her insurance company for coverage. Her comment reflects how emotional responses to previous experiences can strongly influence behavior in future encounters. A similar dynamic is clear in this woman's story: "I decided to join their [Starbuck's] WiFi, and I got hacked into. It only took the one experience for me to say, 'Enough, no more'" (PT-009). This respondent describes a common emotional reaction to a negative experience that cannot be accounted for in a privacy calculus that weighs risks and benefits.

Similarly, many respondents described motivations to share information that did not involve direct benefits to themselves, but the potential to help others or society in general. Many of these responses addressed research specifically, such as, "I would hope that the information that I would provide would help others" (PT-010), "I think I'm doing good for hopefully the future generations" (FG-P3), or "I'm really for research. Otherwise, I wouldn't do this. I really believe in research" (PT-012). Some respondents saw being open about their health information as a political act, for example, "I want the culture around this conversation to change and I need to be a part of making that change" (CG-052). Others saw sharing as a way to reach out to others in similar circumstances: "I guess if I am trying to encourage someone else who has come down with some horrible disease and they're not sure what the net result is going to be, I will mention my situation, [and that] things have turned out positively" (PT-014).

Table 5. Definitions of philosophies of privacy

Philosophies of Privacy	Definition
Fatalism	Privacy cannot be controlled or does not exist.
Moral right	Privacy is a moral right—something that everyone is entitled to.
Nothing to hide	Protection of personal information is unimportant as long as the information does not include something sensitive or stigmatizing.
Something to hide	Protection of personal information is important because that information includes something that is sensitive or stigmatizing.
Personal responsibility	Privacy is a personal responsibility; everyone must work to keep or have privacy if they want it.
Tradeoff	Privacy is something to be traded for desired goods, services, or conveniences and reflects a risk/reward or other tradeoff.

Philosophies of privacy

A set of common ideas about "what privacy is" have been discussed in the literature on privacy behaviors and attitudes. When preparing the codebook, we included codes to capture expressions of several common philosophies of privacy. Table 5 presents the names and definitions for those that were represented in the transcripts. These philosophies represent cultural framings[50] or shared definitions of privacy. Our analysis shows how these ideas were discussed as generalized approaches to disclosure, similar to other reasons for and against sharing.

Philosophies of privacy coded as fatalism, tradeoff, or nothing to hide can function as reasons for sharing because they justify disclosure, as in "total privacy doesn't exist" (FG-C5) or "as long as the app serves its purpose for me, I guess I'm okay with it" (PT-027) or "what are they going to use it for? I have nothing to hide" (CG-055). Privacy philosophies like moral right, personal responsibility, or something to hide discourage disclosure because they imply a higher personal value for privacy. When privacy is considered a moral right, it is elevated to something nearly sacred. As one respondent put it, "You really only have a few things in life. Privacy and integrity are 2 of them that I find to be important to me" (FG-P3). The personal responsibility philosophy implies that individuals must work to maintain privacy if they want it, as in, "In this day and age I think you have to be a little bit more cautious and private" (PT-011), or, "If you just throw around information and other stuff like that just willy nilly, then you're not going to keep your privacy" (PT-015). An extreme reading of personal responsibility may even imply that disclosing information is a breach of duty or a character flaw. Moreover, those who value their privacy because they feel they have something to hide might be less willing to disclose anything, or perhaps be more selective about the information they disclose. For example, one respondent told us she does not mind sharing her age because she is proud of it, but "weight is another problem. I'm overweight, so I don't like to share that" (PT-012). If an individual worries about information that they feel must be hidden, they may be more cautious when sharing information in general.

Participants in our study did not always discuss philosophies of privacy, and when they did mention them, these were both expressions of beliefs held by the speaker or by others. For example, one woman attributed a fatalist attitude to her kids and grandkids: "To them, it's a matter of fact. I hear all the time, 'Gram, don't worry about it.' 'Ma? It's all right. Don't worry about it.' 'Don't lose sleep over it. It just happens'" (PT-022). Like reasons attributed to others, secondhand expressions of these philosophies inform our understanding even when they cannot be attributed to our study participants.

