Trauma-Informed Computing: Towards Safer Technology Experiences for All

Niu X. Chen*
Information Science
Cornell University
Ithaca, NY, USA

Allison McDonald*
Computer Science and Engineering
University of Michigan
Ann Arbor, MI, USA

Yixin Zou*
School of Information
University of Michigan
Ann Arbor, MI, USA

Emily Tseng
Information Science
Cornell University
New York, NY, USA

Kevin Roundy
NortonLifeLock Research Group
Culver City, CA, USA

Acar Tamersoy
NortonLifeLock Research Group
Culver City, CA, USA

Florian Schaub
School of Information
University of Michigan
Ann Arbor, MI, USA

Thomas Ristenpart
Computer Science
Cornell Tech
New York, NY, USA

Nicola Dell
Information Science
The Jacobs Institute, Cornell Tech
New York, NY, USA

ABSTRACT

Trauma is the physical, emotional, or psychological harm caused by deeply distressing experiences. Research with communities that may experience high rates of trauma has shown that digital technologies can create or exacerbate traumatic experiences. Via three vignettes, we discuss how considering the possible effects of trauma and traumatic stress reactions provides an explanatory lens with new insights into people's technology experiences. Then, we present a framework—trauma-informed computing—in which we adapt and show how to apply six key principles of trauma-informed approaches to computing: safety, trust, peer support, collaboration, enablement, and intersectionality. Through specific examples, we describe how to apply trauma-informed computing in four areas of computing research and practice: user experience research & design, security & privacy, artificial intelligence & machine learning, and organizational culture in tech companies. We conclude by discussing how adopting trauma-informed computing will lead to benefits for all users, not only those experiencing trauma.

CCS CONCEPTS

• **Human-centered computing** → **Empirical studies in HCI**; • **Security and privacy** → **Social aspects of security and privacy**;

KEYWORDS

trauma; trauma-informed computing; intimate partner violence; transgender; gender-based violence; computer security and privacy

ACM Reference Format:
Niu X. Chen, Allison McDonald, Yixin Zou, Emily Tseng, Kevin Roundy, Acar Tamersoy, Florian Schaub, Thomas Ristenpart, and Nicola Dell. 2022. Trauma-Informed Computing: Towards Safer Technology Experiences for All. In *CHI Conference on Human Factors in Computing Systems (CHI '22), April 29-May 5, 2022, New Orleans, LA, USA.* ACM, New York, NY, USA, 20 pages. https://doi.org/10.1145/3491102.3517475

Content Warning. This paper contains descriptions of intimate partner violence, digital abuse, racial violence, police brutality, and mental health topics including PTSD and trauma.

1 INTRODUCTION

Trauma is the experience and resulting aftermath of an extremely distressing event or series of events, such as disaster, violence, abuse, or other emotionally harmful experiences [183]. Traumatic experiences are unfortunately widespread, with reports suggesting that almost 70% of people experience at least one traumatic event in their lifetimes [128]. Trauma frequently has long-lasting adverse effects on people's lives, careers, and mental, physical, social, or emotional well-being. As explained by van der Kolk [42], trauma leaves traces on *"our minds and emotions, on our capacity for joy and intimacy, and even on our biology and immune systems."*

Although trauma may seem far from the typical concerns of technology developers or user experience (UX) professionals, the prevalence of trauma suggests that billions of technology users are trauma survivors. In addition, a growing amount of HCI research has engaged directly with high-risk or marginalized communities that are known to experience high rates of trauma; examples include survivors of intimate partner violence (IPV) [6, 56, 109], sex workers [8, 111, 181], transgender, non-binary, and other LGBTQ+ people [71, 88, 96], racial minorities [49, 130, 194], people who experience the death of a loved one [3, 28, 107], and more. However, to

*Niu X. Chen, Allison McDonald, and Yixin Zou contributed equally to this research.

CHI '22, April 29-May 5, 2022, New Orleans, LA, USA

ACM ISBN 978-1-4503-9157-3/22/04…$15.00
https://doi.org/10.1145/3491102.3517475

the best of our knowledge, there has been no cohesive accounting of the role of trauma in people's interactions with technology and what, if anything, those responsible for the design, deployment, and support of digital technologies should do to account for the potential effects of trauma.

Our paper begins by investigating how trauma may impact people's technology experiences via three vignettes about communities that are known to have high rates of trauma—survivors of (IPV), people undergoing gender transition, and victims of identity theft. These vignettes demonstrate how technology may directly facilitate trauma (e.g., IPV survivors being stalked via spyware, transgender people being outed due to algorithmic recommendations), as well as how technology may unintentionally retraumatize people (e.g., everyday security notifications triggering a trauma response). User behaviors that may otherwise be difficult to understand—such as excessive frustration, fear, anxiety, or helplessness—may in fact be well-known traumatic stress reactions documented in medical and public health literature [25, 42, 184]. Considering the possible impact of trauma provides new insights that improve our understanding of people's technology interactions. For example, heightened anxiety or hypervigilance may prompt survivors to associate benign software behavior with malicious intent. Of course, traumatic interactions with technology are not necessarily worse, or more important than other types of physical, emotional, or psychological trauma. Rather, technology experiences that may elicit trauma responses happen *on top of* other kinds of trauma, potentially exacerbating their harms. Taken together, our vignettes show how considering trauma and its potential effects on people's behaviors and experiences challenges the concept of "expected" or "normal" user experience, and delivers insights not achievable when the potential effects of trauma are ignored.

Knowing that trauma can impact people's technology experiences, we then ask: how should we design computing systems in light of trauma? Social work and public health have developed extensive literature on how institutions such as schools [153], hospitals [132, 147], recovery centers [18, 74], child welfare services [72], domestic violence programs [94, 202], and others can be trauma-informed. According to the U.S. Substance Abuse and Mental Health Services Administration (SAMHSA) [183], an organization or process that is trauma-informed realizes the widespread impact of trauma, recognizes the signs of trauma, follows best practices to consider trauma, and seeks to avoid retraumatization. To clarify, *trauma-informed approaches are not trauma-specific*. It is not necessary—and could be actively harmful—to attempt to "diagnose" or "prove" evidence of trauma. Instead, by working to account for the possible effects of trauma in all interactions, trauma-informed approaches are widely considered to be generally beneficial for all people, regardless of whether they are trauma survivors [183].

In order to foreground the role of technology in trauma, as well as to emphasize the role technologists can play in building a safer digital world, we propose that *trauma-informed computing* be defined as an ongoing commitment to improving digital technologies by acknowledging trauma and its impact. Our framework recognizes that digital technologies can both cause and exacerbate trauma, and seeks out ways to avoid technology-related trauma and retraumatization. Avoiding retraumatization does *not* mean that computing researchers or practitioners without appropriate training should begin to ask about or actively encourage people to disclose traumatic experiences. Instead, we outline trauma-informed computing as an approach for improving technology while minimizing harm in all phases of technology design, development, and research.

Specifically, we adapt six key principles of trauma informed approaches described by SAMHSA [183]—safety, trust, collaboration, peer support, enablement, and intersectionality—to the design, development, deployment, and evaluation of computing systems. We discuss the application of our framework in four areas of computing research and practice: UX research and design, security and privacy, artificial intelligence and machine learning, and organizational culture in tech companies. For each area, we provide examples of adapting prevalent processes and artifacts to make them more trauma-informed. We conclude by highlighting that trauma-informed computing has to be an ongoing commitment to learning, reflecting, and applying trauma-informed principles, rather than a one-time checklist.

To summarize, our paper makes three key contributions: (1) a discussion of how trauma and traumatic stress reactions may impact—and be impacted by—people's experiences with technology; (2) a framework for trauma-informed computing, which adapts six key principles of trauma-informed approaches to technology design and development; and (3) an illustration of our framework's application in four areas of computing-related research and practice demonstrating how processes and artifacts could be made more trauma-informed.

2 BACKGROUND AND RELATED WORK

Trauma. Trauma is the experience and resulting aftermath of an extremely distressing event or series of events [183]. Every individual may experience a traumatic event differently, which leads to different types of adverse effects on mental, physical, social, emotional or spiritual well-being. Not every person who experiences something traumatic will be traumatized. However, for many people, trauma creates a "fundamental reorganization of the way mind and brain manage perception" [42]. Trauma often manifests in *traumatic stress reactions*, described by researchers as "normal human survival [instincts]" developed in response to the traumatic event(s) that serve to protect from further harms [25, 196]. Trauma reactions can happen during or after the traumatic event—sometimes persisting for months or years. Responses can manifest across multiple domains of a person's life [25, 184]: (1) *physically*, including trouble sleeping, hyperarousal of the nervous system, or extreme fatigue; (2) *emotionally*, including a diverse set of reactions spanning anxiety, grief, shame, and severe mood-swings; (3) *behaviorally*, for example, avoiding situations similar to the traumatic event or engaging in high-risk behaviors; (4) *cognitively*, which may include hypervigilance to threats, self-blame, flashbacks, intrusive thoughts, or difficulty making decisions; and (5) *existentially*, which may include hopelessness or cynicism, or alternatively renewed faith or increased confidence in one's own resilience. The traumatic stress reactions referred to throughout this paper are drawn from the Diagnostic and Statistical Manual of Mental Disorders (DSM-5) [184], the standard classification used by mental health professionals in the United States. Depending on the intensity and duration of trauma symptoms, some survivors may be formally

diagnosed with Post-Traumatic Stress Disorder (PTSD); however, many people who suffer from trauma may not receive a formal diagnosis [196]. In this paper, we refer to trauma broadly as any of the recognized trauma reactions that arise from distressing events.

