Open Access

OBM Genetics

Research Article

"Not Private at All:" Comparative Perspectives on Privacy of Genomic Data, Family History Data, Health-Related Data, and Other Personal Data

Nora B. Henrikson [1, 2, *], Paula R. Blasi [1], Marlaine Figueroa Gray [1], Lorella Palazzo [1], Aaron Scrol [1], Stephanie M. Fullerton [3]

1. Kaiser Permanente Washington Health Research Institute, Seattle WA, USA; E-Mails: nora.b.henrikson@kp.org; paula.r.blasi@kp.org; marlaine.s.figueroagray@kp.org; lorella.g.palazzo@kp.org; aaron.scrol@kp.org
2. University of Washington School of Public Health, Institute for Public Health Genetics, Seattle WA, USA; E-Mails: nhenriks@uw.edu
3. University of Washington School of Medicine, Department of Bioethics and Humanities, Seattle WA, USA; E-Mails: smfllrtn@uw.edu

* **Correspondence:** Nora B. Henrikson; E-Mails: nora.b.henrikson@kp.org; nhenriks@uw.edu

Academic Editor: Anne-Marie Laberge

Special Issue: Use of Genetic Tests in the Context of Population Screening Strategies

OBM Genetics
2022, volume 6, issue 4
doi:10.21926/obm.genet.2204167

Received: August 09, 2022
Accepted: October 23, 2022
Published: October 31, 2022

Abstract

People choose how and if to generate and disclose not just personal genomic data, but also multiple other types of personal health and non-health related data. To contextualize choices about genetic testing and genetic data disclosure, we explored perspectives of genomic data privacy and disclosure compared to other types of data. We conducted a qualitative focus group study with adult members of an integrated U.S. health system, using administrative data to stratify our sample by age and by race/ethnicity. Discussion topics included qualities, rights, benefits and harms of disclosure of genomic, health, family history and non-health related data. We conducted thematic template analysis using verbatim transcripts. The sample (n = 24) was 67% female, mean age 54.1 years (range 23-88), and 37% people of color; 71% reported college degree. Participants considered genetic data, but not other data types,

as a permanent, core part of the individual self and as protected health information under current laws. Participants did not feel that individuals had a right to family medical history disclosure from their relatives. Participants assumed high levels of privacy protections of genetic and other health-related data, but no perceived privacy or protection around other personal data. Participants weighed benefits and risks of generation and disclosure of all data types; harms were more far-reaching for non-health data, possibly related to the perceived lack of protections around these data. People make privacy-related choices about genetic testing in the context of related considerations for multiple types of data and rely on perceived privacy protections under current U.S. health privacy laws. Genetic research and screening programs should consider providing clear guidance on privacy protections afforded to genetic information in U.S. clinical settings. Future research should examine connections between privacy-related views on genetic and multiple other types of personal data.

Keywords
Health data; genetic data; genetic testing; genetic research; privacy; Protected Health Information; HIPAA; qualitative; patient perspectives

1. Introduction

Genomic data are increasingly available, and with it, increasing chances of privacy erosion as potential for identification increases [1-5]. An individual's views about privacy – one's ability to control the use and sharing of one's personal data - may influence their choices to participate in genetic research or population-based genetic screening programs [3, 6, 7]. At the same time as the clinical use of personal genetic data rapidly increases, unprecedented amounts of personal data are being generated and shared in multiple other contexts, such as wearable app technologies, smart personal and home devices, online activity, and biometric technology [8, 9]. Further, the proliferation of data is so vast that some question whether we are entering a new, post-privacy era in which the relinquishment of privacy is an accepted cost of using new technologies [10, 11].

Existing research suggests that people weigh the potential clinical benefit against the risk of privacy breach when making choices about genetic testing [12]. However, little is known about how people weigh privacy-related concerns for genetic testing within the broader social context of frequent choices about the privacy of non-genetic personal data. Understanding the role of privacy-related choices in the larger social landscape is important to designing privacy policies for population genetic screening initiatives [13]. We conducted a qualitative focus group study to contextualize participants' views of privacy of genomic information compared to privacy of other types of personal information.

