# Privacy and Activism in the Transgender Community

**Ada Lerner**
Wellesley College
Wellesley, MA, USA
alerner@wellesley.edu

**Helen Yuxun He**
Oberlin College
Oberlin, OH, USA
yhe@oberlin.edu

**Anna Kawakami**
Wellesley College
Wellesley, MA, USA
akawakam@wellesley.edu

**Silvia Catherine Zeamer**
Wellesley College
Wellesley, MA, USA
szeamer@wellesley.edu

**Roberto Hoyle**
Oberlin College
Oberlin, OH, USA
rhoyle@oberlin.edu

## ABSTRACT

Transgender people are marginalized, facing specific privacy concerns and high risk of online and offline harassment, discrimination, and violence. They also benefit tremendously from technology. We conducted semi-structured interviews with 18 transgender people from 3 U.S. cities about their computer security and privacy experiences broadly construed. Participants frequently returned to themes of activism and prosocial behavior, such as protest organization, political speech, and role-modeling transgender identities, so we focus our analysis on these themes. We identify several prominent risk models related to visibility, luck, and identity that participants used to analyze their own risk profiles, often as distinct or extreme. These risk perceptions may heavily influence transgender people's defensive behaviors and self-efficacy, jeopardizing their ability to defend themselves or gain technology's benefits. We articulate design lessons emerging from these ideas, contrasting and relating them to lessons about other marginalized groups whenever possible.

### Author Keywords

security; privacy; transgender; gender identity; social networks; presentation management; user-centered design

## INTRODUCTION

Transgender people are a highly diverse population who nevertheless share many vulnerabilities and experiences. Technology offers them disproportionate benefits: for example, queer youth are much more likely than other groups to have important online friends, often first come out as queer online, engage in activism and civic participation online at high rates, and search for sensitive (e.g., sexuality- and medical-related) information online at much higher rates than non-queer youth [21]. They also face high levels of risk: transgender status is associated with lower socioeconomic status and elevated rates of suicide, violence, harassment, homelessness, and discrimination, including in key areas such as housing and employment [6, 41, 45, 21, 37, 26, 40, 54, 15, 25]. Safety and harm of transgender people has been studied previously Scheuerman et al. [58], categorizing threats and harm reduction techniques, and by others (e.g., Haimson [27]) who have found that supportive communities online enhance the emotional well-being of trans people. It is necessary, however, to explore this area through a computer security and privacy lens as well, as many of the risks and challenges that have been studied in this space previously may not apply to transgender individuals. Understanding transgender people's computer security and privacy experiences can enable us as technologists and designers to mitigate these risks and allow them to derive enormous benefits from technology in critical social, civic, and educational domains.

At least 1.4 million Americans – over 1 in every 200 – are transgender, and this paper investigates their security and privacy experiences. Although transgender people are as diverse as humanity, they often share unique experiences of self-presentation, ostracism, microaggressions, and more. Common experiences for transgender people, such as specific medical interventions and changes to legal gender markers and first names, are rare in the general population. Since security systems, such as airport security and authentication systems, sometimes use rarity as a reason for suspicion, such systems often spuriously flag transgender people's bodies and everyday behaviors, creating severe usability challenges, such as account lockout, invasive searches, missed flights [55, 66, 34]), and opportunities for discrimination and harassment.

To understand their experiences and needs, we performed semi-structured interviews with 18 transgender adults from three U.S. metropolitan areas. Participants were not preferentially recruited for being activists; nevertheless, activism, political action, and prosocial behavior (such as role-modeling, experience-sharing, and advice-giving) emerged as major themes, as may be expected from past work such as Whittle which found that networked technology has enabled new forms of activism among trans and gender non-conforming people [62]. Our results and analysis presented in this pa-


*CHI '20, April 25–30, 2020, Honolulu, HI, USA.*

ACM ISBN 978-1-4503-6708-0/20/04 ...$15.00.
http://dx.doi.org/10.1145/3313831.3376339

per focus heavily on these activist themes. We report on our participants' goals, risk models, experiences, use of defenses, and challenges, as well as on significant heterogeneity of experience for transgender people with intersecting marginalized identities. Our discussion analyzes the risk models our participants applied to understand their privacy and activism, and the effects that those risk models may have on their self-efficacy, self-blame, and use of defenses.

**Contributions.** The contributions of this paper include:

- Qualitative interviews exploring broadly the security and privacy needs of transgender people.
- A focused analysis of these needs in the context of activism and prosocial behavior, including trans peoples' goals, models of risk, and challenges.
- A taxonomy of the risk models we found, and analyses of how these risk models may affect transgender people's ability to protect themselves.
- Analysis of design challenges and opportunities for two technologies that respond to challenges we uncovered.

### Vocabulary and Usage

Specialized terms used in this paper are defined here, with definitions and usage based on norms and practices of the queer community [22].

**Transgender** *adj.*: Of or relating to a person whose gender identity differs from their sex assigned at birth.

**Cisgender** *adj.*: Not transgender. Also "cis".

**Queer** *adj.*: A reclaimed term for LGBTQ.

**Transgender status** *n.*: Whether or not a person is trans.

**Gender Transition** *n.*: The process of changing gender roles, or of matching outward appearance with internal gender identity. Sometimes simply "transition".

**Deadname** *n./v.*: The old name of a trans person, or the (disrespectful) act of calling someone by it.

## RELATED WORKS

In this section, we summarize the most relevant prior work, starting with an overview of transgender populations and HCI research on them, privacy and security research on marginalized populations, and HCI research on activism and activists.

### Transgender Populations

Transgender people have traditionally been a highly vulnerable population, having correlation with lower socio-economic status [6], higher rates of homelessness [41], high rates of discrimination [20, 38], harassment, and violence both online [21] and offline [45, 37, 42] and suicidal ideation [13]. The process of 'coming out' and having one's public persona match one's private persona has been studied [16, 18], along with potential positive benefits [52, 51], but still, revealing one's transgender status may have severe implications [13]. Whittle finds that online technology has enabled new community structures, forms of activism, and identities among trans and gender non-conforming people [62], while Haimson [31] examines Tumblr as an example enables such activity.

### Security and Privacy Needs of Marginalized Groups

It is a moral imperative to extend the benefits of research beyond the average person and towards under-represented minorities. Fortunately, the HCI community has been investigating how research that affects the typical user may not apply to the unique needs and desires of different users. Researchers have investigated how visual impairment affects online privacy [2, 3], social network use [65], authentication [5, 33], and how technology can improve their everyday lives [9]. Wisniewski et al. [63, 64] have studied how teens protect themselves online and how managed risk will increase their resilience to online threats and cyber-bullying. Siek et al. [59] have studied how the design of tools for younger people may disadvantage the elderly.

The HCI community has investigated various aspects of transgender identity. Carrasco and Kerne [12] investigated how LGBTQIA people managed visibility in social networks. Haimson et al. investigated how queer people manage online information during periods of transition [29] and how online social networks can both be a source for stress and a mechanism by which stress can be managed [28]. Blackwell et al. [8] investigated how parents managed their online transitions, balancing needs of their families with their self-presentation. Duguay [16] investigated unintentional context collapse on social network sites and the ways that queer individuals attempted to minimize it. Hamidi, Scheuerman, and Branham studied transgender people's attitudes toward automatic gender recognition systems [32], finding overwhelmingly negative responses and severe privacy concerns. DeVito et al. [14] studied how LGBTQ+ populations interact with social media systems, concluding that they create a system of related online personas, each handling different aspects of their presentation and that a system that forced them into a single platform could impinge on their privacy.