Trauma-informed Approaches. In recent years, many advocacy organizations and public institutions have been working to adopt what are known as *trauma-informed approaches*. Taking a trauma-informed approach involves realizing the widespread impact of trauma, recognizing the signs of trauma, responding by updating best practices to consider trauma, and consciously working to minimize the potential for harm or retraumatization for all stakeholders, including service providers [25, 85, 183]. Importantly, implementing a trauma-informed approach does not require individuals to disclose their trauma or personal history; by assuming the prevalence of trauma and implementing trauma-informed principles in every area of work, trauma-informed approaches enhance "safety, control, and resilience" [145] for everyone involved.

Prior research has linked the importance of creating and applying trauma-informed approaches in many contexts: service delivery in mental health [22, 126], addiction [18, 36, 74], adverse childhood experiences [72, 132], IPV [94, 152, 199, 202], nursing [87, 126] and more. In particular, "SAMHSA's Concept of Trauma and Guidance for a Trauma-Informed Approach" [183] is is unique in its adaptability and adoption across many fields. SAMHSA integrated "trauma focused research work; practice-generated knowledge; and the lessons articulated by survivors of traumatic experiences who have had involvement in multiple service sectors" [183], as well as extensive feedback from experts, federal agencies, and public comments to create the manual. Unlike other context-specific frameworks [47, 97, 117], SAMHSA's framework was created with the intention of being adapted to "other sectors such as child welfare, education, criminal and juvenile justice...and other settings that have the potential to ease or exacerbate an individual's capacity to cope with traumatic experiences" [183]. Following its publication, research spanning social policy [16] to education [139] have used and cited SAMHSA's framework. Likewise, in our own computing research and practice, we found SAMHSA's principles to be the most relevant. Importantly, SAMHSA's framework focuses on the *awareness* of trauma as pervasive and impactful rather than *recovery*, which is the focus of many other frameworks. While recovering from trauma is crucial, we believe that trauma awareness is most relevant for general technology and interaction design. Directly addressing or facilitating recovery from past trauma should not be undertaken by technologists without further training and guidance.

We chose SAMHSA's framework to form the basis of the principles presented in this paper with computing-specific adaptations. SAMHSA's original principles are safety; trustworthiness and transparency; peer support; collaboration and mutuality; empowerment, voice, and choice; and cultural, historical, and gender issues. For each principle, we considered how it may apply and be useful for computing practitioners in their day-to-day contexts. For example, how might a researcher build trust with trauma survivors in conducting interviews? How might a security expert consider safety in threat modeling? As discussed in Section 4, we shortened these titles for clarity and brevity (e.g., "intersectionality" instead of "cultural, historical and gender issues"). In addition, we use "enablement" rather than SAMHSA's empowerment principle. Like empowerment, enablement focuses on actions to develop survivors' strengths on both an individual and organizational level, but without the implication that doing so creates a shift in power [45].

Trauma-related Research in HCI. A growing body of work in HCI considers how technology can be used to care for people with trauma. Several studies focus on how technology might serve patients experiencing PTSD or mental health professionals working with them, including in screening [168], therapy [124], and rehabilitation [48]. Evans et al. examine the ecologies of care for veterans with PTSD, exploring how clinicians, families, and friends can support mental well-being [51]. Other studies explore how therapy for PTSD can be supported by technologies such as conversational agents [124] and virtual reality [48, 123].

More broadly, HCI researchers have been interested in improving technology experiences for marginalized communities, many of whom experience high rates of trauma. Recent work has examined tech-related harms among people experiencing pregnancy loss [2, 3], racial minorities [49, 130], survivors of IPV [56, 109], refugees [171, 172], and non-binary or transgender people [71, 141, 163]. To these bodies of work, we contribute an overarching *trauma-informed computing framework* that considers how technology intersects with trauma across different contexts. With this framework, we hope to help researchers draw parallels between accounts of tech-enabled trauma that might otherwise seem unrelated.

In addition, past research has contributed frameworks for designing safer and more equitable technologies, including approaches that are justice-oriented [35, 45], consentful [82, 180], feminist [7], queer [100, 177], postcolonial [83] and allyship-based [99]. Other work has advanced critical race theory for HCI [130] and discussed how HCI can account for intersectionality in research and as a research community [49, 151]. Our *trauma-informed computing framework* is intended for use in concert with these approaches. While there is overlap between some principles in our framework and prior work (e.g., enablement in social justice-oriented design [45], intersectionality in critical race theory for HCI [130]), our framework builds on prior work by highlighting an *orientation* toward developing trauma-informed computing systems. This includes considering and applying the six principles outlined in our framework, but also having a fundamental *awareness* of the pervasive nature of trauma and the role technology can play in exacerbating or alleviating trauma. Similar to existing frameworks, we urge technologists to not only design computer systems that are sensitive to many users' needs, but also to acknowledge how larger systemic issues in computing and society at large can cause or exacerbate harm. Existing frameworks do not propose that more justice-oriented technology design approaches will solve the problems that people face [45]—similarly, we do not argue that trauma-informed computing will solve users' trauma. Instead, we hope our framework provides a productive starting point from which technologists can

mitigate tech-enabled harms, while working with affected communities to address structural conditions via policy and activism.

Positionality Statement. In line with past calls in HCI research [45, 99, 165], we reflect on how our work is influenced by our experiences and identities. Our motivation for this paper came from first-hand observations of how trauma-affected survivors interact with technology. We became interested in using trauma-informed approaches to better situate these unexpected experiences and came to realize how a trauma-informed approach might improve computing systems and benefit all technology users. Our team includes a mix of cisgender women and men, and a mix of academic researchers and industry practitioners. While our team members hold multicultural backgrounds from the United States, Canada, China, Germany, Turkey, Zimbabwe, and Taiwan, all are currently based in the United States. Thus, we primarily draw inspirations from trauma-related research conducted in the North American context. Our positioning as researchers and practitioners at Western institutions influence our cultural beliefs, attitudes, and epistemologies in conducting research around trauma-informed computing. Many of us directly engage or have engaged with trauma survivors in research and practice. Although none of us are mental health professionals, some have received trauma-informed training and applied it when working with survivors.

3 STORIES OF TRAUMA IN TECHNOLOGY EXPERIENCE

In this section, we present three vignettes to illustrate how technology and trauma can interact. We focus on three populations that are known to be highly traumatized and whose experiences with trauma are well-documented in prior work: survivors of intimate partner violence (IPV), people who go through gender transition, and people who experience identity theft. We begin each vignette with a brief background about the context, followed by a fictional vignette. The vignettes are based on existing literature, blog posts, news stories, and the authors' past experience working with these communities. The vignettes do not represent any one person's experience and are not meant to illustrate a representative experience; rather, we sought to highlight common examples of the emotional, psychological, and physical impacts of technology for people experiencing acute trauma.

We close this section with a discussion of how technology in each of these contexts can cause, exacerbate, or alter the way people experience trauma. In aggregate, these vignettes show how trauma might serve as a useful explanatory lens for understanding user interactions with technology.

3.1 Vignette: Intimate Partner Violence

IPV is a global health problem. One in four women and one in ten men report experiencing sexual, psychological, or physical violence such as stalking, aggression, and coercion from an intimate partner [175]. IPV can occur in all socioeconomic, cultural, and religious groups, but the "overwhelming global burden of IPV is borne by women" [133]. The consequences of IPV are severe, including mental and physical harms: survivors are more likely to suffer suicidal ideation, substance abuse, sleep disturbances, and depression [44]. Mertin and Mohr found that 40–60% of women IPV survivors suffer from PTSD and experience symptoms like flashbacks, nightmares, avoidance of triggers, and emotional numbing [115]. Other survivors who may not be formally diagnosed with PTSD nevertheless often experience PTSD symptoms [86].

Technology is a key but understudied aspect of IPV. Recent work shows that perpetrators of violence (or abusers) frequently use technology to harm their target [56, 109]. This may happen, for example, by installing spyware on the survivor's device, harassing them online, and compromising their accounts [56]. As more abuse is perpetrated via technology, the trauma resulting from the abuse will also inevitably be more intertwined with technology use.

The following fictional vignette is based on common experiences that IPV survivors have described, including in academic literature [56, 109] and in the authors' experiences working with IPV survivors. Several authors have years of experience meeting with survivors to help them navigate tech abuse and conducting research in this domain. Collectively, they have heard dozens of stories similar to the one presented below.

Jamie trusted her partner with managing all the technologies in their house, including her phone and email accounts. After all, she did not feel tech-savvy, and her partner was a software engineer. However, over several years of their marriage, her partner increasingly watched and sought to control her. He would demand to know why she took a certain bus route or talked to a particular coworker. He would accuse her of cheating on him, and demand that she unlock her phone to prove to him that she was not. Soon she realized he was logging into her social media accounts and reading all her private messages. Jamie became increasingly scared that her partner could see her every click and keystroke. She often froze in uncertainty while trying to use the computer even for everyday tasks. She also avoided using her devices to search for advice and support. Eventually, she left him, moving out of their apartment and briefly into a domestic violence shelter before finding her own place. She got a restraining order against him, switched to a new phone number, and started rebuilding her life.