2. Materials and Methods

2.1 Sampling and Recruitment

We conducted four focus groups with members of Kaiser Permanente Washington (KPWA), an integrated health care system that provides care and insurance coverage to more than 700,000

members in Washington state. Our inclusion criteria were intentionally broad and included English-speaking KPWA members ages 18 years and older. Striving for age and racial/ethnic diversity across the sample to get a range of perspectives, we used KPWA administrative data to create four separate samples: white participants ages 18-39; non-white participants ages 18-39; white participants ages 40 and older; and non-white participants ages 40 and older. We used a consecutive sampling approach, approaching eligible members by mailed letter with phone outreach to each sample until recruitment was filled. Recruitment for each focus group closed when at least 8 people had agreed to participate in the session or until recruitment efforts were exhausted.

2.2 Focus Group Design

We developed and refined our focus group guide to elicit group sharing and discussion about aspects of privacy following Solove's taxonomy of privacy, which includes multiple aspects of privacy and its potential violation: data collection, data processing, data disclosure, and data misuse [14]. We designed the focus groups to understand participants' views about genetic data and multiple other types of data: family medical history data; other health-related data; and personal data not related to health or genetics. Discussion topics included data ownership, rights to privacy, and use and misuse of data.

In the first half of each focus group, facilitators asked participants to share their thoughts on rights, ownership, and privacy with respect to genetic data. During the second half of the focus group, facilitators asked participants to brainstorm other types of data that people might knowingly or unknowingly disclose (such as social media posts, online shopping history, etc.) and share their expectations regarding rights, ownership, and privacy of these types of data. Finally, the facilitators asked participants to consider whether and how their views on the privacy of genetic data differ from their views on the privacy of other types of data.

Focus groups were held in person in late 2019 just before the COVID-19 pandemic. Each focus group was attended by at least two study team members trained in qualitative research and focus group facilitation; one served as primary facilitator and one as secondary facilitator and notetaker; notes were made on a whiteboard that participants could view. All focus groups were audio-recorded and transcribed with identifiable personal data such as names omitted. A court reporter attended three of four sessions and audio-recorded the session while making a real-time transcription. After the session, the court reporter finalized the transcript after checking against the recorded audio, produced a full transcript for each session with personal identifiers removed. For the fourth session, the study team made an audio recording of the session and commissioned a professional transcription.

2.3 Analysis

We conducted template analysis of focus group transcripts and facilitator field notes. Template analysis involves using an existing framework (e.g., topics in a focus group guide) to create an initial codebook, while allowing for the addition of new codes based on emergent themes discovered during analysis [15-17]. We created a draft codebook based on our research question and focus group guide, and then four researchers (NBH, PRB, MFG, LP) independently piloted the draft codebook on a subset of excerpts from two focus groups. The coders then compared their codes, discussed discrepancies to reach consensus, and revised the codebook based on emergent themes

in the data. After finalizing the codebook, one researcher independently coded each transcript and a second researcher reviewed and provided input on the initial coding; discrepancies were resolved through team discussion and consensus. All data were coded using Atlas.ti (version 8.4) [18, 19].

To identify notable insights from each session and to compare discussion topics across sessions, four researchers each reviewed the transcript of one focus group and developed an episode profile for that group (k = 4). An episode profile is a document summarizing the main points discussed by the group's participants; notable quotations; and the researchers' impressions of the discussion [20, 21].

After completing the coding and episode profiles, we developed coding memos describing in detail the thematic findings for each type of data (genomic data, family medical history data, non-genetic health data, other data). We developed tables to focus our analysis on comparative and contrasting views of privacy across genetic and non-genetic data types. Where possible, we attempted to qualitatively assess any differences in response across groups. Over a series of analysis sessions, the team collectively synthesized the data and refined the findings. We did not conduct member checking.

This study was reviewed by the Kaiser Permanente Washington Institutional Review Board (Federal-wide assurance # FWA00002344, IRB Registration # IRB00010902). It was approved on 08/12/2019. The internal IRB project ID is IRBNet#1469215.

3. Results

The sample (n = 24) was 67% female, mean age 54.1 years; and 62% White race. Eighty percent of participants had a college or post-graduate education (Table 1). Six participants (25%) reported a personal history of cancer.

Table 1 Population characteristics.