Most recently, Scheuerman et al. [58] wrote about safe spaces and harm reduction for transgender people. They categorized various types of harm and harm reduction techniques addressing similar topics to ours. Complementing their work, we frame our findings around privacy theory, via impression management [23], contextual integrity [53], and context collapse [48]. Doxxing, for example when looked via a privacy lens, is unwanted intrusion of information from one context into another by others, causing an invasion of privacy. We reach some of the same conclusions that they found looking at safety and safe spaces, such as concerns around physical safety, while we also make distinct contributions e.g., conceptualizing and taxonomizing risk models of online threats.

### Activism and HCI

The HCI community has investigated controversial subjects such as activism. A sampling of published recent research yields a variety of reports dealing with many forms of activism. Ahmed et al. [1] discussed broadening content restrictions in HCI publications to remove limitations on sex and sexuality. Blackwell et al. [8] wrote about advocacy among LGBTQ parents and the issues that they faced balancing their family lives with their changing identity. Bellini et al. [7] started a Feminist HCI Special Interest Group (SIG).

Michie et al. [50] wrote about HCI being used to design storyboards for abortion-rights activists enabling women to tell their stories. Irannejad et al. [36] studied networking applications used to increase youth community engagement, and the issues faced between the youth users and the older administrators. Li et al. [44] studied online participants in a virtual disability march and how they balanced their disabilities with their desire to be activists for their cause. These papers are just a narrow cross-section of HCI research being focused on activist movements, and this paper fits in with them while focusing on the transgender movement.

## METHODS

We performed semi-structured interviews in Boston, Massachusetts; Cleveland, Ohio; and Seattle, Washington in the early half of 2018. The interviews were recorded as audio files, transcribed into text format, and coded for analysis.

### Recruitment

Participants were recruited via 1) emails to student organizations at Oberlin College and Wellesley College and 2) contacts with administrators of LGBTQ+ organizations in Boston, Cleveland, and Seattle. Adults identifying as transgender, non-binary, or genderqueer were eligible. 44 total individuals responded to these publicity measures, and we interviewed 18 in total, at neutral locations chosen for privacy and the convenience of the interviewees or over the phone when no mutually agreeable time and place could be determined.

### Demographics

Participants were aged from 18 to 49 and included people who self-identified as non-binary (10), genderqueer (3), trans-masculine (3), trans-feminine (1), gender non-conforming (1), genderfluid (1), men (2), and women (2); gender identities sum to more than n=18 because some participants used more than one term. Participants identified with racial and ethnic identities including: Asian-American (2), Ashkenazi Jewish (2), Black (1), Latinx (1), multiracial (3), and White (9). 5/18 participants reported having a disability of some kind. Unprompted, one person disclosed engaging in sex work, which we report because rates of sex work are very high among the transgender community (72% [37]). Education levels ranged from high school to master's; 8/18 participants were students. Income levels represented ranged from poor to wealthy, with a plurality reporting family incomes in the $30,000s.

### Interview Methodology

Prior to each interview, participants were informed of the study purpose and method, and written and verbal consent was obtained for both interviews and recordings. The interviews began with demographics followed by questions about technology use; issues around computer security and privacy; experiences with online dangers; and about how transgender-specific experiences, such as transitioning or coming out, were affected by technology. Throughout the interviews, we reminded participants that we were interested in their experiences both as transgender people and independent of their transgender status, and about experiences related to other identities they held. The semi-structured interview template is included as supplementary material. 11/18 interviews were conducted or supervised by the transgender first author.

### Analysis

The recordings were next transcribed and then coded using a grounded theory approach. Four lab members coded a single interview using an interactive coding process with initial coding and identified concepts. These codes were then combined using axial coding into an initial codebook, organized under agreed-upon categories [56, 57]. These categories were first used to code each interview for the higher-level concepts, and all disagreements between categories were resolved by discussions between the coders until consensus was achieved. Once the higher-level categories were coded, the process was repeated for the more granular codes within each category.

### Ethics and IRB Approval

Ethics and the comfort and autonomy of participants were enacted throughout the research process. Participants were reminded that they were free to refuse to answer questions, to share as much or as little as they wished, and that they could opt out of recording. They were also had opportunities to ask questions about the study both upon initial contact, after reading, but before signing the consent form, and following the completion of the interview. They were also provided with a summary of the research taking place. Furthermore, participants were reminded of the option to opt out and have their data deleted up to 30 days following interview's conclusion. They were given a $20 gift card as compensation. Interviews were held in a private location convenient for participants or over the phone, in efforts to maximize their convenience and comfort. To prevent re-identification of participants we lists counts of demographic attributes, rather than giving each participant's demographics separately. The study was approved by the researchers' Institutional Review Boards.

## FINDINGS

Our interviews explored computer security and privacy broadly, but participants often returned to activism and prosocial behavior, on which we focus this paper. Our findings cover several themes: goals for tech use; models of risk; defenses; tensions between privacy and social good; and privilege and discrimination within the queer community.

### Goals for Using Technology for Social Good

Participants frequently described a strong motivation to use technology for social good in their own personal communities, in the broader trans community, and in the world at large. They often aimed to engage in **activism** by organizing and participating in collective action; to **visibly represent** transgender people and identities, sometimes to the broader world and sometimes internally by role-modeling for and mentoring other trans people; and to engage in **political discourse**.

**Activism.** Some participants (2/18) use technology to organize, discover, or publicize offline protests and demonstrations. Some (3/18) described never using social media to engage in activism for fear of negative consequences, while others (2/18) said their *only* use of public posts on social media were for activist or political purposes.

**Representation/Visibility.** A frequent theme (8/18) was being visible as a representative of transgender people and identities. Participants often saw this goal as a prosocial act that benefits trans welfare and rights. One participant discussed educating people about trans identities, including her own:

> *I always love, I absolutely love sharing what it means to be trans with people who just don't know, who are interested to know, but who are not assholes. (P16, Woman)*

Others (2/18) focused on role-modeling for trans people, especially those with whom they shared identities. P18 uses Instagram to "empower other black trans women" by dispelling myths about femininity through posts involving pictures of herself and her friends and other role-models for those earlier in the process of transitioning

One form of representation with strong privacy implications is public or semi-public revelation of private information, such as medical information or pre-transition photographs. Participants shared this as a form of empowerment, a demonstration of control, and a visibility-raising tactic. For example, P15 said that "admitting" that they take hormones is a "huge" way they act in order to represent non-binary people.

**Political Discourse.** Participants also discussed security and privacy implications of political discourse, with many (9/18) saying they avoid public posts or discussions about politics, though some acted otherwise. For example, one participant said that they post publicly on social media only rarely, but when they do so, it is only on political topics.

One specific form of political discourse consists of a sort of low-grade activism: posting content identified as political, with the aim of changing minds:

> *I occasionally repost things that seem vaguely political and could incite my family members [who] I know on Facebook to think about things every once in a while. (P2, Non-binary person)*

### Tensions of Social Good with Privacy

While pursuing their goals, participants (4/18) sometimes felt tension between their security and privacy needs and the socially positive actions they took. One participant described the tension as two inevitably related sides of a coin:

> *Especially [...in this] political climate, although in some ways it feels riskier now, it feels a lot more urgent and a lot more necessary to be really transparent and honest and explicit about who I am in literally all circumstances. (P17, Genderqueer person)*

Another participant similarly valued representing their non-binary identity specifically because of the danger:

> *...I want to protect myself from people who might mean me harm just for being trans, which is definitely a thing. [But] then it also makes me want to be more visible because I think that non-binary representation is so important. (P15, Non-binary person)*

### Threat Models

We characterize participants' threat models by discussing the adversaries, threats, risks, defenses, and other factors they use to make decisions surrounding their goals for social good. We focus on participants' perceptions and beliefs, and do not attempt to assess or characterize whether they are realistic. Instead, we aim to understand the ways in which their perceptions inform their values and fears and affect their behavior.