Recently, Jamie cannot use technology without being plunged back into the fear that her ex is watching. Weird things have started happening. When she is on a phone call, she sometimes hears an echo. She gets locked out of her email accounts, seemingly at random, and receives texts from unknown numbers about jobs she never applied for. Acquaintances on messaging apps send her links to porn, but when she asks them about it, they get confused and say they never sent it. Her phone battery drains quickly, and when she searches Google for why, Google tells her it could be hacking. She feels paranoid and on edge—is her ex hacking her, or is it all in her head? Is she crazy?

Last week, when she received a text from an unknown number, her heart started racing and she could not breathe. She feels like any notification can trigger panic and make it as if the nightmare will never end. But Jamie cannot avoid technology—she needs to use her devices for work and to contact her family, friends, and lawyer. Anxious and stressed, Jamie goes to her phone provider for help, but all they suggest is resetting everything. It feels like no one believes her. Feeling helpless, Jamie wonders if she can ever truly start anew.

3.2 Vignette: Gender Transition

Coming out as transgender (trans) can be an affirming and liberating experience. Nevertheless, stigma and discrimination against trans people may result in numerous physical and psychological harms, many of which compound the likelihood that a trans person will experience trauma [57, 102, 120]. The 2015 U.S. Transgender Survey, which collected data from more than 27,000 trans people in the United States, highlights the significant burden trans people face: almost half of respondents reported verbal harassment in the preceding year, and nearly one in ten had been subjected to physical violence because of their gender [84]. The impact of harassment, violence, and discrimination on mental health is stark: 40% of survey respondents had attempted suicide at some point in their lives [84]. Relationships too are a site of potential trauma: when coming out as trans to family, trans people may face invalidation of their identities or family estrangement [46]. Trans people are also 2.2 times more likely to experience physical IPV and 2.5 times more likely to experience sexual IPV than cisgender individuals [137].

Technology can be valuable in helping trans people to find community and support [31, 70], health-related information that may be impossible or dangerous to seek in person [4], and tools to fight stigma via increased visibility and organizing [96, 141]. However, online spaces can also lead to stress and harm. Many social media sites, for example, are not built with trans people in mind, and may require a user to have a single and static name or select from a limited number of genders [70, 89]. Online spaces shared with friends and family complicate the presentation of gender identity [21] and may make forming supportive and healing communities difficult [46]. Recommender systems may deprioritize or remove trans people's content [173], leading to further marginalization.

The fictional vignette below highlights some negative technology experiences that trans people may have during or after transition. The vignette is inspired by stories and experiences from academic work [21, 30, 96, 141, 163], blog posts [91, 92], and news stories [138]. We also shared the vignette with domain experts, including trans people and expert researchers, for review and feedback.

When Max first began seeking online support during his transition, finding community was hard. Although Reddit was a useful resource, transphobic harassers seemed to find their way into every forum to abuse and threaten members. After a few weeks, Max found that he panicked every time he got a new notification, not knowing if he'd find support or vitriol on his posts and in his private messages. He decided to delete the account. Although the group had some supportive people, the benefits did not outweigh the costs to his mental health.

Instead, he decided to make a second Facebook account so he could like and post content about being trans without worrying so much about being harassed. Max had slowly begun to tell his friends that he was trans and add them as friends on his new account, but he wasn't quite ready to share his new name and his pronouns with his family. Unfortunately, Max found out that Facebook recommended his second Facebook account to his parents and grandmother when his mother recognized him in a photo and confronted him. Despite all his careful effort, Facebook had hijacked his decision of how and when to come out as trans to his family. His mother was so angry that she kicked him out of the house, and he had to sleep in his car for three months before being able to get his own apartment. Max felt angry and helpless. He deleted the account in a rage, feeling that social media would never be safe.

Nowadays Max is out and has been slowly going through the process of correcting his name and pronouns on his license, health insurance, work email, social media...the list feels never-ending. Whenever he thinks he's close to done, he gets another email about an account he forgot about, misgendering him and using his deadname.[1] *Every time it happens, it feels like a slap in the face—like his identity will always be in question. The hundreds of hours of work he spent on his name change feel like a waste, like the name will never be out of every database. He is afraid that years from now, after a lifetime as Max, his deadname will still be out there, and he will always feel anxious about someone finding it and using it to hurt him.*

3.3 Vignette: Identity Theft

Identity theft has become one of the fastest-growing cybercrimes [142]. Data from 2018 shows that in the United States, an estimated 23 million people, or about 9% of all U.S. residents over the age of 16, reported that they had experienced identity theft in the previous year [73]. Identity theft can cause monetary loss and damaged credit, potentially through unauthorized use of someone's existing credit cards or bank accounts. However, research has also documented the prevalent non-monetary harm caused by identity theft. According to the 2012 U.S. National Crime Victimization Survey, over 80% of people experiencing identity theft reported resulting emotional distress such as anger, depression, and anxiety; over 21% of respondents reported experiencing physical consequences in the form of headaches, trouble sleeping, or changes in eating habits [61]. Physical and emotional symptoms of distress become more likely to occur when the individual suffers financial losses or has to spend significant time clearing up resulting problems [149].

Identity theft also has far-reaching consequences beyond physical and emotional symptoms associated with distress. Identity theft may cause strained relationships with social connections as the crime leads to problems with jobs and families [73, 81]. In more extreme cases, identity theft survivors disclose suicidal thoughts that they did not have before [81]. Other research has found that identity theft may lead to behavioral changes, such as refraining from online transactions and information disclosure [98, 155].

The vignette below is based on past reports of people's experiences with identity theft, including academic literature [59], technical reports [80, 81], and news stories [5, 161, 201]. Several authors also work at a large computer security company that specializes in identity theft protection software, and have analyzed customer data about identity theft experience as part of their profession.

Alice's nightmare with identity theft started in 2012 when she received a text message informing her that her mobile number was being ported to a different network provider, which she did not authorize. She tried contacting her mobile provider to find out what was going on but they weren't able to help her. Shortly after, she received emails about changes to her contact information and her credit card PIN. Alice tried but couldn't log into her online banking account.

[1] "Deadname" is the term used to refer to a person's former name.

It turned out that the scammer, by taking over Alice's phone number and receiving her private texts and calls, had managed to reset the credentials for many of her accounts before she realized it. Even after Alice told her bank to lock her accounts and cards, the scammer managed to lift the lock and max out her credit card the very next day. New credit cards that she did not apply for also began to arrive at her apartment. It then became a daily job for her to contact different companies, go through long waits to reach a customer support agent, and convince them that she was not the one who applied for these bogus accounts. As a result, her credit history was ruined. She was horrified to see that her credit score—which she spent many years of hard work building up since college—was destroyed in a few months.

For years, Alice did not tell anyone what happened. Even though she had concerns, she hid her experience because she was embarrassed and felt it must have been her fault for not protecting her accounts. But when she heard about the Equifax data breach in 2017, she immediately checked to see if she was affected on Equifax's website. When she saw the line "your personal information may have been impacted by this incident," she came to realize that sensitive information about her such as Social Security number was again at risk, up for grabs by anyone. She was thrown back to the fear, frustration, and anger she went through all these years. She even collapsed into tears in her bank consultant's office. She was overwhelmed by the fear of losing money and the hopeless feeling that this whack-a-mole game with identity thieves would keep going on forever.

3.4 Discussion: Trauma as a Lens for Understanding Technology Experiences

Our vignettes explore contexts in which trauma is both prevalent and well-documented, highlighting some ways trauma and technology may interact. We now relate the vignettes to well-known traumatic stress reactions. We discuss how technology can itself be a cause of trauma, but also how trauma unrelated to technology use may still impact interactions with technology. Finally, we discuss the value of examining user behavior via the lens of trauma.

We want to be clear that we are not suggesting that traumatic interactions with technology are worse, or more important than physical, emotional, or psychological trauma. Instead, technology experiences that elicit trauma responses may occur *in addition* to all the other kinds of trauma survivors are also trying to cope with.

Traumatic Stress Reactions Impact Technology Interactions. Experiences with trauma can both stem from technology and impact how one experiences technology. Using the vignettes, we highlight how trauma may manifest in a user's interactions with technology. See Table 1 for a concise summary of examples from our vignettes.

Harmful, negative, or other upsetting experiences with technology are well-documented in HCI research, and there has been significant effort around understanding and preventing these harms. In many of these cases, *the technology itself is a cause of trauma and/or catalyst for harm.* For example, Max's gender identity was algorithmically exposed to his family before he was ready. A friend suggestion on social media led to real-life consequences—in this case, temporary homelessness, which is both a risk factor and cause of trauma [63]. Similarly, continuing to be deadnamed even months after diligent work of changing his name led Max to experience frustration, depression, and feelings of hopelessness. Jamie's experience of being surveilled by her partner is another example of technology directly enabling a traumatic experience. Because her partner was able to access her social media accounts and possibly install a keylogger, Jamie developed an anxious reaction to technology use that persisted even after leaving the relationship.

Perhaps more subtly, *a person's technology experiences can be changed by experiencing trauma.* For example, Jamie, after experiencing years of tech-enabled abuse, shows signs of hypervigilance when she encounters common technical challenges like a quickly depleting battery. Instead of first considering common and potentially innocuous explanations, she instead fears that her ex has access to all of her accounts again and changes her behavior accordingly.