	N	**%**
Total	24	
Female	16	66.7%
Age, mean (range)	54.1	(23-88)
Age group		
18-29	4	16.7%
30-39	4	16.7%
40-49	4	16.7%
50-59	2	8.3%
60-69	2	8.3%
70-79	5	20.8%
80+	3	12.5%
Race/ethnicity (not mutually exclusive)		
American Indian/Alaska Native	1	4.2%
Hispanic	8	33.3%
White	15	62.5%
Black or African-American	2	8.3%
Asian	2	8.3%

Other	4	16.7%
Education		
High school equivalent or less	3	12.5%
Some college	4	16.7%
4-year college degree	7	29.2%
Post-graduate	10	41.7%
Employment		
Working/stay at home	14	62.5%
Retired	9	37.5%
Marital status		
Married	9	37.5%
Divorced	4	16.7%
Single	11	45.8%

The most frequently discussed topics were beliefs about rights around data ownership, how data should be used (or not used), and perceived benefits and risks associated with intended or unintended disclosure. Beliefs about rights associated with data and how they should be used were primarily mentioned in reference to genomic data. By contrast, perceived risks of data disclosure were more commonly discussed around other types of data, as were mentions of passive disclosure, use by corporations or government, and potential data breaches. Discussions of non-health personal data included concerns about data protections and laws governing use; data breaches; perceived risks and benefits of disclosure; and concerns about corporate or government use of data. An overview of comparisons between data types is summarized in Table 2 and below.

Table 2 Participants' views of genetic privacy compared to other kinds of data privacy.

Qualities	Privacy related rights	Benefits; potential misuse	Potential harms/misuse
Genetic data			
Permanent, unalterable Core component of self Is a type of medical information Has shared quality with relatives Can be known or unknown	Privacy expected and assumed protected under current laws Individual, personal ownership of testing choices, one's genetic data, and sharing Obligation, not duty, to share with family Limited sharing (e.g., specific genetic risks) was more acceptable than unlimited (e.g., full sharing of genome)	Self and relatives manage health care Personal utility	Data breach (by health care) Unauthorized disclosure (by relatives) Promoting racism/white supremacy (by governments) Spam/ad targeting (by corporations)
Medical family history data			

Shared between family members, part of family story Is valued less than genetic data by clinicians May be incompletely shared/known	Family members have right to learn about, but individuals have right not to contribute to family history knowledge	Personal utility Self and relatives manage health care	Unauthorized disclosure (by relatives) Stigma (e.g., addiction) Worrying relatives
Health-related data (non-genetic)			
Highly personal and individual All known personal medical history and health care received Lives in medical record More visible than genetic/family history data (e.g., pregnancy, injury)	Privacy expected and assumed protected under current laws No duty to share with family members Individual, personal ownership of data and disclosure	Manage personal health care	Data breach Discrimination (by employers, insurance)
Other data (non-health, non-genetic)			
Includes many types of personal data (e.g., social media, shopping history) Is "out there" by choice or assent; cannot be made private/erased Is not a core part of self Is individual (not shared) Can be altered (e.g., name, phone #) but not made private	No expectation of data privacy Individual right to some control over how data are used Personal responsibility to control or at least know how data are used Insufficient opportunities for informed consent over data use (by corporations)	Convenience, personal safety	Data breach Being tracked/surveilled (by government) Immigration-related misuse (by government) Fuzzier conceptions of misuse (e.g., Big Brother, data security, future)

3.1 Qualities of Genetic Data Compared to Non-Genetic Data

Participants considered genetic data, but not other data types, as a permanent, core part of the individual self. Participants recognized the shared nature of genetic information between biologic relatives, but tended to express a strong sense of ownership of their genetic information as a core individual feature. One participant described genetic data as "it's who I am." Another person stated:

> *"People are really private. But those things can change. Your genetics don't change. You can change everything on the outside, really, but your genetics are your blueprint and I can't change it. I mean, I wish I could go back and say "mama, I wish I would have got your blue eyes and not this." But it is what it is. So, yes, especially my genetics."*

By contrast, family medical history data was considered as shared data among biologic family members rather than an individual characteristic. As one participant put it: “we’re all in the same boat.” Some participants considered family medical history as less completely known or shared.

Other health data were considered more visible than genetic data. Participants reflected that conditions such as pregnancy, illness, or injury can introduce inherent risk by their visibility, in particular from employers:

“Basically, you're kind of talking about health problems. There was a time when being a young woman, and, therefore, able to get pregnant could keep you from getting a job…I mean, health problems in general may potentially put you at risk with an employer, and genetic issues in particular also could potentially I suppose.”

All health-related data (genetic; family medical history; and other health-related data) was considered by participants as protected medical information. As one person stated:

“For me [genetic data] is the same as any medical information, so it's -- you know, we didn't put any of that stuff up there, other than maybe fingerprints. …genetics is more related to medical information. It isn't just out there for anybody to look at, other than insurers at times, different levels of insurance.”