#### *Adversaries*

Participants described some adversaries which many groups do not face or which have specific reason to target trans people. Adversaries named included family members, friends, acquaintances, strangers, hate groups, political extremists, corporations, governments, and others. Some participants (4/18) described adversaries from within the broader feminist or progressive community, such as Trans-Exclusionary Radical Feminists (TERFs) [1] and "Transmedicalists". [2]

We observed that in the specific context of activism and social good, participants often focused more narrowly on a subset of these adversaries, which included hate groups (e.g., "neo-Nazis"), political extremists (e.g., "right-wing trolls"), opposing political groups, and government actors.

> *A family member of mine was involved [in LGBTQ activism], and became a target for right wing trolls, and I therefore became a target even though I actually had no role in what this person was doing. (P14, Man)*

Hypothesizing that the U.S. government might specifically target transgender people, one participant said:

> *...because I'm pretty out [as transgender], does that make me more of a target for government monitoring? Like you hear all the time about, "Oh, and these protesters were being monitored by the FBI," [...] when they hadn't done anything except like go to peace marches and rallies for civil rights... (P12, Non-binary/genderqueer person)*

#### *Threats*

Participants described threats their adversaries might enact, including blackmail, shaming, doxxing, harassment, physical violence or property damage, surveillance, and privacy-invasive searches in security-sensitive locations such as borders and airports. As many of these were described by Scheuerman et al. [58], we focus on ones that have a online security and privacy angle, namely **blackmail** and **doxxing**.

[1] A negative term to describe "gender-critical feminists", who are often critical of the transgender community's beliefs about gender

[2] People who believe gender dysphoria a necessary component of being transgender, deny the transgender status of those who do not feel gender dysphoria, and often exclude non-binary identities from the transgender umbrella. [43]

Participants (2/18) identified **blackmail** threats to disclose sensitive information, including possibly their transgender status. Many (9/18) discussed public **shaming** by others over trans status, including shameful accusations of dishonesty for having "lied" about being cisgender before coming out.

Many participants (10/18) brought up **doxxing** as a threat, making it one of the most commonly cited threats. They linked threats of doxxing to being trans, associating increased risks of violence and the existence of hate groups particularly dangerous for this group. Some viewed it as common:

> *People get doxxed all the time... like, "Oh my God. You said this thing I don't agree with. I'm gonna reveal your address to all these Neo-Nazis or something. That's scary to think about...[] Just the idea of being a woman on the internet is pretty scary. I think more so for me now, being pretty visibly [trans]. (P3, Gender nonconforming/non-binary person)*

Both of these threats can be interpreted through the *context collapse* framework [48], in which information that is appropriate in one context is shared with an inappropriate audience in a different context.

### Risks

Security and privacy researchers use threat models as a way to analyze a security or privacy challenge, describing specific values, assets, threats and defenses which are relevant in a specific context. We consider a specific aspect of threat models for transgender people: their mental models of risks. We focus on their beliefs about online security and privacy risks and their observations and experiences that they used to assess what actions to engage in, what defenses to deploy, and what dangers to fear. While these models often relate strongly to discussions of safe spaces and harms [58], our work differs in that we emphasize an analysis of transgender people's perceptions of risk and the ways that those perceptions, and the models they inform, can modify their decision-making processes around security and privacy. For example, while Scheuerman et. al raises the danger of targeted attacks, we recontextualize the fear of this type of attack as sometimes being part of a risk model of identity, under which unchangeable identity factors, i.e. transgender status, may cause targeted attacks and other dangers, and the ways in which that model influences defensive and other behaviors. Our exploration of these models can help us understand how transgender people judge which spaces are safe. They can also help us view how transgender people understand and react to risks, including those that are rare or irrational, and how those perceptions affect their ability to accomplish goals and protect themselves when using technology.

These models are not mutually exclusive, and we do not suggest that a single person always uses the same models for all analyses. We found that participants often contextualized their risk models in terms of their transgender status, and we observe that even similar risk models may be interpreted and acted on significantly differently among cisgender people. We taxonomize the models we observed under three headings: visibility, luck, and identity, which we characterize in this section, and which our discussion explores in terms of their potential effects on decision-making, defenses, and privacy challenges faced specifically by transgender people.

**Risk Model: Visibility.** Visibility-based risk models suggest that being "out there" or "visible" makes victims appealing targets to attackers, increasing risk. Most participants (13/18) described variations on this model. P7 illustrated this mode of risk attribution this way:

> *Because I'm so private, nobody's ever wanted to bother [to harass me]. I don't produce things that people feel entitled to interpret[.] (P7, Non-binary person)*

Another participant echoed this sentiment:

> *But I don't think it's that likely because I just think I'm not interesting. I think people who are more, who kind of put themselves forward in their activism [...] are more at risk. I think I'm boring. (P14, Man)*

P11 related the likelihood of harassment specifically to voicing political views and to actions which "attract attention":

> *I have to be very careful when I voice any sort of political views in certain spaces[...] I am very careful about what I put out and what might attract people's attention to me. (P11, Non-binary person)*

**Risk Model: Luck.** About a quarter of participants (5/18) emphasized the attribution of risk to random or unknowable factors, out of their control or controlled by distant, impersonal adversaries. For example, one participant said they were low profile, but:

> *...[Even so], you can become a target because a lot of it is so random. (P14, Man)*

Participants using this model to make decisions

**Risk Model: Identity.** Many participants (12/18) pointed to identity-based, rather than behavioral factors, as major sources of increased risk. For trans people, this model is naturally backed up by statistics on the victimization of transgender people, which show their vulnerability to violence, harassment, discrimination, mental health issues, suicidal ideation, and other challenges [37, 21, 45, 42, 13, 20, 38]. Additionally, both white participants and participants of color attributed risk to racial identity as well as transgender or queer status, and a nearly all participants (16/18) gave examples which resisted the universal application of this model.

Answering a question about negative experiences and harassment online, one participant of color emphasized the intersectional nature of stereotype-based harassment. She said:

> *Yes, it's always gonna be about my gender and race. It's never a pick or choose one, it's always both. (P18, Woman)*

While this work and past work (e.g., Scheuerman [58], Whittle [62]) find that safe spaces online can act as refuges from persistent danger in the real world, this quote reminds us that

online spaces can also be places of risk and harassment for those holding multiple marginalized identities.

A white participant describing the doxxing of a queer, cisgender acquaintance believed that politics were the primary cause, but that the person's race played a significant role:

> *I think it had more to do with her politics, and it had, I think, a little bit to do with her being black. (P13, Non-binary/genderfluid person)*

Not all participants of color perceived race as a risk-increasing factor for privacy violations, due to the statuses of different minorities in America. One Asian-American participant said:

> *I am considered a model minority [...] I don't feel that, even with more conservative and restrictive administrative policies, that I am specifically being surveyed online [by the U.S. Government]. (P7, Non-binary person)*

One participant also described situations in which they believed that identity-related factors were irrelevant to the likelihood of threats occurring. Speaking of an incident in which acquaintances were doxxed, one participant said:

> *I feel like [...] their privacy as people was jeopardized, but not on the basis of their gender. Their gender wasn't the focus of it. (P4, Non-binary person)*

#### *Defenses and their Cost*

Participants discussed defenses employed against perceived threats, and the costs that they incur because of them. We report on these themes of defensive action: explicit gathering of consent, preemptive disclosure, obfuscation, identification of others, triaging of assets and activities, and opting out.