Technology can also trigger existing trauma and even retraumatize a person. This may happen when something in one's environment causes them to recall a traumatic experience, often with a recurrence of the emotional state during the original event. In learning about the Equifax breach, Alice realized that the traumatic experience might happen to her again, prompting traumatic stress responses including fear, anxiety, and anger.

Trauma may also lead someone to avoid environments and stimuli that are reminiscent of the traumatic event. Both Jamie and Max, after experiences with harmful and upsetting messages, developed an anxious reaction to message notifications. These reactions were so distressing that Max chose to delete his account to avoid dealing with notifications.

Finally, trauma can have a long-term impact on a person's emotional state, sometimes making emotional regulation more difficult [25]. This might explain why some experiences are exceptionally difficult or emotional for trauma survivors. Alice and Max experienced extreme hopelessness at the prospect of endlessly needing to remove fraudulent accounts or change a name over and over. While problems like these may be frustrating for any user, the problem's connection to their traumatic experiences makes it especially difficult for Alice and Max to manage emotionally.

Trauma as an Explanatory Lens. The vignettes, and our own experiences working with survivors, suggest that trauma may be a valuable lens for making sense of user behaviors and experiences. Indeed, *not* acknowledging the possibility of trauma risks mischaracterizing people's lived technology experiences. Without taking trauma into account, actions like completely deleting accounts, avoiding technology altogether, or being seemingly paranoid about mundane software notifications may seem irrational or eccentric, rather than a natural survival response. Understanding and responding appropriately to people's potential trauma reactions is a key motivation for, and benefit of, a trauma-informed approach. We argue that using trauma as an explanatory lens for technology may engender the same benefits.

We therefore suggest considering trauma as a critical and underutilized lens that may explain adverse experiences with technology. Crucially, we are *not* suggesting that researchers and practitioners seek out disclosures of traumatic experiences to justify people's behaviors. Of course, not all users have experience with trauma, and not all negative experiences with technology can be explained by trauma. Nevertheless, we can assume that trauma is prevalent across any population and that any technological artifact will certainly have traumatized users. Thus, instead of seeking to prove

	Example Tech Experience	Possible Explanation Using the Lens of Trauma
Jamie	. . . assumes seemingly benign glitches are evidence of hacking.	Jamie may be **hypervigilant**, constantly scanning for signs of technology compromise as a defense.
	. . . is resigned to never having secure devices, accounts.	Jamie may be experiencing **anxiety** and **helplessness**.
Max	. . . stops using Reddit and turns off notifications.	Max may be **avoiding triggers** as a mechanism to prevent retraumatization.
	. . . angrily deletes Facebook account.	Max may be reacting to a traumatic event with **anger**, feelings of **hopelessness** about being safe online, and chooses to **withdraw**.
Alice	. . . is overwhelmed with fear by the breach notification.	Alice may be triggered by the new breach, leaving her feeling **fear**, **anxiety**, and **hopelessness**.
	. . . hides her experience from tech support.	Alice may be experiencing **shame** and **self-blame**.

Table 1: Examples of technology experiences from our vignettes, and how one might understand them using the lens of trauma. Stress reactions known from the trauma literature are boldfaced. Even if Jamie, Max, or Alice are *not* traumatized, we argue that the trauma lens still provides utility to understanding their experience.

trauma exists for an individual or a group, we argue for adopting a trauma-informed approach that assumes the possibility that trauma may be at play when making sense of *any* technology experience. This avoids forcing trauma survivors to disclose potentially traumatic experiences, which may cause re-traumatization and lead to further harms and marginalization rather than benefits for them.

4 TRAUMA-INFORMED COMPUTING

Our vignettes show many ways in which trauma may intersect with technology. We now describe a broader framework, *trauma-informed computing*, that aims to help people involved in the design, development, deployment, and support of computing technologies to accommodate trauma and, ultimately, improve technology experiences for all users—both traumatized and not.

A Definition of Trauma-informed Computing. We first lay out a proposed definition for trauma-informed computing. We start by adapting definitions found in the public and mental health literature on trauma-informed care. For example, SAMHSA [183] states that a program, organization, or system is trauma-informed if it *"realizes the widespread impact of trauma and understands potential paths for recovery; recognizes the signs and symptoms of trauma in clients, families, staff, and others involved with the system; and responds by fully integrating knowledge about trauma into policies, procedures, and practices, and seeks to actively resist re-traumatization."* This definition is tailored to, but not exclusively for, service providers that interact with potentially traumatized patients, children, and clients. Since SAMHSA's definition is broad, we reframe it to make the role of technology more evident and make our definition more actionable to technologists:

> Trauma-informed computing is an ongoing commitment to improving the design, development, deployment, and support of digital technologies by explicitly acknowledging trauma and its impact, recognizing that digital technologies can both cause and exacerbate trauma, and actively seeking out ways to avoid technology-related trauma and retraumatization.

In addition to foregrounding technology, trauma-informed computing emphasizes that companies and individuals involved in technology should *commit* to a trauma-informed viewpoint and acknowledge their role in building technology that minimizes trauma and retraumatization. We see trauma-informed computing as a framework that complements trauma-informed care, and helps technologists see the role their work has in creating a safe and healing world.

Six Principles for Trauma-informed Computing. Our trauma-informed computing framework consists of six principles adapted from SAMHSA [183]: safety, trust, peer support, collaboration, enablement, and intersectionality (see Section 2 for the specific wording of SAMHSA's principles). We shorten some of SAMHSA's principles for brevity, e.g., "trust" instead of "trustworthiness and transparency." We also rename "empowerment, voice, and choice" to "enablement" in line with Dombrowski et al. [45] to avoid a techno-determinism narrative, since trauma survivors may be *enabled* to find their own strength, but not necessarily *empowered* when the underlying structures that cause trauma remain unchanged.

For each principle, we begin by providing a definition. The core definitions were first drawn from SAMHSA [25]; we then conducted a thorough review of trauma-informed care best-practices in domains such as social work and public health, as well as a literature review within HCI to identify work with and for trauma survivors. This enabled us to significantly expand the definitions and contextualize them for technologists. We then explain how a principle could be honored in computing research and practice, noting how it is similar to or different from the principle's application in other domains. We also discuss negative consequences when a principle is violated, drawing connections to the vignettes in Section 3. In Section 5 we provide more specific examples of applying the principles in four computing-related areas.

Safety: Safety refers to ensuring that people feel safe when using, designing, or otherwise interacting with technology. Traditionally, notions of safety in trauma-informed care [53, 114, 183] mean ensuring a physically safe environment (e.g., keeping noise levels low) [114] as well as psychological safety, which encompasses "a sense of safety, or the ability to feel safe, within one's self and safe from external harm" [26]. Safety in computing encompasses not only digital safety in the sense of protection against malicious

websites and software [169], but also feeling psychologically safe in using a product or navigating a platform. As negative examples, Jamie, Max, and Alice all experience a lack of psychological safety when interacting with technology. Alice, through experiences with identity theft, was left fearing for her financial security. Online experiences may also lead to physical safety being threatened, as in Max's case when he was outed as transgender by a social media platform against his wishes.

Trust: Trust is the basis for security, dependability, and confidence in social relationships [60, 113]. Trust in others is essential to developing healthy relationships and progressing in healing and recovery from trauma [25]. Violations of trust—particularly by the technology or support infrastructure that is supposed to be helping—can lead to "the collapse of all that was known to be safe and trustworthy" [76]. The key to trustworthy computing is ensuring technology artifacts, processes and organizations operate transparently, predictably, and reliably while providing users with the ability to make mistakes and corrections [90]. Safety and trust are intertwined: creating a feeling of safety supports trustworthiness, and vice versa. As our vignettes show, trust can be elusive: Jamie could not trust that her devices were safe from her ex hacking them. Alice hid her experience from customer support due to self-blame. Facebook violated Max's trust by "hijacking" his decision about when to come out to his family.

Peer Support: Peer support refers to connecting with fellow trauma survivors as a vital part of healing and recovery [25]. In peer support, trauma survivors share their stories and lived experience with each other [13], which builds trust, creates hope, enhances safety, and overcomes the sense of isolation that often follows from traumatic events [114]. From crisis telephone lines to social media, technology can play a crucial role in facilitating peer support as it helps connect people in different time and space [131]. However, participating in online peer support could be distressing [187], especially when mechanisms to ensure the support is non-judgmental, empathetic, and respectful are lacking. Max's vignette particularly illustrates the complexities of peer support, as online communities in theory create space for it, but may end up being unsafe due to the community's and platform's inability to prevent abuse.

Collaboration: Collaboration means ensuring that trauma survivors are actively involved in decisions regarding their care and support. In essence, trauma survivors should be treated as "experts in their own lives" [25], which means recognizing and valuing their opinions and decisions. Adapting from SAMHSA's work [25], we define collaboration in computing as (1) ensuring interfaces and user interactions with a platform (e.g., through customer support agents) are collaborative rather than autocratic; (2) encouraging interaction and support from the broader ecosystem (e.g., suggesting relevant resources in search results) and from peers (in line with the principle of peer support); and (3) ensuring survivors have representation and input during the development and evaluation of new technologies. In our vignettes, Jamie's phone provider told her to just reset all her devices instead of working with her toward solutions that solved her specific problem. In Max's case, the fact that many sites do not provide options to update pronouns and names suggests a lack of diversity and inclusion in feature design.