DISCUSSION

Here, we report results from a qualitative study designed to guide development of a psychometric instrument to assess individual differences in sensitivity toward disclosure of personal health information. This study yielded 3 key insights that gave shape to a conceptual model of privacy disposition on which our instrument will be based. These insights are the following:

1. **Privacy-related behavior is both contextual and habitual**. Interviewees described varying sensitivities and distinct privacy-related behaviors across institutional and interpersonal contexts. Interviewees described habitual repetition of these behaviors within each context. Many empirical studies of privacy focus on particular technological contexts, such as social media or mobile app use.[40,51,52] We asked our respondents about their practices and habits in interpersonal contexts as well as a broad range of technological and biomedical contexts, for example, with respect to electronic health records (EHRs), biobanking, and fitness trackers. Therefore, we included habits specific to interpersonal and institutional relationships as important and distinct influences on privacy disposition.
2. **Motivations and deterrents extend beyond risks and benefits**. The reasons interviewees gave for their privacy-related behaviors encompassed more than conventional assessment of risks and benefits. Where the "privacy calculus" approach focuses on risks and benefits of information disclosure,[29] we broaden the scope to reasons for sharing and reasons against sharing to better capture the many considerations that we heard about in our interviews and focus groups. These considerations included not only consequences and benefits, but also feelings—including feelings of trust (encompassing features such as reliability, competence, or integrity), experiences, preferences, and privacy philosophies.
3. **Philosophies of privacy should be classified as motivations or deterrents**. Philosophies of privacy are one type of reasons for or against sharing that interviewees gave for privacy-related behaviors. Existing approaches that focus on privacy attitudes focus on and prioritize identifying an individual's philosophy of privacy, such as privacy as a property right (eg, psychological ownership)[31]; privacy as moral right (eg, privacy fundamentalism)[15]; or privacy as no longer existing (eg, privacy cynicism).[29] Our analysis helped us to see these philosophies as a special class of reasons for or against sharing that may not be held by all individuals. In addition, these qualitative data suggest that an individual may express contradictory privacy philosophies and may even do so simultaneously. The meaning of such contradictions is unclear, although examination of other reasons for or against sharing may offer clarifying insights. Therefore, we incorporate privacy philosophies into the category of reasons alongside risks, benefits, and subjective experiences—without elevating any above the others.

The qualitative analysis presented here suggests a simple but potentially powerful conceptual model of privacy disposition, or what makes a more or less private person. This model describes privacy

disposition as a function of the 4 categories of influences that we have described: institutional habits, interpersonal habits, reasons for sharing, and reasons against sharing. Including contextualized habits helps account for 2 distinct arenas associated with information privacy. Using the broad categories of reasons for sharing and reasons against sharing builds on existing models that describe concerns or attitudes toward privacy and the risks and benefits of disclosure as the main antecedents to privacy-related behaviors. Bringing all such considerations under the umbrella of reasons allows us to include in our model the range of motivations and deterrents described by interviewees without prioritizing them a priori. Future quantitative work may help determine what features are most indicative of privacy disposition.

This model is specifically designed to describe the factors related to an individual's general comfort with disclosure of personal health information vs an all-encompassing model of the broad construct of privacy. Nissenbaum[11] described privacy as "contextual integrity": Where expectations and norms of information flow are not violated, there is a sense of privacy.[53] Our model might be seen as nested within Nissenbaum's description, as a way of identifying, and eventually anticipating, the expectations and values most significant to a given individual. Although the term *disposition* may imply something that is fixed or preexisting, privacy disposition need not be conceptualized as an enduring personality trait. Indeed, it would require empirical study to understand how the factors of habits and reasons may shift over a lifetime or according to circumstance. However, we hypothesize that privacy disposition is stable enough to be useful and meaningful within some sets of defined circumstances (eg, with respect to biomedical information). Should future work find that this latent construct is less stable than expected, other language to describe it may be warranted (eg, use of the label privacy perspective vs privacy disposition).

Limitations

This model is grounded in careful and systematic qualitative analysis, but our method does have important limitations. First, the participants we spoke to are not representative of the general population, though we did work to speak to many different groups of people who might have particular views of privacy and disclosure of personal health data. The questions we asked of our respondents focused on 2 main contexts—general online sharing and where health data are disclosed. As with any qualitative data, this study does not allow us to know the prevalence of the thoughts, ideas, and concerns we observed in our data. However, this is the first phase of a mixed-methods project. We seek to develop a psychometrically sound instrument, through which we will be able to test both the prevalence of similar sentiments and the reliability and validity of our model.