**Consent.** Several participants (4/18) described privacy norms involving consent for the taking and posting of photographs. These norms were sometimes attributed to the importance of consent in the transgender community, and sometimes described as imported from other activist communities:

> *...domestic violence [activists,] they've really pushed efforts to make sure people get consent before they take photos of other people. Because when you put that out there you don't know who's gonna see it, and what their intentions are. I think with queer and trans people especially, it has really become something just because there's talk of consent. (P3, Gender-nonconforming/non-binary person)*

Another participant described it this way:

> *When I'm posting up pictures from an action I've been at, I will try to make sure [...] that other people's faces are not visible, that people are not identifiable in the background of a rally, in case that's something that they wouldn't want. (P15, Non-binary person)*

This participant also described taking actions to enact location privacy at protests, such as by "not posting where I am when I'm still there." This is a risk management choice which crosses physical and digital boundaries. While other work has found that transgender people often use technology in physical situations to increase feelings of safety (e.g., using Find My Phone features to allow family to know where they are [58]), our result compliments this to illustrate situations in which the combination of physical and digital presence represents instead a risk that must be managed, for example by not posting online until having physically left a protest. Note that this choice could potentially reduce the efficacy of a protest (if it reduces protesters' social media presence), and thus this represents a complicated risk assessment tradeoff dependent on values, perceptions, and risk models.

**Preemptive Disclosure.** One participant viewed coming out as a defense against blackmail.

> *And so if it's not a secret, then you can't stress about the secret. (P14, Man)*

This defense emphasizes the importance of control, rather than pure secrecy, over the disclosure of sensitive information in some contexts.

**Obfuscation and Encryption.** Participants (3/18) who mentioned secure tools such as Signal[3] perceived it as targeted at those involved in especially dangerous activism:

> *I have a handful of friends who do really risky activism, and they will not text. They will only use Signal. (P17, Genderqueer person)*

In addition to cryptographic defenses such as Signal, many participants (8/18) also described informal obfuscation. For example, describing defensive steps taken by friends involved in pro-Palestinian protests, one participant said:

> *They changed their profile pictures to not their faces and changed their names. (P4, Non-binary person)*

In person at rallies, a participant obfuscated their physical appearance to prevent identification by the government or by people with opposing political views in person and in photographs:

> *...when I'm out I'll be wearing like a hat and/or sunglasses or something so it's like a little bit harder to identify me. Or wear like less distinctive clothing sometimes. (P15, Non-binary person)*

**Identification of Others.** P18 moderates a Facebook group exclusive to trans people of color. She described often ad-hoc processes she uses to vet applicants as trans people of color, including asking questions about LGBTQ topics and examining profiles for indications of race and ethnicity. However:

> *Sometimes peoples' profile pictures will have like cartoons on them, and so we will try to message them and say "hey, if you're comfortable can you tell us your ethnic background, or send a selfie of you" unless there's a mutual friend and the mutual friend can tell us their race. (P18, Woman)*

[3] A secure messaging application for phones: https://signal.org

P18 also said that U.S. Immigration and Customs Enforcement agents had made attempts to access some of these race and ethnicity-specific queer groups by making profiles pretending to be trans people of color. She described members of those communities informing each other about this potential threat via public warning posts saying things like:

> *"If this person is trying to add you on Facebook or be in one of your groups, delete them, block them because they work for the ICE police." (P18, Woman)*

**Emotional Defenses and Contextual Integrity.** Many defensive strategies used by participants involved the defense of emotional well-being, rather than the hiding of information or prevention of attacks. At its simplest, some participants (4/18) reported ignoring comments on social-good oriented posts. One filtered with whom they discussed politics:

> *I tend to avoid talking about it with specific people. And often with strangers I avoid it. With people I know and trust, yeah, I'll let them know, and I will sometimes argue. (P13, Non-binary/genderfluid person)*

In a form of contextual integrity, participants (2/18) also described "compartmentalizing" highly visible activities:

> *So when I'm doing something more public, it'll be something like in a specific community. I mentioned cosplay [4] is one that I feel relatively safe in putting gender stuff out there. Less so with activism, so I don't tend to put something in the same post about my gender and the activism I'm doing. It's more like my gender and the art I'm doing for visibility. So I guess compartmentalizing it like that. (P15, Non-binary person)*

This participant cross-posted activist and gender content from the same account, but not as part of the same post. Others entirely isolated political or activist accounts.

Another participant posted sensitive information publicly as long as responses were respectful and didn't "trigger verbal violence (P8, Non-binary person). One also worried about responses to posts, but feared frequent uncomfortable conversations even if they were not directly abusive:

> *"...talking about [transitioning] online did feel a little either riskier or more unwieldy, like is this going to lead to more conversations that I do not feel like having with these people? Who I know I don't owe any information to..." (P17, Genderqueer person)*

P7 outlined subtle norms of "creepiness" related to being partially out. Their LinkedIn profile used their deadname, but peers knew them only under their current name. P7 said that LinkedIn requests by peers therefore violated a social norm because it showed that they had "looked at an aspect of [me] that I didn't tell them about." (P7, Non-binary person)

**Opting Out.** Some participants (3/18) described people who choose not to be politically active online, despite engaging in activism in real life. Other participants (3/18) defend against concerns of photographs and identification at protests by opting out political events. These participants choose not to engage in certain types of political action they might otherwise engage in because of fears about privacy.

> *I don't go to protests because I think that will lead to more people potentially capturing pictures of me and portraying me in ways that are skewed towards [being outed]. (P7, Non-binary person)*

#### Privilege and Discrimination in the Queer Community

Participants noted instances of differential privilege and marginalization within the queer and trans community, creating additional challenges for trans people of color, those with disabilities, and those on other axes of marginalization.

Several participants (3/18) discussed "Queer Exchange" Facebook groups, where LGBTQ people exchange advice, goods, and services. However, several participants (2/18) perceived these groups to be problematic because of challenges relating to privilege and marginalization. Instead, they opted to join specialized groups that branched off from the general LGBTQ group. One participant of color said:

> *. . . [Queer, Trans, and People of Color is] the same concept[,] but its more secure because [Queer Exchange is] run by white people. Sometimes they'll push their privilege onto people of color. (P18, Woman)*

Others had the same perception. One participant describing the local group for a large city said:

> *It turned into some people decided they needed to police everything. Sometimes [policing] politics, sometimes [policing] wanting to move to a different part of the city, being yelled at for being gentrifiers... it's like no, I'm poor, queer, and disabled: That's where I have to go. And people would just attack you [based on life choices]. It was vicious. (P11, Non-binary person)*

One participant described feeling alienated in the queer community for holding less common or more marginalized queer identities, such as being non-binary, being asexual, or for engaging in consensual non-monogamy:

> *Pretty much every aspect of myself[...] [falls in] liminal spaces that make it hard for me to really find community and solidarity. So, being non-binary, being genderfluid, I'm not exactly a man or a woman. [...] And then, you know, being asexual, being poly, being pan, straight and gay spaces kind of elude me, and that's a story that a lot of people talk about, but it's definitely a thing. (P13, Non-binary/genderfluid person)*

Differential privilege also motivated participants, including one participant with greater privilege, to be more active and visible in order to support, represent, and empower those more marginalized. They identifying as "white[...], upper middle class, and well-educated" explained:

> *I also feel a strong responsibility to my larger community and communities to be visible and be willing to amplify*

[4] "The practice of dressing up as a character from a film, book, or video game, especially one from the Japanese genres of manga or anime."(https://en.oxforddictionaries.com/definition/cosplay)

*the voices of other folks who cannot be as visible. (P17, Genderqueer person)*

## DISCUSSION

In this section, we discuss the broader implications of our findings by exploring several aspects of broad design lessons and challenges we uncovered, and conclude by discussing specific technologies that emerge from our research.