Participants did not mention specific laws, nor did the facilitators query about knowledge about specific laws. Rather, participants mentioned the protected nature of the physician-patient relationship:

"I think the disclosure of your health is just between you and your doctor; that's the relationship."

and the responsibilities of health systems or employers to protect data:

"I'm less worried that Kaiser or a doctor are going to give [genetic information] out than a capitalist corporation."

"I mean, you know, doctor privacy. It's all -- nobody is going to demand to see Group Health [Kaiser Permanente] records."

"Employees are protected. If somebody were to have something like your brother, employees are protected because if somebody let you go because you were ill, that's not allowed."

Examples of non-health data included social media posting, shopping or other online behavior, facial recognition technology, fingerprints, immigration status, and social security number. In contrast to genetic data, these data were not considered a core part of one’s self (one person called it more of a “persona”) and were considered clearly individual, rather than shared, information. Participants considered these types of non-health data alterable (e.g., changing one’s phone number), yet also irreversibly "out there" and not able to be made private or erased once disclosed.

3.2 Privacy Rights of Genetic Data Compared to Non-Genetic Data

Participants felt that an individual owns their genomic data and other personal health data and should have control over how it is used and disclosed. One participant described genetic data as "my right to share with whom I please." This sense of personal ownership extended even to family members. Participants considered disclosure of one's personal genomic data to relatives, at most, an obligation or courtesy. However, participants recognized tensions between personal ownership and relatives' potential right to know, recognizing that one's personal medical history might be relevant to other family members:

"The privacy issue kind of -- I see it as overlapping with this -- or carried along with rights, my rights versus your rights. It's your right to decide not to be vaccinated but my right to not be put in a place where you're jeopardizing me. …You know, the right to know and the right to -- whose rights are you infringing on when you do or don't do something. … it's the same as, you know, my right to keep the information to myself. But is it my niece's right to know? …Or her right to refuse to know. So they kind of -- I see them as overlapping in some cases. Privacy and rights are tied up a little bit together."

Some people reflected that sharing only select portions of one's personal health data with relatives might be more acceptable than sharing one's full medical history:

"There's things that people might not be that comfortable being part of the family knowledge, like, STDs or herpes or miscarriages. It's really private for a lot of people, and sometimes a lot of people don't share their miscarriage stories even to their own family. So there's some stuff that people might be, like, "oh, yeah sure." But then erectile dysfunction, like, you might not want your kids to know that or you might not want, you know so there's a big range so it's kind of complex. I know that's why you brought us here because it's not easy."

One person described how not disclosing family history could protect relatives:

"Gosh, I wish I had the right to know more about my family history. I think maybe just along the lines information gets lost or sometimes people are fearful of having to share information I think because it comes with there's a lot of pain of experiencing these illnesses and diseases. I don't know. Maybe it's a sense of feeling like they're protecting us from what illness that we might encounter as well or get passed along to us."

Participants also expressed concerns about worrying family members by disclosing medical information. Some participants noted generational differences in medical history sharing, as one person who discussed their family history of cancer: "it wasn't until more recently in the past few years we started talking about it, but even so I feel like there's a lot of information I don't know for my family."

Participants had no expectation of individual privacy around non-health-related personal data. The following exchange was typical of views expressed in all focus groups:

"FACILITATOR: And so this information that's already out there about us, how private do you think it is? --

RESPONDENT 7: Not private at all.
RESPONDENT: I have no illusion.
RESPONDENT 1: Not private at all.
RESPONDENT 7: To a certain extent. I don't think my next-door neighbor can necessarily learn, but if he or she is sophisticated, probably could."

Whereas participants assumed privacy protections for genetic or personal health data, no such protections for non-health data were assumed:

"We actually have been forced to be part of a system that hasn't really been fully tested, you know, the internet. Just everyone gets really psyched about it because the benefits. There's pros and cons. The pro is that you don't have to go shopping. You can shop in the comfort of your home and time limit. But then you have the other part that the system itself of online shopping, online banking, online everything, even your, you know, like dating everything. Your medical profile, you can access it online now. You can have an app. So I feel like what I -- I personally feel like quite -- it will help us because we're not going to go to the manual, you know, analog era…. if nobody's really securing that, there is no way any of our information, genetic or financial or whatever, is going to be safe."