Enablement: Enablement refers to "facilitating and developing opportunities for people to fulfill their potential and to develop their own capacity" [45]. With regard to computing, setting *enablement* as a goal allows technologists to recognize the impact of a design decision on individuals and communities [195], and what changes could be made to give people greater control over their decisions and well-being. Like collaboration, this can involve establishing shared decision-making between users and technological artifacts, but also providing the necessary transparency and information to enable users to make informed choices. In our vignettes, Jamie is not provided sufficient information and choice from tech support to be able to navigate her security options. Alice feels powerless as problems with identity theft continue to arise, and the data breach notification she receives does not give her confidence to cope with the potential aftermath.

Intersectionality: Intersectionality offers a lens for understanding how people's lives are mediated by multiple interlocking forms of oppression. Developed through lineages of Black feminist scholarship [32, 37, 38, 189], intersectionality goes beyond accounting for identity in the form of *"checking the boxes for gender, race, or class"* and considers how *power relations* at different levels of social structure are intertwined and mutually constructed [33, 151]. Since trauma is intimately tied to people's identities, in both their own lived experiences and their historical and generational traumas, computing must therefore contend with intersectionality to create trauma-informed spaces. In our vignettes, Jamie's concerns may not have been taken as seriously by her phone provider because of gendered assumptions around who has access to computing knowledge. Relatedly, Max's experience of being outed and deadnamed demonstrates how social media platforms can enforce oppressive gender binaries.

5 TRAUMA-INFORMED COMPUTING IN RESEARCH AND PRACTICE

Equipped with a definition of trauma-informed computing and its corresponding six principles, we now discuss the application of trauma-informed computing in four areas of computing research and practice: (1) UX research & design, (2) security & privacy, (3) artificial intelligence & machine learning, and (4) organizational culture in tech companies. Drawing from work in HCI and beyond, we provide concrete examples to illustrate how computing practitioners (researchers, designers, software developers, data scientists, managers, etc.) can incorporate trauma-informed computing in their own practices (see Table 2 for an overview). Throughout, we refer back to the three vignettes from Section 3 about tech-enabled IPV (Jamie), gender transition (Max), and identity theft (Alice) and discuss how honoring principles from Section 4 could support trauma survivors in preventing re-traumatization. Similar to prior work on feminist HCI [7] and affirmative consent [82], we illustrate how our framework can be used to not only critique existing problems, but also generate novel ideas to make future computing-related artifacts and processes more trauma-informed.

As we discuss a path forward, we note that implementing trauma-informed computing faces structural and systemic constraints: the

capitalist incentives around technology development (e.g., the "move fast and break things" motto embraced by big tech companies such as Facebook and Google [188]) are likely to lead to violation of trauma-informed principles when companies prioritize monetization and engagement over safety and collaboration. It is possible for individual designers and engineers to carefully follow trauma-informed computing principles, only to face major resistance from companies embedded within larger capitalist systems. Trauma-informed computing alone cannot solve the underlying causes of trauma and retraumatization. We view our framework as an actionable guide for computing professionals to taking steps to mitigate harm in the short term while envisioning bolder and more fundamental shifts in the long term—for example, stop fixing technologies that are undeniably broken and generate profit from harm [110]; instead, work with experts in other domains (e.g., activism, social work, law and policy) and impacted communities to build new technologies that resist the existing structures and systems that produce trauma without repercussion.

5.1 User Experience Research and Design

User Research. Many prevalent HCI and design paradigms (e.g., user- and human-centered design, design thinking, participatory design, etc.) emphasize the need for researchers to deeply understand users' needs and/or experiences [75]. This work often requires researchers to directly ask participants about their experiences [95] through interviews, focus groups, surveys, workshops, etc. These forms of participant engagement may cause retraumatization by requiring people to remember and recount traumatic events. We now unpack how HCI researchers and practitioners might conduct user research in trauma-informed ways.

In line with the goal of *avoiding retraumatization*, researchers should carefully consider how their research may be retraumatizing and work to minimize potential harm. In some cases, this may mean opting not to directly interact with participants when there are other means to achieve the research goal. Researchers might look to, for example, customer support chat logs or transcripts from prior interactions with trauma survivors. Analyzing publicly posted data such as those in online forums may also be an alternative to asking survivors to recount their stories, although researchers should thoroughly weigh the ethical and privacy implications of using such data [144] to avoid potential violations of users' expectations [54]. In other cases, researchers may have strong motivations to directly engage with trauma survivors. A trauma-informed approach to user research [204] requires researchers to be attuned to the power dynamics in researcher-participant relationships, be transparent about the research's goal and procedure, and give the participant substantial autonomy and flexibility. Below we discuss how researchers could follow these principles via specific practices.

Even before beginning the research, researchers should consider the *intersectional issues* at play by reflecting on how their own social identities, privileges, and lived experience relate to or differ from the communities they study, which may in turn impact participants' feelings of *safety* and *trust* [198]. Prior work has demonstrated "race of interviewer" effects when Black Americans' sensitivities to the interviewer's race shaped their reported political views [39], particularly with regard to police violence [159]. Taking *intersectionality* into account, Owens et al. had a Black researcher interviewing family members of incarcerated people in their study, the majority being Black, as a way to make participants more comfortable and forthcoming in their responses via shared experiences [134].

Similarly, researchers should actively build *safety* and *trust* in interacting with participants. *Safety* can be pursued by ensuring that the research takes place in a location that is safe and familiar to participants, and by providing participants with appropriate trigger warnings. In Freed et al.'s study on the role of technology abuse in IPV [56], the researchers conducted focus groups with clients at a survivor advocacy organization that survivors already visited and knew to be a safe space. The authors partnered closely with organizations that survivors knew and trusted in designing the study protocol to establish *trust*, and chose focus groups over individual interviews to enable *peer support* as survivors discuss difficult experiences. As discussed by Wong [204], *trust* can also be built by having a warm-up and a debrief to build rapport, using active listening and empathy to create a welcoming space, and mirroring the participant's language in describing their experience to avoid potentially harmful labeling.

Following the principles of *collaboration* and *enablement* may also lead researchers to involve survivors directly in the research when survivors have the interest and capacity to do so. For example, in studying recurrent episodes of homelessness among single mothers, Bertsch [12] established *collaboration* by involving study participants as co-researchers in analyzing their own narratives, thereby giving them an active voice in telling their stories and fostering a partnership between researcher and participant. The principle of *collaboration* may also lead researchers to involve trauma and mental health professionals in the research process, who can bridge the gap between researchers and participants and provide stakeholder input [157]. Wong [204] suggested that researchers can honor *enablement* by clearly communicating choices of skipping a question, stopping the participation, or revoking consent during the research as well as providing referral paths after the research if the participant becomes distressed.

As we outline example strategies researchers could deploy to better account for trauma in their work, researchers should bear in mind that each study will have its own requirements depending on the community, context, and methods. We urge all researchers to carefully consider their own studies—especially those that involve marginalized and/or potentially traumatized participants—and identify ways to incorporate the principles of trauma-informed computing into their practices.

User Interface Design. Another common phase of HCI work is the design and prototyping of new features, interfaces, or products. Considering trauma survivors in design processes may surface ideas that make end products more trauma-informed. As demonstrated in the redesign of Callisto Campus, an online system for reporting sexual assault [23], the designers consulted with experts in neurobiology and institutional betrayal in creating the system's report form, which led to trauma-informed features such as enacting progressive disclosure (in line with *enablement*) and avoiding gender-specific pronouns (attuned to *intersectionality*). Similarly, Rabaan discusses a transformative justice approach supported by trauma-informed concepts to help Muslim survivors of IPV in the

Area	Topic	Example Good Practice
UX Research & Design	User research	• Carefully consider how user research can be retraumatizing and work to minimize potential harm [*"seek ways to avoid retraumatization"*] • Conduct user studies in a place where participants feel safe and familiar [safety, trust] • Consider involving survivors in the research process [collaboration, enablement]
	User interface design	• Draw inspiration from trauma-informed design principles in other environments such as physical spaces [safety, trust] • Create, publish, and encourage reuse of trauma-informed design patterns [trust, collaboration]
	Usability assessment	• Evaluate how a technology or interface may traumatize or retraumatize its users *["seek ways to avoid retraumatization"]*
Security & Privacy	Threat modeling	• Include "causing psychological distress" as a common adversarial goal *["acknowledge trauma and its impact"]* • Work with survivors to surface adversarial goals and capabilities [collaboration]
	Indicators & settings	• For software updates, provide clear information that warns users ahead of time on any upcoming changes, with options for whether and when to update [safety, trust] • For security warnings, reflect on the impacts of established "best practices" (e.g., using harsh colors and forcing attention) on hypervigilant users *["seek ways to avoid retraumatization"]*
Artificial Intelligence & Machine Learning	Automated social decisions	• Audit algorithms and datasets in systems that make socially consequential decisions (e.g., in criminal justice, employment) [trust, collaboration, intersectionality]
	Recommender systems	• Clearly explain why a particular recommendation shows up (e.g., a GPS system ad is a result of search histories, not an indicator of being stalked) [trust] • Let users disallow certain ad topics across different websites and platforms [collaboration, enablement] • Enable users to opt out friend recommendation systems [safety, trust, enablement]
	Content moderation & filtering	• Be attuned to how automatic flagging can inadvertently remove benign content important to marginalized communities [intersectionality] • Create content policies with input from impacted communities [collaboration]
	Intelligent agents	• Ensure agents do not judge users or increase users' anxieties [safety, trust] • Build agents that empathetically respond to intersectional issues [intersectionality]
Organizational Culture	Work processes	• Provide training & resources to help workers better interact with trauma survivors and process secondary trauma [safety, peer support, enablement] • Provide accommodations for employees to flexibly manage their schedules, workload, and exposure to traumatic content [collaboration, enablement]
	Workplace culture	• Ensure that workplace policies account for employees experiencing traumatic events (e.g., death, illness, racism) [*"acknowledge trauma and its impact,"* intersectionality] • Ensure that internal processes for handling harassment and discrimination cases hold perpetrators accountable and enable survivors to heal [safety, trust, intersectionality]

Table 2: Overview of the application areas we explore for trauma-informed computing, with examples of good practices. Each example is connected to our definition of trauma-informed computing in Section 4 and/or one or more of the six principles.