### Risk Models Create Challenges

We infer three categories of risk model: **visibility**, **identity**, and **luck**, from our participants' explanations of how they assess vulnerability and choose to use technology and defenses. Our analysis suggests that applications of these models can create challenges, including loss of self-efficacy and feelings of hopelessness, and that a combination of these psychological effects with the internal logic of these models may induce choices to opt out of technologies and defenses, thus sacrificing benefits. We do not imply that each individual uses only one risk model; each person's perception of risk may involve features of each, and a person may apply different types of analyses in different situations. Our findings suggest that transgender people may be more likely to apply these models in ways that cause the challenges we describe. We focus our analyses on users' perceived risk models, not their accuracy. While their accuracy is an important topic for future research, in our analyses of their potential effects, even an inaccurate risk model influences the choices of our participants.

Participants employing **visibility-centered models** emphasized that vulnerability emerges from being "interesting" to adversaries. They saw engaging visibly in activism while being transgender as a dominant risk factor, since it controlled their level of visibility, and thus their level of interest, to attackers. Examples include P11's self-censorship to avoid "attract[ing] people's attention to me", and P7's analysis that "nobody's ever wanted to bother me" because they are "so private". This model implies significant self-efficacy [5], since participants believed their actions controlled risk. However, it suggests that fault for compromise and violation may lie with victims, promoting victim-blaming. Visibility models may also overemphasize targeted attacks; they assume an attacker pays individual attention to their victims. We observe that our results explore similar ground to Haimson's findings that transition bloggers reduced in self-disclosure, possibly as a form of self-censorship for safety, in the wake of political changes perceived as threatening to transgender people [30]. Visibility-based models may play a vital role in how trans people choose to balance the safety sought through self-censorship with the potential benefits of sharing transition information with sympathetic audiences [27] and the danger of reduced accomplishment of activist goals.

Some participants considered risk primarily a random phenomenon: P14 said: "you can become a target because a lot of it is so random." Such a **luck-based model** may reduce victim-blaming, but may also reduce self-efficacy. Trans people reasoning via luck may be less likely to deploy valuable defenses or make reasoned risk assessments and tradeoffs.

Others considered risk primarily a function of inherent characteristics, such as gender, transgender status, and race. P18 said that risk was "always gonna be about my gender and race", while P13, who is transmasculine, said "I worry more for trans women than myself". An **identity-based model** may reduce self-efficacy since identity characteristics are often immutable, and may make compromise and privacy violations feel inevitable. We saw that participants sometimes felt that they were subject to *differentiated* risks that are more powerful, dangerous, and targeted than those faced by the others: P12 made historical analogies to civil rights activists, stating that being out as trans might "make me more of a target for government monitoring".

#### *Overlaps with harm reduction*

Privacy research is commonly framed these days via impression management, contextual integrity, and context collapse. Goffman [23] discussed how individuals have different presentations that are selectively shown to peers. Nissenbaum [53] extended this to show how privacy could be reframed as the ability to separate information from one's different impressions to different people, for example, keeping information about one's personal life separate from one's work life. boyd et.al [48] then extended this with the concept of context collapse, in which privacy invasions can be interpreted as being unwarranted information from one context being seen in another context. Scheuerman et. al [58] presented harms that affect the transgender community, categorizing them into six different groups. In our work, we found significant overlap with several of the harms that they found, validating their findings while complimenting them through a privacy lens and analyzing and taxonomizing them through an orthogonal approach of risk models. Our findings help to relate past work on people's privacy to reduction of harm to transgender people, and help us to explore new ideas about how the modeling of risk might affect transgender people's behavior (e.g., deployment of security and privacy defenses).

#### *Risk Models May Induce Suboptimal Technology Use*

Our results suggest that risk models used may strongly influence trans people's use of technology. Models that may induce low self-efficacy (luck, identity) or which emphasize perceptions of differentiated, powerful, or targeted attacks (visibility, identity) may reduce motivation to deploy even effective defenses, leading to a greater risk of exposure. Meanwhile, models that encourage self-blame (visibility) may encourage people to avoid the use of technology altogether, forgoing its potentially significant benefits.

Several participants described low **self-efficacy** in situations we observed to be frequently related to luck- and identity-based risk models. Luck-based models emphasize randomness and de-emphasize causality, which may reduce perceptions of defensive behaviors as effective risk mitigation. Identity-based risk models similarly leave little room for action, since participants cannot change immutable identity-based characteristics that they perceive to drive their risk. Our

[5] Self-efficacy refers to an individual's belief in their capacity to execute behaviors necessary to produce specific performance attainments [11]

results suggest that these risk models may be linked to self-efficacy, and that self-efficacy may be linked to users who "give up" on security and privacy, opening themselves to further risk. For example, they may be more vulnerable to *privacy fatigue* [39], in which complexity and low usability of privacy controls induce the sharing of more private information, if they begin with lesser faith in their ability to protect themselves. Future work should further study the relationship between risk perception, self-efficacy, and defensive behaviors. Our results suggest particularly salience of these concerns for transgender people due to their marginalized status and their perceptions of differential and targeted risk. There may be a gap in the deployment of defensive techniques by some transgender people, suggesting that design and nudges which induce self-efficacy may be able to narrow this gap. Self-efficacy has been found to influence compliance with corporate security policies [10] significantly, and we suggest that for a marginalized individual protecting personal privacy, the influence of self-efficacy may even be stronger, making it high-leverage for encouraging secure behaviors.

Visibility models may increase self-efficacy by explaining risk as caused by one's own choices to be a visible target. They may also cause **self-blame**, since the person could have taken actions to lower their profile (e.g., not engaging in activism). For many negative life events, **self-blame** correlates with greater self-efficacy [35], providing motivation to deploy defenses. However, in cases of sexual assault, self-blame is not generally adaptive [61]. Recalling transgender people's particular vulnerability to sexual violence [37], it is unclear in which situations self-blame and visibility-based models might be (mal)adaptive for transgender people and activists. Our results suggest that visibility models may sometimes induce very conservative risk avoidance, such as among participants who said they entirely avoid the use of technology for political speech. This opting-out is likely to deny significant benefits of technology to both communities and individuals. Therefore, design and communication approaches that encourage self-efficacy without inducing self-blame are likely the best approach to producing a balanced approach to reducing risk among transgender people.

### Comparing With Other Marginalized Groups

Transgender people are disproportionately likely to be of low socioeconomic status (SES), homeless, and/or survivors of sexual violence and intimate partner violence (IPV) [37] People of low SES are more often victims of security and privacy violations [46], face greater "networked privacy" and algorithmic bias challenges [47, 60], and have lower levels of confidence around security [46]. Intersectionally, low confidence may combine with transgender-specific factors, multiplying the importance of self-efficacy. Low SES people's primary computing devices are often mobile devices, suggesting that improving mobile tools and UX could improve security for transgender people as well. We observe that relying heavily on mobile devices could backfire for young, closeted transgender people, who, similarly to survivors of IPV [19, 49] and low income New Yorkers of color [17], may be particularly vulnerable because they live with roommates or family members who may own or have physical control of their devices. We suggest considering whether features which ease and secure the use of public terminals may be beneficial across these groups. We also suggest that Elliott's recommendations [17] to more clearly articulate value propositions for security tools to be extended to those that offer benefits for specific populations, since we find that trans activists perceive targeted dangers similarly to civil rights activists of color, and that transgender people of color are more endangered in real life, thus having a higher risk perception.