In response to this perceived lack of regulation, some participants cited personal responsibility as the primary means to control, or at least know, how one's data is being used. For example:

"Every time I do something or somebody call me on the phone, I'm like 'Hey, no. I won't give you that information.' So it, again, comes back to the knowledge that you have that brings you, like, 'uh, I'm not so sure.' So you're the only one that can protect yourself. Like, don't give much information. Don't buy too much stuff online."

3.3 Potential Use, Risks, and Misuse of Genomic Data Compared to Other Types of Personal Data

For genetic data, family history data, and other health data, the main benefit of data disclosure was the potential for improved health or health care management. Personal utility in the form of reassurance, life planning, and/or reduced uncertainty was also mentioned for genetic data and family history (e.g., "filling out the blanks" of family history).

For non-health data, perceived benefits were more varied, ranging from convenience (e.g., use of smart speakers for information and entertainment), shopping discounts to a feeling of personal safety, as in this example:

"[London] is one of the most photographed cities, so it's kind of, like, well, I want to go to London. I want to see these things. And I know I'm going to be filmed. And if there's a terrorist thing there, I know they can do that to find people. So, okay. I'm okay with that. So, again, giving up that kind of privacy."

The most commonly noted privacy risk for all data types was unauthorized disclosure, and potential subsequent misuse of the disclosed data. For genetic data, unauthorized disclosure by relatives ("I want to trust, like, folks that I'm related to to keep that information, but I don't know if I would"), by clinicians ("sometimes doctors hand people the wrong information"), or misuse of data

by governments, employers, or insurers to promote discrimination or racist ideas such as eugenics ("It's white supremacy, basically"). Even though protections on health and genetic data were assumed, some participants noted that "laws can change" so protections could change over time. As discussed in one focus group*:*

"PARTICIPANT 3: Stigma.
PARTICIPANT 2: Yes. And also because …In the history of humans, we--I mean, you know, you know what can happen. You know racism and persecution."

Some participants noted concerns about genetic information being used for marketing purposes, as in this example:

"I personally am very interested in advertising… I already know all sorts of nefarious things I could do if I had people's genetic testing. I could do targeted ads for insulin or for -- and not just to you, but if -- if I had -- if I had information that you or somebody else had diabetes, and then I could also find out through some sort of sources that you had kids, I could start targeting those kids with prediabetes ads or all sorts of things. I could target people with -- who I know are going to have arthritis with prearthritis creams. Or just people who have a tendency towards Alzheimer's with pills and home remedies, homeopathic things that they may know are coming but aren't affecting them yet. And so you can get them when they're in their 30s and 40s of things that might help stave it off. And just -- there's a lot of damage that they could do."

Potential privacy risks following misuse of non-health data were more varied, ranging from discomfort with the idea of being tracked or surveilled to a general discomfort with data-based technology:

"I saw this thing on China. I think where we're going -- they have so many cameras and it's just, like, kind of public shaming. Say you jaywalk and they take your picture and then it's flashing, like, on this huge, like, New York Times size screen, and it's, you know, jaywalker, jaywalker."

"I don't see all the Alexa stuff and the network of facial features and stuff -- I don't see that as beneficial. Like, I see that as just another step closer to Big Brother is watching."

"It is kind of creepy in the sense that I just did a search on Google, which is a completely different service than Instagram, and it popped up on my Instagram and how they're connected like that."

Some participants expressed concern about government misuse of personal data, including health care data, for enforcing immigration laws. This concern was only noted by non-White participants. For example:

"[Data privacy] is a huge deal right now with where I work. We're very cautious about not, like when we're sending email, not including the child more than just their initials and like no name or birthday gets sent out. All of our servers and systems that we use are very high security, and there's lots of emails that are going out. If ICE shows up, this is what you do. You don't let them in, like all these different things. It's a huge deal, and families are afraid to seek services that they can use, but they're not informed on what they can and can't do. It's this tricky thing of am I safe

going to the doctor to get my child's immunizations or am I safe to go get myself a checkup and all of that? People are very fearful of anything that's public, a public service with their personal information."

4. Discussion

This qualitative focus group study compared views on privacy of multiple types of data, in order to contextualize privacy considerations about use of individual genetic data. We found that genetic data were considered individual, permanent, protected, and highly personal health information. We also found that while people appreciated the tension between individual and family concerns with respect to potentially shared genetic data between biologic relatives, they did not consider sharing of family-relevant genetic or medical history information to be a relative's right or an individual's duty. Benefits of data disclosure varied between data types, from health and health care management and increased knowledge the main benefits of genetic data, and convenience and enhanced public safety for non-health personal data. Unauthorized disclosure was the primary privacy concern for all data types, by individuals and health systems for genetic data and primarily by corporations or government authorities for non-health data. Specific concerns about misuse of immigration status data were noted.