U.S. [146]. Trauma-informed principles make space for considering the gendered Islamophobia and racial discrimination faced by Muslim women (*intersectionality*) and supporting survivors' decisions (*collaboration*), e.g., to stay embedded in their communities [146].

There are existing recommendations on how behavioral health employees can implement trauma-informed approaches in their work environments, and these recommendations also apply to technology designs. For instance, guidelines for designing a trauma-informed physical environment [34, 58] suggest creating detailed but not overcrowded visuals, avoiding clutter that may prove irritating, and using cool colors for a calming effect. Drawing from these recommendations, designers could use muted color palettes and simple and predictable layouts to create a more trauma-informed interface, which could minimize erratic behavior that triggers Jamie and other hypervigilant survivors of tech-enabled abuse.

A promising opportunity for HCI research and practice is the creation of design patterns that incorporate trauma-informed principles. A design pattern is a general and reusable solution to a common design problem (e.g., media player toolbars, calendar widgets) [164, 192]. Designers frequently incorporate design patterns rather than making a new design from scratch, because design patterns are familiar to users, have already been tested, and enable standardization across applications, all of which may help to build user *trust* by reducing unfamiliar or unpredictable platform behavior. Designers working with researchers to create, publish, and encourage

reuse of design patterns that are known to be trauma-informed—which would include *collaboration* with trauma survivors—could be a highly effective way to integrate trauma-informed computing into a wide variety of platforms. Successful early research in this space includes Spiel et al.'s guidelines for surveying gender in HCI that are known to be inclusive and appropriate for trans and nonbinary people [176], which could provide *safety*. As discussed by Decker [40], dark patterns that trick users into doing something they did not mean to do (e.g., limited-time discounts with countdown clocks [122] and pre-ticked checkboxes in cookie consent banners [15]) are counterexamples designers should avoid as they breach users' *trust*.

Usability Assessment. Prior sections make clear that traumatic stress reactions can impact usability. To incorporate trauma-informed principles into usability assessments, we draw inspiration from Nielsen and Molich's heuristic evaluation method for identifying usability problems [129]. Heuristic evaluation is a "discount" usability evaluation method in which a small set of evaluators systematically assess an interface for compliance with a set of pre-defined heuristics [129]. Similarly, HCI researchers and practitioners can develop a "trauma-informed heuristic evaluation" to systematically assess a technology or interface for compliance with the principles of trauma-informed computing. Take, for example, a single sign-on feature that propagates personal information (e.g., name, gender, photos) to a variety of linked accounts without notifying users or providing ways to control or prevent this propagation. This type of propagation could be dangerous and violate *safety* and *trust* for users like Max, who may use different names or pronouns strategically in different online spaces. A trauma-informed usability evaluation may highlight that this feature violates the principles of *safety*, *enablement*, *collaboration*, and *trust*. Future work could investigate if trauma-informed computing principles themselves serve well as heuristics, or if we need to derive more granular heuristics based on the principles.

5.2 Security and Privacy

Security and privacy stand to play a prominent role in building trauma-informed technology. We discuss how established security and privacy processes and workflows could incorporate the principles of trauma-informed computing.

Threat Modeling. A key part of security research and practice is threat modeling: a structured process for identifying potential security risks in software, systems, and enterprises and developing mitigation strategies [179]. Threat models generally involve the target under attack, the likely type(s) of adversary performing attacks, and the adversary's assumed capabilities and goals. Prior work has introduced threat models for specific high-risk communities [56, 96, 109, 174], some of which have surfaced providing emotional or psychological safety as a goal [96, 111]. Below we discuss opportunities to extend threat modeling so that these considerations are made by default rather than by exception.

First, causing psychological distress—for example, by sending transphobic messages to trans users, as Max experienced—should be considered a common high-level adversarial goal, akin to the traditional high-level goals of violating confidentiality, integrity, authenticity, or availability. This is increasingly, if implicitly, acknowledged in abuse threat models [191], but we believe the principles underlying trauma-informed computing can be used to make these considerations explicit. Security practitioners can employ threat modeling to speculate about how adversaries would aim to reduce *safety* and *trust*, increase isolation (which in turn reduces *peer support*), disable users, or exploit a target's identities. For example, an abuser might cause devices to behave or appear differently to gaslight the survivor into thinking their devices are compromised, thereby undermining their *trust* in technology and feeling of *safety*, demonstrated by Jamie's experience in the aftermath of her abusive relationship. Relatedly, security practitioners should also consider software vulnerabilities that can be exploited to generate the illusion of compromise (violating *trust* and *safety*) or to add friction to the process of accessing resources or mitigations (violating *enablement*).

Second, security practitioners conducting trauma-informed threat modeling should consider the potential burden of trauma when estimating the amount of effort required for taking protective measures, such as choosing new passwords, turning on multi-factor authentication, spotting phishing emails, and the like. Traumatic stress tends to cause emotional dysregulation as feeling either too much (overwhelmed) or too little (numb) [25], both of which can increase the difficulty of deploying countermeasures. In line with *enablement*, practitioners should recognize and value the effort put forth by the survivor and accept that emotional capacity is an inevitable component of digital defense. As Tseng et al. [195] discuss in their operation of remote security clinics for IPV survivors, future work could examine the long-term effects of such interventions (e.g., assessing when and how clients use provided guides) to understand whether the intervention helps clients develop their capacity or creates unwanted burdens.

Security Indicators and Settings. Existing usability issues for security and privacy may have amplified consequences for trauma survivors. For example, automatic software updates that don't warn or inform users [200] may be annoying or disruptive to many users [108] and triggering to others. If someone is hypervigilant or anxious about hacking, as Jamie was, unexpected changes in the appearance or behavior of an interface can be frightening. In considering how trauma-informed principles might apply to update processes, security practitioners and designers may build *trust* by providing clear information that warns users ahead of time about coming visible changes. In the spirit of *collaboration* and *enablement*, updates should explain why the changes are needed and provide options for whether and when to update [114].

Similarly, many security and privacy settings for limiting content visibility, checking activity logs, or deleting accounts are known to be complex and difficult to use [68, 121, 162]. Computing practitioners may be incentivized to further deploy "dark patterns" for better monetizing consumer data, which remove or impede access to meaningful choices [55], violating *collaboration* and *enablement*. As *intersectionality* indicates, this burden is not borne by all people equally. Navigating complex settings is even more difficult for people who already feel helpless and overwhelmed as a result of traumatic experiences on the platform. With regard to LGBTQ+ people, Carrosco and Kerne [24] showed how *enablement* was not

respected, regardless of the illusion of choice, with public-by-default dark patterns on social media platforms; even users who interact with in-depth privacy settings, as Max did, often feel uneasy or have a negative experience with how their actions are shown to and beyond their social circles.

Furthermore, some security "best practices" are at odds with the needs of trauma survivors. For example, security warnings usually aim to capture the user's attention and resist habituation [9]. Prior work has suggested various ways for achieving these goals, such as using the color red to induce fear [185], using signal words (e.g., "danger" or "threat") [67], and forcing users to interact with the warning [140]. However, designers adhering to the principles of *safety* and *trust* may require a different approach: for trauma survivors, red can be associated with aggression, dominance, and power [29]; signal words for security warnings can trigger panic or feel overwhelming, as Alice experienced when she was warned about the Equifax data breach. A persistent, hard-to-dismiss spyware warning could successfully raise the attention of a typical user, but could also threaten an IPV survivor's *safety* if their abuser sees the warning. By helping researchers identify the real, unaccounted-for costs of current security solutions to weigh against the benefits for the typical user, trauma-informed computing principles will enable future researchers to explore alternative solutions to navigate the tension between the deficit of attention among typical users and the surfeit of attention among hypervigilant users.

5.3 Artificial Intelligence & Machine Learning

We now turn to how researchers and practitioners in artificial intelligence (AI), machine learning (ML), and related areas might incorporate trauma-informed computing. We focus on four areas in which AI/ML systems are widely deployed in society: (1) algorithms for automating social decisions, (2) recommender systems, (3) content moderation and filtering, and (4) intelligent agents.

Automating Social Decisions. ML algorithms are increasingly involved in socially consequential decision-making: producing risk scores for judges to set bail or parole [11]; informing the distribution of resources in social service programs [50]; justifying arrests with facial recognition systems [93]. These algorithms are often built with the intention of supporting humans overwhelmed by the sheer number of decisions that need to be made (e.g., rising caseloads for social workers [160]) and the scope and complexity of the considerations required to make them (e.g., judges assessing risk of recidivism [112]). In addition, the use of data-driven systems often appeals to people's desire for "objective" tools that they believe will reduce human biases [10].