While trans people share many such concerns, we discuss two differences. First, as P18 said regarding her race and gender, intersections of multiple identities lead to new concerns. For example, a low SES transgender person may find it harder to access resources due to discrimination or trans-specific targeting. Second, trans people, and especially trans activists, may have unique privacy needs specific to their transgender status, e.g., comparing transgender contextual integrity norms to those of other groups. IPV survivors might hold norms of strict confidentiality around denying abusers access to behavioral information, such as content and metadata of texts, calls, pictures, and location [19]. Our results reveal that trans norms may include publicly sharing privacy-sensitive personal characteristics such as former or legal names and gender markers [4], medical information, and old pictures. Sometimes private information is shared publicly for empowerment, role-modeling, and representation. At other times, it is shared for practical reasons, such as P7's LinkedIn profile under their legal name. Many participants expressed principles related to respect: sharing private information publicly was acceptable if audiences used and responded to that information respectfully. Respect, we infer from our participants, often corresponds to following norms from transgender culture, such as avoiding the use of deadnames. For example, P7 found it creepy when a peer they knew in real life contacted their deadname-using LinkedIn, because they felt it violated this cultural norm and thus constituted a privacy violation. We suggest that systems should provide tools for online communities to express and encourage such norms. One example of such design is found in the gaming streaming service Twitch, which allows streamers to write customized "Chat Rules" which are shown to first-time viewers as a nudge to which they must agree before chatting in that stream, allowing individual streamers to articulate their privacy norms. We encourage designers to explore other similar opportunities, such as detecting deadnames and reminding users to reconsider their use, to help translate community norms into adequate privacy in the face of public sharing.

### Design Possibilities

We illustrate applications of our results and design lessons by exploring design of two technologies informed by our results.

#### *Differentiated Defense for Differentiated Risk Models*

Participants often described a high-risk self-perception, wondering if bad things happened because they were trans, or, as activists, if trans status increased their chances of being targeted by government surveillance. We suspect these perceptions are accurate in some domains and unwarranted in others. Future work should explore where real vulnerability

is higher for the transgender population and where it is not to help both the population and designers respond appropriately to actual threats with realistic threat models.

Given the reality and perception of differential risk profiles, transgender people, and in particular transgender activists, may find significant practical and psychological benefits from differentiated security programs such as Google's Advanced Protection Program (APP), an opt-in higher level of security for "anyone at risk of targeted attacks", such as "activists" [24]. More systems should consider adopting defensive models of lower and higher security and analyze which populations should be enrolled. To understand the design of such systems, we advise researchers and companies to explore the threat models held by groups, such as transgender people, who view themselves as targets. In a social system, we imagine such a differentiated system providing a higher level of privacy protection for those vulnerable to harassment, doxxing, and outing on the internet by increasing the level of human review on posts related to accounts held by members of vulnerable population; setting secure defaults for privacy settings; or enabling increased protection measures against hacking and phishing attacks.

Differentiated security and privacy systems might mitigate real threats for trans people. They may also support self-efficacy. An extraordinary defensive program may be seen as an answer to extraordinary risk, one that restores confidence and encourages the deployment of defenses and use of technology for meaningful purposes. Future research in this area should examine actual risk profiles for marginalized populations; explore differentiated security models' ability to respond to those risk profiles; and determine whether differentiated programs can overcome self-efficacy deficits. For example, while journalists and activists are subject to targeted account compromise, transgender people may be subject to targeted harassment, which likely requires different, but potentially still differentiated, defenses to mitigate.

#### *Privacy-Preserving Ways to Prove Identity Traits*

P18 moderated a Facebook group exclusive to trans people of color and discussed membership management challenges involved in the ad-hoc screening of applicants. Drawing on our findings, we consider here ideas for the design of a system aimed to make the applicant screening process for a closed-membership group both secure and privacy-preserving. We believe that the system would have these requirements:

a) Allow people to voluntarily prove that they possess identity characteristics, such as race, ethnicity, or transgender status to others; we infer this requirement from participants who described groups limited to those with shared identity characteristics.
b) Protect identity characteristics and group membership from accidental disclosure, adversarial theft, and mass compromise; we infer this requirement from the sensitive nature of characteristics such as transgender status, but also from our participant's claim that she feared active infiltration by ICE agents, suggesting that users will trust the system only if they feel that it defends against such powerful adversaries. Our findings may suggest a peer-to-peer system, or one that lacks a centralized database in order to avoid having a single point of compromise.
c) Work with existing social networks and group administration systems; opening opportunities to use (e.g., via OAuth) existing infrastructure, but may also be limiting.

We imagine a system that would allow parties to request identity-characteristic proofs from one another based upon "endorsements" from other people in the system, not unlike a centralized system such as LinkedIn's skills endorsement system, or a traditional web-of-trust system from PKI cryptography. Importantly, the system would need to allow applicants to verify group administrators as the origin of requests.

There are significant cryptographic, technical and usability challenges to this system, just as there are for any attempts providing some notion of distributed trust. However, we believe that exploring the possibility of such a system, and especially exploring the perceived utility and trustworthiness of such a system in the eyes of marginalized activists, may be a fruitful direction. Such a project would involve an in-depth investigation of marginalized activists' practices and needs surrounding their audiences and communities, the results of which would lead to other important design directions as well.

### Limitations of this Study

Our sample is composed of people willing to share their experiences. Such people are unlikely to be "stealth", biasing our results toward people who are open about their trans status. While stealth people could have responded to our recruitment, none of our participants said they are stealth now or plan to be in the future. This limitation is hard to avoid in studies of transgender people generally. Recruitment was focused on maximizing diversity (racial, SES, student/not-student, etc.), but was limited by geography and is not representative of any specific population. Our future work will include quantitative research with a more geographically diverse pool.

## CONCLUSION

Trans people are a marginalized population often engaged in activist and prosocial behavior to strengthen their communities and the broader world. Whether explicitly political or intensely individual, this work often uses technology, amplifying the computer security and privacy concerns that they face. In this work, we interviewed transgender participants who repeatedly returned to themes of activism and prosocial behavior, leading us to focus on the analysis of these crucial concerns. We characterized their goals and challenges; compared them to other marginalized groups; described a taxonomy of their risk models; analyzed those models for their effects on self-efficacy, deployment of defenses, and use of technology for these critical, sensitive purposes; and concluded by applying our lessons to design opportunities for specific technologies which would benefit trans people's abilities to maintain their well-being and enact positive social change.

### Acknowledgements

The authors would like to thank Isabel Ehrhardt, Nicole Gates, and Aidan Kidder-Wolff for their assistance with interviews and analysis. This research was possible through funding provided by Oberlin College and Wellesley College.

## REFERENCES


[1] Alex A. Ahmed, Teresa Almeida, Judeth Oden Choi, Jon Pincus, and Kelly Ireland. 2018. What's at Issue: Sex, Stigma, and Politics in ACM Publishing. In *Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems (CHI EA '18)*. ACM, New York, NY, USA, Article alt07, 10 pages.

[2] Tousif Ahmed, Roberto Hoyle, Kay Connelly, David Crandall, and Apu Kapadia. 2015. Privacy concerns and behaviors of people with visual impairments. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI '15)*. ACM, New York, NY, USA, 3523–3532.

[3] Tousif Ahmed, Roberto Hoyle, Patrick Shaffer, Kay Connelly, David Crandall, and Apu Kapadia. 2017. Understanding the Physical Safety, Security, and Privacy Concerns of People with Visual Impairments. *IEEE Internet Computing* 21, 3 (May/June 2017), 56–63.