Our findings are consistent with other work on privacy in health care that find that people make tradeoffs between personal benefits and potential privacy risks when making decisions, and that trust in protections on health-related data may influence those decisions [22, 23]. In a qualitative study of privacy considerations by people using digital pill systems that allow monitoring of PReP adherence, participants wanted access to their adherence data and were largely willing to share these data with their clinicians [24]. In a qualitative study of pregnant individuals' acceptability of mobile health technologies, participants weighed benefits of sharing their data with clinicians against potential privacy breaches [25]. Our study participants' reflections about the tension between data disclosure obligations between biologic family members reflect current ethical and legal debates about duty to warn of genetic risk on the part of patients and clinicians [26-28].

Our findings are consistent with current debates and conceptual models about the relationship between privacy and technology. Privacy as it relates to genetic and other technologies has largely been debated and interpreted as an individual right that may clash with shared interests. Individual privacy is foundational to participation in social groups, and perhaps in particular for health technology, privacy is understood by its violation, which may disproportionately harm vulnerable groups [10, 14]. A scoping review of studies of privacy needs related to participatory health technology (e.g., mobile health technology; patient portals) found balancing patient privacy and confidentiality concerns to be central to maximizing the potential benefit of these technologies [29]. The conceptual model of privacy and emerging technologies by Schairer and colleagues, based on more than 100 qualitative interviews, found that an individual's disposition toward privacy can change based on the context. Choices about sharing one's data varied according to considerations that were "conventional" (e.g., for medical care), intangible (e.g., altruism, perceived improved community standing), or philosophical (e.g., fatalism that privacy does not exist, trading privacy for other benefits) [12]. Qualitative work by Haeusermann et al. (2018) found that people who had shared their genetic testing results obtained through direct-to-consumer testing on an open, public platform reflected on potential privacy-related harms. Sociodemographic status, gender, ethnicity,

sexual orientation, and health conditions associated with stigma, as well as existing legal protections, informed people's views about the relative harm in these contexts [30].

As debates about genetic exceptionalism move toward consideration of contextual factors and specific uses of data in specific settings [3, 31], consideration of the social contexts within which individuals make choices and form views on genetic data are crucial. Our study shows that people make choices about multiple kinds of data in the course of their daily lives and actively seek to understand the nuances between types and uses of data. One study used a similar comparative approach to ours, asking participants to discuss privacy concerns in a health-related (mHealth apps) and non-health related (smart speakers) domains. In the qualitative study by Schroeder and colleagues, older adults reported accepting tradeoffs between privacy and the potential benefits of using mHealth apps. Surprisingly, participants valued the privacy of their recorded verbal data more than that of personal health data and reported increased personalized ads as a greater potential harm than misuse of their health data [32].

Our study did not attempt to rank the relative value of privacy of different types of data but did find that perceived privacy-related harms may be related to their accompanying level of perceived legal or regulatory protection. In our study, participants noted specific concerns for genetic or health care data (primarily unauthorized disclosure), but more diffuse concerns of misuse by various actors for non-health related personal data (e.g., surveillance, direction of society). However, participants did note some very specific potential harms related to government unauthorized use of immigration-relevant personal data, consistent with current debate about whether immigration status should be protected health information [33].

Demertzis and colleagues theorize that people may experience "digital resignation" and accept as inevitable that their personal data will be used by corporate entities [11]. A focus group study among Canadian youth found that when navigating social media sharing, older teens may embrace a "nothing to hide" perspective in which the very idea of privacy is not relevant to them [34]. We found some evidence of this phenomenon in participants who reported not caring about their data being released, particularly for participants under age 40, but this primarily applied to types of data other than genetic or health care data. Perhaps this is related to the noted assumed privacy protections associated with genetic data.

Our study has some limitations. These data represent one point in time just before the COVID-19 pandemic began, in a relatively small sample of insured adults in a defined geographic area. While we intentionally recruited a sample that was diverse in age and race/ethnicity to learn from as many perspectives as possible, the majority of participants reported a 4-year college degree or more, which may limit the generalizability of our findings. Further, the small sample size prevented a thorough assessment of views between specific population groups, including race and ethnicity. We found some suggestion that participants of color were particularly concerned about government authorities' misuse of immigration-related data and that people under age 40 may have more relaxed attitudes about personal data privacy, and this is supported by other research [35-37]. These findings should be explored in future research as a potential barrier to genetic testing. Similarly, we found some suggestion of generational differences in sharing of family medical history data, which may be of interest for future work.