However, automatic decision-making via ML has a documented history of causing grievous harms, including trauma. Core to the problem is the fundamentally "*black-box*" nature of ML systems: there can be no *trust* in or *collaboration* with a system that produces judgments by drawing layered statistical comparisons at a scale humans cannot comprehend, from datasets that may be biased towards harmful perspectives or that cement social inequities. Recent research in ML interpretability and explainability is attempting to bridge this gap [41, 156], but concerns remain that these systems exacerbate social inequalities [10, 19, 148]—a clear violation of the *intersectionality* principle.

Trauma-informed computing would suggest that ML researchers should center the *safety* and *trust* principles in creating these systems by ensuring, for instance, that an algorithmic risk model does not have the final say in deciding if someone is arrested or goes to jail. Specifically, practitioners interested in applying ML techniques to social problems might consider foregrounding contestability (*enablement*) in the design of ML-based decision-making systems [77, 125, 143] by making use of methods for auditing algorithms and datasets [148, 158]. Indeed, prior auditing studies have shed light on how online ads about arrest records appear more often with searches of names predominantly given to Black babies than those predominantly given to white babies [186], and how facial recognition systems tend to misclassify darker-skinned women more than other groups [19]. In cases where an algorithm must be developed, researchers might also pursue ML paradigms that better embrace the diversity and complexity of human judgment. For example, Gordon et al. [64] developed the disagreement deconvolution, a method that aligns ML classification metrics with "the proportion of the overall population that would agree with each classification decision," thereby providing a more human-centered approach to ML classifiers in line with the *collaboration* principle.

Existing efforts to improve algorithmic fairness, accountability, and transparency are making headway in surfacing and remedying similar issues. Trauma-informed computing complements these efforts by providing principles that, when incorporated into ML design, systems, and processes, help center individual well-being alongside creating just systems. The examples here are only starting points; there are rich opportunities for future work to incorporate trauma-informed computing into ML research and practice.

Recommender Systems. Another area of AI/ML research that might benefit from trauma-informed computing is recommender systems: ML systems that help users discover new products and services that might be relevant or interesting to them [136]. Recommender systems are widely deployed in practice across numerous domains and applications, including targeted advertising. There are many examples of how AI-inferred ad recommendations might unintentionally lead to trauma. For example, an ad might recommend maternity wear to survivors of pregnancy loss [17] or wedding services to people who have broken up [62].

We see many opportunities for AI/ML practitioners to make recommender systems more trauma-informed. Past research has shown that users view recommender systems more *trustworthy* when they perceive that the personalized algorithm is more transparent and explainable [1, 170]. Ideally, users would have clear information about why a particular recommendation is showing up to reduce anxious speculation and fear (e.g., Jamie may feel safer if an ad for GPS tracking devices was clearly due to her own search behavior rather than her ex's: "*This ad is shown to you because you searched 'is my location being tracked'*"). Similar features are already provided on a few platforms (e.g., "*Because you liked movie A, we recommend movie B*") but are not universal, and the explanations were often incomplete or misleading [79].

Beyond seeing why a recommendation is shown to them, users should also have some control over their ad topics. Letting users disallow ad topics in the moment (e.g., "*Never again show me ads related to location tracking*") supports *collaboration* and *enablement*.

More proactively, as suggested by Im et al. [82], platforms and ad companies should consider allowing users to curate a list of topics that systems could use to avoid potentially triggering content. This is not an impossible task: Facebook already does this to a limited extent by allowing users to minimize the number of ads shown in specific categories: alcohol, parenting, pets, and social issues, elections, and politics [52]. Ideally, such mechanisms could be designed in ways that propagate across different platforms and products, so that users do not need to manually curate multiple lists for every platform or website.

Some recommender systems, in any form, will be dangerous for a subset of users. In Max's case, he may not have been outed to his family if he had been able to prevent his Facebook profile from being shown to others via "friend recommendations." Being able to prevent these recommendations can also be helpful for other populations, such as IPV survivors who share friends and family with an abusive ex [56] and sex workers who want to keep their personal social media hidden from clients [111]. Providing options to opt out, in addition to transparency, would further *enable* users to navigate their own trauma, and, more broadly, could improve *safety* and build *trust* in computing systems. However, users are often not aware that opt-outs exist; in order to avoid retraumatization, platforms may need to keep these friend recommendation features off by default and ask users if they want to opt in as part of their interaction paths. This change, while reducing burden on the user's end, is at odds with most platforms' engagement and growth priorities, and may require regulatory intervention.

Content Moderation and Filtering. Many platforms employ ML-based content moderation and/or filtering systems to automatically detect and remove offensive or problematic content. Some goals of these systems align with trauma-informed computing principles as platforms seek to improve *safety* by removing content that may (re)traumatize people. However, the design and deployment of these systems may also lead to harms, often when designers, engineers, and other stakeholders fail to account for *intersectionality*. For example, prior research has shown how automated content moderation algorithms can flag or remove benign content, often from marginalized users like Black or transgender people [69] and sex workers [8, 14]. Such actions violate *trust* and *collaboration* for the people whose content gets removed, and the removal itself could be traumatizing. Removing content shared within these communities can also hamper *peer support* by decreasing the information and resources available, and decrease *safety* by severing vital connections with advocates and resources [27].

Online harassment remains a challenge for content moderation as profound harm can come from other users in digital spaces. As Schoenebeck et al. [167] discuss, restorative justice supported by trauma-informed approaches could play a role in social media companies' response to harassment. In particular, the authors identify *intersectionality* as an important lens to consider when navigating online mediation, as different communities may have differing ideas of justice due to cultural histories of exclusion and trauma [166].

A potential downside of content moderation and filtering is "filter bubbles" that limit the content people are shown, often invisibly, to a subset of what might be relevant. Engineers and designers could follow the principles of *collaboration* and *enablement* to incorporate people's conscious choice into their information feeds. Furthermore, filter bubbles could disproportionately impact certain populations when the algorithm fails to take *intersectionality* into account. At-risk or marginalized communities, who may already experience higher prevalence of trauma, may be more likely to be shown traumatizing content. A poignant example comes from Erete et al.'s autoethnographic study [49], in which the authors, who are Black women, reflect on the negative mental health impacts they have experienced from repeated, unwanted exposures to video recordings of police officers murdering George Floyd in May 2020.

At a higher level, content moderation systems enforce company-created content policies. These policies inherently prioritize some values over others when deciding what content will be flagged and removed and what will not. Thus, it is important that the processes involved in creating content policies are themselves trauma-informed. In line with the *collaboration* principle, Haimson et al. [69] suggest that platforms should work with marginalized communities (e.g., by hiring community members as consultants) to create moderation policies and viable enforcement mechanisms that more appropriately reflect community voices and needs.

Intelligent Agents. Recent advances in natural language processing have enabled powerful AI-based intelligent agents, including chatbots and voice-based agents such as Siri, Cortana, and Alexa. Such agents are also prevalent in companies' customer support, providing automated responses to frequently asked questions and connecting customers to human representatives. In addition to general purpose agents, there is growing interest in creating agents that specifically serve communities experiencing high rates of trauma; examples include chatbots to reduce psychosocial distress for cancer survivors [66], to help veterans suffering from PTSD [104], and to counsel survivors of sexual assault [78]. However, if not designed properly, intelligent agents could also exacerbate their users' trauma. In Alice's case, if she were to call her bank today to report identity theft, she would likely encounter a voice-operated agent before being able to speak to a human. If the agent offered only limited options, worked poorly, or tried and failed to authenticate Alice without connecting her with a human, her financial trauma may have been even worse.

There are important opportunities for future research to consider how to build agents that are trauma-informed. For example, agents are often intentionally designed to create the illusion of being human, responding in ways that seem emotional or empathetic [101], which could compromise *safety* and *trust* if the user believes they are interacting with a human and then discovers they are not. That being said, non-human agents provide benefits in certain cases. Lucas et al. [104] documented how veterans suffering from PTSD preferred to tell their stories to a virtual agent over a human therapist, since the agent would not be critical or judgmental.

When designing agents, it is also important to consider *intersectionality*. For example, Microsoft created Tay, an agent trained to seem like a teenage girl. Tay "learned" via input from Internet users, which quickly led to it producing abusive, racist, and sexist responses [203]. When creating Tay's successor, Zo, designers chose to incorporate "strong checks and balances to protect her from exploitation" [116] by programming it to refrain from engaging in potentially controversial subjects like race or religion. As a result,

Zo would respond empathetically to the phrase, *"I get bullied sometimes"* by saying, *"ugh, I hate that that's happening to you."* However, when told, *"I get bullied sometimes for being Muslim,"* it responded, *"I really have no interest in chatting about religion."* More broadly, Zo refused to respond to chats containing words such as "hijab," "muslim," "bar mitzvah," or "jew" regardless of the content, but had no problem engaging in conversations about Christianity [182].

These examples highlight the complex, deeply social, and value-laden nature of human communication, all of which complicate the prospect of designing safe, trustworthy, and trauma-informed agents. As we move towards an online world in which agents are prevalent and may be increasingly indistinguishable from humans, researchers and practitioners should question how to best create agents that involve trauma-informed computing—incorporating the principles of *safety*, *trust*, and *intersectionality*.