CONCLUSION

We have suggested a conceptual model of privacy disposition based on 3 insights that emerged from a qualitative study of how people discuss attitudes and behaviors related to the disclosure of health information. First, privacy-related behavior is both contextual and habitual, implying that current disclosure decisions will likely resemble previous disclosure decisions in a given context. However, behavior is not necessarily consistent from one context to another. Second, when people make decisions about information disclosure, they are influenced by a range of motivations and deterrents that may include risks and benefits but are often also based on subjective experiences. Finally, privacy philosophies—ideas about "what privacy is"—can also be motivations or deterrents that influence privacy decisions. We have presented the qualitative data that prompted these insights and used these data to illustrate the concept of privacy disposition as a function of interpersonal habits, institutional habits, reasons for sharing, and reasons against sharing.

We believe this model of privacy disposition has the potential to inform applications and interventions in medical decision making, research design, informed consent processes, and policy. If individuals' privacy dispositions can be identified this could serve as a useful tool in developing more "user-centered" recruitment strategies, procedures, communication tools, or informed consent processes for research. For example, one could imagine this model forming the basis of a tailored decision aid for use in research or even clinical decision making where privacy-related issues are at stake. In the clinic, providers could use privacy disposition to anticipate and address points of concern surrounding EHRs or information flows in hospitals and clinics. If the rates of different types of privacy disposition can be identified within populations, it could help identify ways to improve the design of data-use policies to be more user-centered and responsive to privacy-related expectations and values. It may also be possible to identify privacy concerns and values that are not currently addressed in research and healthcare settings.

The model of privacy disposition has the potential to be applied more generally to how individuals approach disclosure of personal data beyond the context of medicine and health. Many of the topics and themes identified here are related to an individual's history and demeanor toward privacy, such as generalized concerns about information flows, privacy philosophies, or habits pertaining to mobile app use. Therefore, while the instrument we are currently developing pertains to the disclosure of personal health information, future work could use this model of privacy disposition to understand patterns and expectations for disclosure of other types of information.

FUNDING

This work was supported by the National Human Genome Research Institute "Impact of Privacy Environments for Personal Health Data on Patients" (PI: Bloss, R01 HG008753, 2015-2018).

AUTHOR CONTRIBUTIONS

CS conducted data analysis and interpretation, drafted the manuscript, and revised the manuscript for important intellectual content. CC contributed to data collection as well as data analysis and interpretation, drafted parts of the manuscript, and revised the manuscript for important intellectual content. CKR contributed to data analysis and interpretation, and revised the manuscript for important intellectual content. MC and LFC revised the manuscript for important intellectual content. CB designed the study, oversaw data collection and analysis, contributed to data interpretation, and revised the manuscript for important intellectual content.

ACKNOWLEDGMENTS

The authors thank the patients who shared their experiences and generously gave their time to participate in this research. The authors also thank Elizabeth Heitman and Aaron Levine for their constructive and thorough feedback on a draft of this manuscript. Finally, the authors thank Dr Matthew Bietz, Dr Camille Nebeker, Lindsay Dillon, and Beatriz Valenzuela-Guzman for

providing administrative assistance and/or for facilitating focus groups and interviews.

CONFLICT OF INTEREST STATEMENT

None declared.