These findings show that people consider privacy implications of sharing multiple types of data and suggest that consideration of the broader social context of technology-generated personal data may be relevant to the design and implementation of genetic screening programs and genetic

research. Future research can explore how privacy concerns vary across data types and over time, and compare privacy-related views and experiences of people from specific population groups.

5. Conclusions

People make privacy-related choices about genetic testing in the context of other privacy considerations for multiple types of data and rely on perceived privacy protections afforded under current U.S. health privacy laws. Genetic research and screening programs should consider providing clear guidance on privacy protections afforded to genetic information in U.S. settings. Future research should examine connections between privacy-related views on genetic data and multiple other types of personal data.

Acknowledgments

The authors acknowledge the time and generosity of the study participants, without which this study would not be possible.

Author Contributions

Nora Henrikson and S. Malia Fullerton led the conception and design of the study. Nora Henrikson drafted the manuscript. Lorella Palazzo, Marlaine Figueroa Gray, Paula Blasi and Nora Henrikson conducted the focus groups and wrote portions of the manuscript. All authors made substantial contributions to data acquisition, analysis and interpretation and reviewed and revised the manuscript for intellectual content. All authors approved the version of the manuscript to be published.

Funding

U01 HG008657 (Larson, Jarvik) National Human Genome Research Institute; and by R01HG010144-01A1 (Henrikson); National Human Genome Research Institute.

Competing Interests

The authors have declared that no competing interests exist.

References

1. Backes M, Berrang P, Humbert M, Shen X, Wolf V. Simulating the large-scale erosion of genomic privacy over time. IEEE/ACM Trans Comput Biol Bioinform. 2018; 15: 1405-1412.
2. Bonomi L, Huang Y, Ohno-Machado L. Privacy challenges and research opportunities for genomic data sharing. Nat Genet. 2020; 52: 646-654.
3. Clayton EW, Evans BJ, Hazel JW, Rothstein MA. The law of genetic privacy: Applications, implications, and limitations. J Law Biosci. 2019; 6: 1-36.
4. Wang S, Jiang X, Singh S, Marmor R, Bonomi L, Fox D, et al. Genome privacy: Challenges, technical approaches to mitigate risk, and ethical considerations in the United States. Ann N Y Acad Sci. 2017; 1387: 73-83.

5. Berger B, Cho H. Emerging technologies towards enhancing privacy in genomic data sharing. Genome Biol. 2019; 20: 128.
6. Clayton EW, Halverson CM, Sathe NA, Malin BA. A systematic literature review of individuals' perspectives on privacy and genetic information in the United States. PLoS One. 2018; 13: e0204417.
7. Haga SB, O'Daniel J. Public perspectives regarding data-sharing practices in genomics research. Public Health Genomics. 2011; 14: 319-324.
8. Schwab AP, Luu HS, Wang J, Park JY. Genomic privacy. Clin Chem. 2018; 64: 1696-1703.
9. Ram N, Guerrini CJ, McGuire AL. Genealogy databases and the future of criminal investigation. Science. 2018; 360: 1078-1079.
10. Pyrrho M, Cambraia L, de Vasconcelos VF. Privacy and health practices in the digital age. Am J Bioeth. 2022; 22: 50-59.
11. Demertzis N, Mandenaki K, Tsekeris C. Privacy attitudes and behaviors in the age of post-privacy: An empirical approach. J Digit Soc Res. 2021; 3: 119-152.
12. Schairer CE, Cheung C, Kseniya Rubanovich C, Cho M, Cranor LF, Bloss CS. Disposition toward privacy and information disclosure in the context of emerging health technologies. J Am Med Inform Assoc. 2019; 26: 610-619.
13. Bayefsky MJ. The human genome as public: Justifications and implications. Bioethics. 2017; 31: 209-219.
14. Solove DJ. Understanding privacy. Cambridge, MA: Harvard University Press; 2010.
15. Crabtree BF, Miller WL. Using codes and code manuals: A template organizing style of interpretation. In: Doing qualitative research. 2nd ed. Thousand Oaks, CA: Sage Publications; 1999. pp. 163-177.
16. Brooks J, McCluskey S, Turley E, King N. The utility of template analysis in qualitative psychology research. Qual Res Psychol. 2015; 12: 202-222.
17. Braun V, Clarke V. Using thematic analysis in psychology. Quali Res Psychol. 2006; 3: 77-101.
18. Friese S. Qualitative data analysis with ATLAS.Ti. 3rd ed. London: SAGE; 2012.
19. Saldaña J. The coding manual for qualitative researchers. 3rd ed. London: SAGE; 2015.
20. Maietta RC. State of the art: Integrating software with qualitative analysis. In: Improving aging and public health research: Qualitative and mixed methods. Washington, DC: American Public Health Association and the Gerontological Society of America; 2006. pp. 117-139.
21. Fryer CS, Passmore SR, Maietta RC, Petruzzelli J, Casper E, Brown NA, et al. The symbolic value and limitations of racial concordance in minority research engagement. Qual Health Res. 2016; 26: 830-841.
22. Cherif E, Bezaz N, Mzoughi M. Do personal health concerns and trust in healthcare providers mitigate privacy concerns? Effects on patients' intention to share personal health data on electronic health records. Soc Sci Med. 2021; 283: 114146.
23. Shen N, Bernier T, Sequeira L, Strauss J, Silver MP, Carter-Langford A, et al. Understanding the patient privacy perspective on health information exchange: A systematic review. Int J Med Inform. 2019; 125: 1-12.
24. Goodman GR, Kikut A, Bustamante MJ, Mendez L, Mohamed Y, Shachar C, et al. “I’d feel like someone was watchin’ me… watching for a good reason”: Perceptions of data privacy, access, and sharing in the context of real-time PrEP adherence monitoring among HIV-negative MSM with substance use. AIDS Behav. 2022; 26: 2981-2993.