[4] Kevin L Ard and Harvey J Makadon. 2011. Addressing Intimate Partner Violence in Lesbian, Gay, Bisexual, and Transgender Patients. *Journal of General Internal Medicine* 26, 8 (March 2011), 930–933.

[5] Shiri Azenkot, Kyle Rector, Richard Ladner, and Jacob Wobbrock. 2012. PassChords: secure multi-touch authentication for blind people. In *Proceedings of the 14th international ACM SIGACCESS conference on Computers and accessibility (ASSETS '12)*. ACM, New York, NY, USA, 159–166.

[6] MV Lee Badgett, Laura E Durso, and Alyssa Schneebaum. 2013. New patterns of poverty in the lesbian, gay, and bisexual community. (2013).

[7] Rosanna Bellini, Angelika Strohmayer, Ebtisam Alabdulqader, Alex A. Ahmed, Katta Spiel, Shaowen Bardzell, and Madeline Balaam. 2018. Feminist HCI: Taking Stock, Moving Forward, and Engaging Community. In *Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems (CHI EA '18)*. ACM, New York, NY, USA, Article SIG02, 4 pages.

[8] Lindsay Blackwell, Jean Hardy, Tawfiq Ammari, Tiffany Veinot, Cliff Lampe, and Sarita Schoenebeck. 2016. LGBT parents and social media: Advocacy, privacy, and disclosure during shifting social movements. In *Proceedings of the 2016 CHI conference on human factors in computing systems (CHI '16)*. ACM, New York, NY, USA, 610–622.

[9] Erin Brady, Meredith Ringel Morris, Yu Zhong, Samuel White, and Jeffrey P Bigham. 2013. Visual challenges in the everyday lives of blind people. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '13)*. ACM, New York, NY, USA, 2117–2126.

[10] Burcu Bulgurcu, Hasan Cavusoglu, and Izak Benbasat. 2010. Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS quarterly* 34, 3 (2010), 523–548.

[11] Michael P Carey and Andrew D Forsyth. 2019. Teaching Tip Sheet: Self-Efficacy. (2019). `https://www.apa.org/pi/aids/resources/education/self-efficacy` Accessed 17-December-2019.

[12] Matthew Carrasco and Andruid Kerne. 2018. Queer Visibility: Supporting LGBT+ Selective Visibility on Social Media. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (CHI '18)*. ACM, New York, NY, USA, 250.

[13] Anthony D'Augelli. 1998. Lesbian, gay, and bisexual youth and their families: disclosure of sexual orientation and its consequences. In *American Journal of Orthopsychiatry*, Vol. 68.

[14] Michael A DeVito, Ashley Marie Walker, and Jeremy Birnholtz. 2018. 'Too Gay for Facebook' Presenting LGBTQ+ Identity Throughout the Personal Social Media Ecosystem. *Proceedings of the ACM on Human-Computer Interaction* Vol. 2, CSCW (Nov. 2018), 1–23.

[15] Franco Dispenza, Laurel B Watson, Y Barry Chung, and Greg Brack. 2012. Experience of career-related discrimination for female-to-male transgender persons: A qualitative study. *The Career Development Quarterly* 60, 1 (March 2012), 65–81.

[16] Stefanie Duguay. 2016. "He has a way gayer Facebook than I do": Investigating sexual identity disclosure and context collapse on a social networking site. *New Media & Society* 18, 6 (2016), 891–907.

[17] Ame Elliott and Sara Brody. 2015. Straight Talk: New Yorkers On Mobile Messaging And Implications For Privacy. (2015), 13.

[18] Jesse Fox and Rachel Ralston. 2016. Queer identity online: Informal learning and teaching experiences of LGBTQ individuals on social media. *Computers in Human Behavior* 65 (Dec 2016), 635–642.

[19] Diana Freed, Jackeline Palmer, Diana Minchala, Karen Levy, Thomas Ristenpart, and Nicola Dell. 2018. "A Stalker's Paradise": How Intimate Partner Abusers Exploit Technology. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (CHI '18)*. ACM, New York, NY, USA, 667.

[20] Samantha Friedman, Angela Reynolds, Susan Scovill, Florence Brassier, Ron Campbell, and McKenzie Ballou. 2013. An estimate of housing discrimination against same-sex couples. (2013).

[21] Lesbian Gay, Straight Education Network, and others. 2013. Out online: The experiences of lesbian, gay, bisexual and transgender youth on the Internet. (2013). `https://www.glsen.org/news/out-online-experiences-lgbt-youth-internet` Accessed 17-December-2019.

[22] GLAAD. 2018. Glossary of Terms - Transgender. (2018). `https://www.glaad.org/reference/transgender` Accessed 17-December-2019.

[23] Erving Goffman. 1956. *The presentation of self in everyday life*. Anchor Books, New York, New York.

[24] Google. 2019. Advanced Protection Program. (2019). https://landing.google.com/advancedprotection/. Accessed 17-December-2019.

[25] Jaime M Grant, Lisa Mottet, Justin Edward Tanis, Jack Harrison, Jody Herman, and Mara Keisling. 2011. Injustice at every turn: A report of the national transgender discrimination survey. (2011).

[26] Ann P Haas, Philip L Rodgers, and Jody L Herman. 2014. Suicide attempts among transgender and gender non-conforming adults. *work* 50 (2014), 59.

[27] Oliver L Haimson. 2019. Mapping gender transition sentiment patterns via social media data: toward decreasing transgender mental health disparities. *Journal of the American Medical Informatics Association* (2019).

[28] Oliver L Haimson, Jed R Brubaker, Lynn Dombrowski, and Gillian R Hayes. 2015. Disclosure, stress, and support during gender transition on Facebook. In *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing (CSCW '15)*. ACM, New York, NY, USA, 1176–1190.

[29] Oliver L Haimson, Jed R Brubaker, Lynn Dombrowski, and Gillian R Hayes. 2016. Digital footprints and changing networks during online identity transitions. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems (CHI '16)*. ACM, New York, NY, USA, 2895–2907.

[30] Oliver L Haimson and Gillian R Hayes. 2017. Changes in social media affect, disclosure, and sociality for a sample of transgender Americans in 2016's political climate. In *Proceedings of Eleventh International AAAI Conference on Web and Social Media (ICWSM '17)*. The AAAI Press.

[31] Oliver L Haimson and Anna Lauren Hoffmann. 2016. Constructing and enforcing" authentic" identity online: Facebook, real names, and non-normative identities. *First Monday* 21, 6 (2016).

[32] Foad Hamidi, Morgan Klaus Scheuerman, and Stacy M Branham. 2018. Gender Recognition or Gender Reductionism?: The Social Implications of Embedded Gender Recognition Systems. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (CHI '18)*. ACM, New York, NY, USA, 8.

[33] Md Munirul Haque, Shams Zawoad, and Ragib Hasan. 2013. Secure techniques and methods for authenticating visually impaired mobile phone users. In *2013 IEEE International Conference on Technologies for Homeland Security (HST)*. IEEE, 735–740.

[34] Amanda Holpuch. 2014. Victory for drag queens as Facebook apologises for 'real-name' policy. (2014). https://www.theguardian.com/technology/2014/oct/01/victory-drag-queens-facebook-apologises-real-name-policy Accessed 17-December-2019.

[35] Stephanie Ann Hooker. 2013. *Self-Blame*. Springer New York, New York, NY, 1731–1732.