REFERENCES

1. Steinhubl SR, Muse ED, Topol EJ. Can mobile health technologies transform health care? *JAMA* 2013; 310 (22): 2395–6.
2. Bietz M, Bloss C, Calvert S, *et al*. Opportunities and challenges in the use of personal health data for health research. *J Am Med Inform Assoc* 2016; 23 (E1): E42–8.
3. Bandara R, Fernando M, Akter S. Is the privacy paradox a matter of psychological distance? An exploratory study of the privacy paradox from a construal level theory perspective. In: *Innovative Behavioral IS Security and Privacy Research*. Hilton Waikoloa Village, HI; 2018.
4. Rothstein MA, Wilbanks JT, Brothers KB. Citizen Science on your smartphone: an elsi research agenda. *J Law Med Ethics* 2015; 43 (4): 897–903.
5. Schairer CE, Rubanovich CK, Bloss CS. How could commercial terms of use and privacy policies undermine informed consent in the age of mobile health? *AMA J Ethics* 2018; 20 (9): 864–72.
6. Preibusch S. Guide to measuring privacy concern: review of survey and observational instruments. *Int J Hum-Comput Stud* 2013; 71 (12): 1133–43.
7. Kumaraguru P, Cranor LF. *Privacy Indexes: A Survey of Westin's Studies*. Pittsburgh, PA: Carnegie Mellon University; 2005.
8. Warren SD, Brandeis LD. The right to privacy. *Harvard Law Review* 1890; 4 (5): 193–220.
9. Heravi A, Mubarak S, Raymond Choo K-K. Information privacy in online social networks: uses and gratification perspective. *Comput Hum Behav* 2018; 84: 441–59.
10. Wirth J. Strength of ties as an antecedent of privacy concerns: a qualitative research study. In: *Information Systems Security and Privacy*. Boston, MA; 2017.
11. Nissenbaum H. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford, CA: Stanford University Press; 2010.
12. Ochs C, Ilyes P. Sociotechnical privacy. Mapping the research landscape. *TECNOSCIENZA: Ital J Sci Technol Stud* 2014; 4 (2): 73–92.
13. Park YJ, Chung JE. Health privacy as sociotechnical capital. *Comput Hum Behav* 2017; 76: 227–36.
14. Westin A. *Privacy on & Off the Internet: What Consumers Want*. Hackensack, NJ: Technical Report for Privacy & American Business; 2001.
15. Westin A. Equifax-Harris Consumer Privacy Survey. Atlanta/New York: Equifax/Harris; 1996.
16. Berendt B, Günther O, Spiekermann S. Privacy in e-commerce: stated preferences vs. actual behavior. *Commun ACM* 2005; 48 (4): 101–6.
17. Dupree JL, Devries R, Berry DM, *et al*. Privacy personas: clustering users via attitudes and behaviors toward security practices. In*: Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, 2016: 5228–39.
18. 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 (4): 336–55.
19. Smith HJ, Milberg SJ, Burke SJ. Information privacy: measuring individuals' concerns about organizational practices. *MIS Q* 1996; 20 (2): 167–96.
20. Sheehan KB, Hoy MG. Dimensions of privacy concern among online consumers. *J Publ Pol Market* 2000; 19 (1): 62–73.
21. Buchanan T, Paine C, Joinson AN, *et al*. Development of measures of online privacy concern and protection for use on the internet. *J Am Soc Inf Sci* 2007; 58 (2): 157–65.
22. Earp JB, Antón AI, Aiman-Smith L, *et al*. Examining internet privacy policies within the context of user privacy values. *IEEE Trans Eng Manage* 2005; 52 (2): 227–37.
23. Dinev T, Hart P. Internet privacy concerns and their antecedents-measurement validity and a regression model. *Behav Inf Technol* 2004; 23 (6): 413–22.
24. Braunstein A, Granka L, Staddon J. Indirect content privacy surveys: measuring privacy without asking about it. In: *Proceedings of the Seventh Symposium on Usable Privacy and Security*, 2011: 15.
25. Awad NF, Krishnan MS. The personalization privacy paradox: an empirical evaluation of information transparency and the willingness to be profiled online for personalization. *MIS Q* 2006; 30: 13–28.
26. Mosteller J, Poddar A. To share and protect: using regulatory focus theory to examine the privacy paradox of consumers' social media engagement and online privacy protection behaviors. *J Interact Market* 2017; 39: 27–38.
27. Norberg PA, Horne DR, Horne DA. The privacy paradox: personal information disclosure intentions versus behaviors. *J Consum Affairs* 2007; 41 (1): 100–26.
28. Spiekermann S, Grossklags J, Berendt B. E-privacy in 2nd generation e-commerce: privacy preferences versus actual behavior. In: *Proceedings of the 3rd ACM Conference on Electronic Commerce*, 2001: 38–47.
29. Culnan MJ, Armstrong PK. Information privacy concerns, procedural fairness, and impersonal trust: an empirical investigation. *Organ Sci* 1999; 10 (1): 104–15.
30. Hoffmann CP, Lutz C, Ranzini G. Privacy cynicism: a new approach to the privacy paradox. *Cyberpsychol J Psychosoc Res Cyberspace* 2016; 10 (4): 7.
31. Choi H, Park J, Jung Y. The role of privacy fatigue in online privacy behavior. *Comput Hum Behav* 2018; 81: 42–51.
32. Cichy P, Salge TO, Kohli R. Extending the privacy calculus: the role of psychological ownership. In: ICIS 2014 Proceedings; December 15, 2014; Auckland, New Zealand.
33. Acquisti A. Privacy in electronic commerce and the economics of immediate gratification. In: *Proceedings of the 5th ACM Conference on Electronic Commerce*, 2004: 21–9.
34. Elhai JD, Chai S, Amialchuk A, *et al*. Cross-cultural and gender associations with anxiety about electronic data hacking. *Comput Hum Behav* 2017; 70: 161–7.
35. Torabi S, Beznosov K. Sharing health information on facebook: practices, preferences, and risk perceptions of North American users. In: *Symposium on Usable Privacy and Security (SOUPS)*, 2016.
36. Osatuyi B, Passerini K, Ravarini A, *et al*. Fool me once, shame on you… then, i learn." an examination of information disclosure in social networking sites. *Comput Hum Behav* 2018; 83: 73–86.
37. van Schaik P, Jansen J, Onibokun J, *et al*. Security and privacy in online social networking: risk perceptions and precautionary behaviour. *Comput Hum Behav* 2018; 78: 283–97.
38. Acquisti A, Gross R. Imagined communities: awareness, information sharing, and privacy on the Facebook. In: *International Workshop on Privacy Enhancing Technologies*, 2006: 36–58.
39. Ketelaar PE, van Balen M. The smartphone as your follower: the role of smartphone literacy in the relation between privacy concerns, attitude and behaviour towards phone-embedded tracking. *Comput Hum Behav* 2018; 78: 174–82.
40. Poikela M, Kaiser F. 'It is a topic that confuses me'–Privacy perceptions in usage of location-based applications. In: European Workshop on Usable Security (EuroUSEC); February 21–24, 2016; San Diego, CA.
41. Rahim FA, Ismail Z, Samy GN. A review on influential factors of information privacy concerns in the use of electronic medical records. *Int J Comput Sci Inform Secur* 2016; 14 (7): 17.
42. Regalado A. 2017 Was the year consumer DNA testing blew up. 2018. https://www.technologyreview.com/s/610233/2017-was-the-year-consumer-dna-testing-blew-up/. Accessed June 1, 2018.
43. Ernsting C, Dombrowski SU, Oedekoven M, *et al*. Using smartphones and health apps to change and manage health behaviors: a population-based survey. *J Med Internet Res* 2017; 19 (4): 1.
44. Piwek L, Ellis DA, Andrews S, *et al*. The rise of consumer health wearables: promises and barriers. *PLoS Med* 2016; 13 (2): e1001953.