25. Li J, Silvera-Tawil D, Varnfield M, Hussain MS, Math V. Users' perceptions toward mhealth technologies for health and well-being monitoring in pregnancy care: Qualitative interview study. JMIR Form Res. 2021; 5: e28628.
26. Kilbride MK. Genetic privacy, disease prevention, and the principle of rescue. Hastings Cent Rep. 2018; 48: 10-17.
27. Rothstein MA. Reconsidering the duty to warn genetically at-risk relatives. Genet Med. 2018; 20: 285-290.
28. Weaver M. The double helix: Applying an ethic of care to the duty to warn genetic relatives of genetic information. Bioethics. 2016; 30: 181-187.
29. Househ M, Grainger R, Petersen C, Bamidis P, Merolli M. Balancing between privacy and patient needs for health information in the age of participatory health and social media: A scoping review. Yearb Med Inform. 2018; 27: 29-36.
30. Haeusermann T, Fadda M, Blasimme A, Tzovaras BG, Vayena E. Genes wide open: Data sharing and the social gradient of genomic privacy. AJOB Empir Bioeth. 2018; 9: 207-221.
31. Garrison NA, Brothers KB, Goldenberg AJ, Lynch JA. Genomic contextualism: Shifting the rhetoric of genetic exceptionalism. Am J Bioeth. 2019; 19: 51-63.
32. Schroeder T, Haug M, Gewald H. Data privacy concerns using mhealth apps and smart speakers: Comparative interview study among mature adults. JMIR Form Res. 2022; 6: e28025.
33. Schweikart SJ. Should immigration status information be considered protected health information? AMA J Ethics. 2019; 21: E32-E37.
34. Adorjan M, Ricciardelli R. A new privacy paradox? Youth agentic practices of privacy management despite "nothing to hide" online. Can Rev Soc. 2019; 56: 8-29.
35. Taitingfong R, Bloss CS, Triplett C, Cakici J, Garrison N, Cole S, et al. A systematic literature review of native American and Pacific islanders' perspectives on health data privacy in the United States. J Am Med Inform Assoc. 2020; 27: 1987-1998.
36. Parobek CM, Thorsen MM, Has P, Lorenzi P, Clark MA, Russo ML, et al. Video education about genetic privacy and patient perspectives about sharing prenatal genetic data: A randomized trial. Am J Obstetr Gynecol. 2022; 227: 87.e1-87.e13.
37. Ewing AT, Erby LA, Bollinger J, Tetteyfio E, Ricks-Santi LJ, Kaufman D. Demographic differences in willingness to provide broad and narrow consent for biobank research. Biopreserv Biobank. 2015; 13: 98-106.