[36] Farnaz Irannejad Bisafar, Lina Itzel Martinez, and Andrea G Parker. 2018. Social Computing-Driven Activism in Youth Empowerment Organizations: Challenges and Opportunities. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (CHI '18)*. ACM, New York, NY, USA, 183.

[37] Sandy E James and Jody Herman. 2017. The Report of the 2015 US Transgender Survey: Executive Summary. (2017).

[38] Shanna K. Kattari, Darren L. Whitfield, N. Eugene Walls, Lisa Langenderfer-Magruder, and Daniel Ramos. 2016. Policing Gender Through Housing and Employment Discrimination: Comparison of Discrimination Experiences of Transgender and Cisgender LGBQ Individuals. *Journal of the Society for Social Work and Research* 7, 3 (Sept. 2016), 427–447.

[39] Mark J Keith, Courtenay Maynes, Paul Benjamin Lowry, and Jeffry Babb. 2014. Privacy fatigue: The effect of privacy control complexity on consumer electronic information disclosure. In *International Conference on Information Systems (ICIS 2014), Auckland, New Zealand, December*. 14–17.

[40] Ronald C Kessler, Guilherme Borges, and Ellen E Walters. 1999. Prevalence of and risk factors for lifetime suicide attempts in the National Comorbidity Survey. *Archives of general psychiatry* 56, 7 (1999), 617–626.

[41] Alex S Keuroghlian, Derri Shtasel, and Ellen L Bassuk. 2014. Out on the street: a public health and policy agenda for lesbian, gay, bisexual, and transgender youth who are homeless. *American Journal of Orthopsychiatry* 84, 1 (2014), 66.

[42] Joseph G. Kosciw, Neal A. Palmer, and Ryan M. Kull. 2014. Reflecting Resiliency: Openness About Sexual Orientation and/or Gender Identity and Its Relationship to Well-Being and Educational Outcomes for LGBT Students. *American Journal of Community Psychology* 55, 1-2 (April 2014), 167–178.

[43] lamblint (Urban Dictionary user). 2017. Truscum. (2017). https://www.urbandictionary.com/define.php?term=truscum Accessed 17-December-2019.

[44] Hanlin Li, Disha Bora, Sagar Salvi, and Erin Brady. 2018. Slacktivists or Activists?: Identity Work in the Virtual Disability March. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (CHI '18)*. ACM, New York, NY, USA, Article 225, 13 pages.

[45] Emilia L Lombardi, Riki Anne Wilchins, Dana Priesing, and Diana Malouf. 2002. Gender violence: Transgender experiences with violence and discrimination. *Journal of homosexuality* 42, 1 (2002), 89–101.

[46] Mary Madden. 2017. Privacy, Security, and Digital Inequality. (2017).

[47] Mary Madden, Michele Gilman, Karen Levy, and Alice Marwick. 2017. Privacy, poverty, and big data: A matrix of vulnerabilities for poor Americans. *Wash. UL Rev.* 95 (2017), 53.

[48] Alice E. Marwick and danah boyd. 2010. I tweet honestly, I tweet passionately: Twitter users, context collapse, and the imagined audience. *New Media & Society* 13, 1 (July 2010), 114–133.

[49] Tara Matthews, Kathleen O'Leary, Anna Turner, Manya Sleeper, Jill Palzkill Woelfer, Martin Shelton, Cori Manthorne, Elizabeth F Churchill, and Sunny Consolvo. 2017. Stories from survivors: Privacy & security practices when coping with intimate partner abuse. In *Proceedings of the 2017 Conference on Interaction Design and Children (IDC '17)*. ACM, New York, NY, USA.

[50] Lydia Michie, Madeline Balaam, John McCarthy, Timur Osadchiy, and Kellie Morrissey. 2018. From her story, to our story: Digital storytelling as public engagement around abortion rights advocacy in Ireland. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (CHI '18)*. ACM, New York, NY, USA, 357.

[51] Brian Mustanski, Rebecca Andrews, and Jae A. Puckett. 2016. The Effects of Cumulative Victimization on Mental Health Among Lesbian, Gay, Bisexual, and Transgender Adolescents and Young Adults. *American Journal of Public Health* 106, 3 (March 2016).

[52] Brian Mustanski, Michael Newcomb, and Robert Garofalo. 2011. Mental health of lesbian, gay, and bisexual youth: A developmental resiliency perspective. *Journal of Gay & Lesbian Social Services* 23, 2 (Jan. 2011).

[53] Helen Nissenbaum. 79. *Privacy as Contextual Integrity*. Washington Law Review.

[54] Matthew K Nock and Ronald C Kessler. 2006. Prevalence of and risk factors for suicide attempts versus suicide gestures: analysis of the National Comorbidity Survey. *Journal of abnormal psychology* 115, 3 (2006), 616.

[55] ProPublica. 2019. When Transgender Travelers Walk Into Scanners, Invasive Searches Sometimes Wait on the Other Side. (2019). `https://www.propublica.org/article/tsa-transgender-travelers-scanners-invasive-searches\\-often-wait-on-the-other-side` Accessed 17-December-2019.

[56] Marcus Renner and Ellen Taylor-Powell. 2003. Analyzing qualitative data. *Programme Development & Evaluation, University of Wisconsin-Extension Cooperative Extension* (2003), 1–10.

[57] Johnny Saldaña. 2015. *The coding manual for qualitative researchers*. Sage.

[58] Morgan Klaus Scheuerman, Stacy M. Branham, and Foad Hamidi. 2018. Safe Spaces and Safe Places: Unpacking Technology-Mediated Experiences of Safety and Harm with Transgender People. *Proceedings of the ACM on Human-Computer Interaction* 2, CSCW, Article 155 (Nov. 2018), 27 pages.

[59] Katie A Siek, Yvonne Rogers, and Kay H Connelly. 2005. Fat finger worries: how older and younger users physically interact with PDAs. In *IFIP Conference on Human-Computer Interaction (INTERACT '05)*. Springer, 267–280.

[60] Janaki Srinivasan, Savita Bailur, Emrys Schoemaker, and Sarita Seshagiri. 2018. Privacy at the margins| The poverty of privacy: Understanding privacy trade-offs from identity infrastructure users in India. *International Journal of Communication* 12 (2018), 20.

[61] Sarah E Ullman. 1996. Social reactions, coping strategies, and self-blame attributions in adjustment to sexual assault. *Psychology of women quarterly* 20, 4 (1996), 505–526.

[62] Stephen Whittle. 1998. The trans-cyberian mail way. *Social & Legal Studies* 7, 3 (1998), 389–408.

[63] Pamela Wisniewski, Heng Xu, Mary Beth Rosson, Daniel F. Perkins, and John M. Carroll. 2016. Dear Diary: Teens Reflect on Their Weekly Online Risk Experiences. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems (CHI '16)*. ACM, New York, NY, USA, 3919–3930.

[64] Pamela J Wisniewski, Heng Xu, Mary Beth Rosson, and John M Carroll. 2014. Adolescent online safety: The "Moral" of the Story. In *Proceedings of the 17th ACM conference on Computer supported cooperative work & social computing (CSCW '14)*. ACM, New York, New York, USA, 1258–1271.

[65] Shaomei Wu and Lada A Adamic. 2014. Visually impaired users on an online social network. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '14)*. ACM, New York, NY, USA, 3133–3142.

[66] Jillian C York and Dia Kayyali. 2014. Facebook's 'Real Name' Policy Can Cause Real-World Harm for the LGBTQ Community. (2014). `https://www.eff.org/deeplinks/2014/09/facebooks-real-name-policy-can-cause-real-world-\\harm-lgbtq-community` Accessed 17-December-2019.