45. PMI Working Group. *The Precision Medicine Initiative Cohort Program—Building a Research Foundation for 21st Century Medicine*. Bethesda, MD: National Institutes of Health; 2015.
46. EUGDPR.org. GDPR key changes: an overview of the main changes under gdpr and how they differ from the previous directive. https://www.eugdpr.org/key-changes.html. Accessed February 23, 2018.
47. Breckenridge J, Jones D. Demystifying theoretical sampling in grounded theory research. *Grounded Theory Rev* 2009; 8 (2): 113–26.
48. Cheung C, Bietz MJ, Patrick K, *et al*. Privacy attitudes among early adopters of emerging health technologies. *Plos One* 2016; 11 (11): e0166389.
49. Sankar P, Jones NL. Semi-structured interviews in bioethics research. In: Empirical Methods for Bioethics: A Primer. Bingley, UK Emerald Group; 2007: 117–36.
50. Goffman E. *Frame Analysis: An Essay on the Organization of Experience*. Cambridge, MA: Harvard University Press; 1974.
51. Keith MJ, Babb J, Lowry PB. A longitudinal study of information privacy on mobile devices. In: *47th Hawaiian International Conference on Systems Sciences (HICSS 2014)*; January 6–9, 2014; Big Island, HI.
52. Young R, Willis E, Cameron G, *et al*. "Willing but unwilling": attitudinal barriers to adoption of home-based health information technology among older adults. *Health Informatics J* 2014; 20 (2): 127–35.
53. Nissenbaum H. A contextual approach to privacy online. *Daedalus* 2011; 140 (4): 32–48.