5.4 Organizational Culture in Tech Companies

The prevalence of trauma in society suggests that most technology companies will also have employees who are themselves trauma survivors. Similar to how institutions like schools [106, 118, 153] and hospitals [105, 147] have adopted trauma-informed approaches, tech companies could similarly shift internally towards trauma-informed practices and policies by (1) accounting for types of work that may directly cause or trigger trauma for workers, and (2) improving the broader workplace culture.

Work Processes. The business of building and maintaining computing platforms has proven to involve work that directly causes trauma and/or retraumatization. A well-documented example is content moderation, which is unrecognized and undervalued "ghost work" [65] that requires employees to constantly watch and report large volumes of disturbing, psychologically scarring content like gore, suicide, revenge, and child pornography [178], often under precarious labor arrangements [154]. Other examples include company employees responsible for dealing with user reports of online harassment or abuse, or customer support agents who directly speak with potentially traumatized users and help them navigate problems [205]. Awareness of trauma in companies' work processes could in turn support their customers as well; for example, if the customer support agents Jamie spoke to about her misbehaving mobile device had been aware of tech abuse and the trauma it can cause, they may have been able to provide Jamie with more actionable advice, increasing her *safety* and *trust* in the company.

As with any trauma-informed approach, an important first step is for tech companies' leadership and management to realize and take seriously the widespread impact of trauma on its own employees [183]. This acknowledgement could help companies prioritize creating processes that enable them to recognize potential signs of trauma in their workers and develop best practices that consider trauma and avoid retraumatization. Putting the principle of *collaboration* into practice, companies could consider flexible ways to work with employees to manage their schedules, workload, and exposure to traumatic content, allowing for accommodations that validate workers' experiences and gives them time to heal. Furthermore, companies could work to *enable* workers by providing access to existing resources developed by social work and public health professionals [190, 197] that help employees learn about and recognize the signs of trauma in themselves, including secondary or vicarious trauma. Example resources may include training, guides, self-evaluations, or information about techniques for dealing with trauma responses. Companies could also ensure that workers have access to appropriate mental health resources and support (e.g., therapy sessions) that would improve worker *safety* and promote *trust* by showing that the company takes trauma seriously and cares for its employees. Workers might also have opportunities to participate in group discussions that help them process distressing experiences, thereby enabling *peer support*.

Workplace Culture. Beyond specific types of work that may be trauma-related, there are opportunities for tech companies to integrate principles of trauma-informed computing in building the broader workplace culture. The tech industry has long struggled with issues of diversity and inclusion [43], and many stories have documented instances of potentially traumatic discrimination, microaggressions, harassment, and assault, which are often disproportionately experienced by workers with marginalized identities [20, 127]. Existing mechanisms for reporting and processing potentially traumatizing workplace experiences often fail to build *trust* when internal processes lack transparency and accountability; survivors perceive these systems to maintain and enforce existing power structures [103], rather than provide meaningful ways to hold perpetrators accountable and/or enable survivors to heal. Moving forward, tech companies should review the tools and procedures they use internally for compliance with trauma-informed principles. For example, at the time of writing, the widely adopted workplace communications tool Slack does not provide a way for users to block messages from other users [193], either privately or in group channels, which may compromise *safety* and *trust*.

At a higher level, adopting a trauma-informed approach may enable companies to better account for the fact that all employees are ultimately people who may experience traumatic events from death, illness, to racism and violence. For many employees, the COVID-19 pandemic has taken a heavy toll on their mental health and well-being [135]. Becoming ill, witnessing close family and friends fall sick or pass away, the erosion of in-person social support, and a sustained, elevated level of panic and anxiety throughout are only a few examples of potentially traumatizing experiences during the pandemic. Through the COVID-19 pandemic, tech companies have opportunities to consider how their workplace policies related to benefits, leave, flexibility in work hours, etc. may impact traumatized employees, including service workers like kitchen staff and custodians. Companies might create mechanisms that recognize and accommodate employees' lived experiences, promoting *safety*, *trust*, and *collaboration*, with particular attention to *intersectionality*, e.g, the disproportionate burden on women employees to also provide childcare during the COVID-19 pandemic [150]. For trauma-informed computing to affect workplace cultures, leadership needs to recognize the prevalence of trauma and create change through action, which may involve a combination of policy changes, training, tools, and resources that differ across companies.

6 CONCLUSION AND REFLECTION

This paper discussed how trauma and traumatic stress reactions may impact people's technology experiences. We proposed a framework called trauma-informed computing and six principles that might improve safety for all users. Finally, we illustrated our framework's application in four areas of computing. As an orientation to research and practice, trauma-informed computing has to be an ongoing commitment to improving design processes and artifacts, rather than a one-time checklist or a set of specific techniques. Becoming aware of trauma is only the first step; learning, reflecting, and applying that knowledge are required throughout design, deployment, and maintenance of computing systems.

We acknowledge that computing researchers and practitioners may feel a natural hesitation or aversion to engaging with trauma in their work. There are deep cultural and social stigmas around discussing trauma and mental health [119]. In addition, people may be understandably reluctant to engage with trauma due to potential negative impacts on their own mental health. Learning about traumatic stories and experiences can threaten one's own sense of safety and possibly cause (re)traumatization, and supporting survivors while being mindful of one's own emotions and behaviors can be a challenging endeavor. Researchers may also be cautious about not overstepping their expertise. People who are not mental health professionals may feel they lack the necessary training, tools, or background to engage with trauma.

Fortunately, applying trauma-informed computing does *not* require the diagnosis, disclosure, or treatment of trauma. In fact, we argue that attempting to discover or measure how much computing-related trauma a user might experience runs the risk of retraumatizing them by mislabeling their experience or forcing them to relive painful experiences. This is counter to the goals of centering individual needs in a trauma-informed approach. Rather, the described principles for trauma-informed computing can be implemented widely to help everyone, regardless of one's experiences with trauma. For example, classroom teachers are not mental health professionals, but can use trauma-informed teaching to support all students. By acknowledging that trauma can impact learning and behavior, educators can reflect on and adapt their practices, such as building positive relationships, communicating with families, and being culturally responsive [118].

With trauma-informed computing, we aim to contribute a new lens that complements other frameworks that consider marginalized or at-risk communities, for example, using trauma-informed computing paired with social justice [45], feminist theory [7], and postcolonial computing [83]. Taken together, this constellation of orientations, design strategies, and principles can broaden perspectives and offer a set of tools for researchers and practitioners to create computing systems that better serve people from all identities, backgrounds, and experiences.

ACKNOWLEDGMENTS

The authors thank Francesca Rossi, Tess Tanenbaum, Oliver Haimson, Sunny Consolvo, CETA volunteers, and our anonymous reviewers for their feedback on our early drafts. This research was funded by NSF Award #1916096 and a gift from Google. Allison McDonald was supported by a Facebook Fellowship; Emily Tseng was additionally supported by a Digital Life Initiative Doctoral Fellowship. This research has also been partially supported by the Defense Advanced Research Projects Agency (DARPA) under grant no. HR00112010010. The content of the information does not necessarily reflect the position or the policy of the U.S. Government, and no official endorsement should be inferred. Approved for public release; distribution is unlimited.

REFERENCES

[1] Mike Ananny and Kate Crawford. 2018. Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability. *New Media & Society* 20, 3 (2018), 973–989. https://doi.org/10.1177/1461444816676645

[2] Nazanin Andalibi. 2020. Disclosure, Privacy, and Stigma on Social Media: Examining Non-Disclosure of Distressing Experiences. *ACM Transactions on Computer-Human Interaction* 27, 3 (2020), 18:1–18:43. https://doi.org/10.1145/3386600

[3] Nazanin Andalibi. 2021. Symbolic Annihilation through Design: Pregnancy Loss in Pregnancy-Related Mobile Apps. *New Media & Society* 23, 3 (March 2021), 613–631. https://doi.org/10.1177/1461444820984473

[4] Laima Augustaitis, Leland A. Merrill, Kristi E. Gamarel, and Oliver L. Haimson. 2021. Online Transgender Health Information Seeking: Facilitators, Barriers, and Future Directions. In *Proceedings of the Conference on Human Factors in Computing Systems (CHI)*. ACM, New York, NY, USA, 205:1–205:14. https://doi.org/10.1145/3411764.3445091

[5] Anna Bahney. 2017. Identity theft nightmares: 'I've spent my lifetime building up my credit'. Retrieved August 28, 2021 from https://money.cnn.com/2017/09/29/pf/identity-theft/index.html

[6] Jane Bailey, Nicola Henry, and Asher Flynn. 2021. Technology-Facilitated Violence and Abuse: International Perspectives and Experiences. In *The Emerald International Handbook of Technology Facilitated Violence and Abuse*. Emerald Publishing Limited, Bingley, West Yorkshire, UK, 1–17. https://doi.org/10.1108/978-1-83982-848-520211001

[7] Shaowen Bardzell. 2010. Feminist HCI: taking stock and outlining an agenda for design. In *Proceedings of the Conference on Human Factors in Computing Systems (CHI)*. ACM, New York, NY, USA, 1301–1310. https://doi.org/10.1145/1753326.1753521

[8] Catherine Barwulor, Allison McDonald, Eszter Hargittai, and Elissa M. Redmiles. 2021. "Disadvantaged in the American-Dominated Internet": Sex, Work, and Technology. In *Proceedings of the Conference on Human Factors in Computing Systems (CHI)*. ACM, New York, NY, USA, 563:1–563:16. https://doi.org/10.1145/3411764.3445378

[9] Lujo Bauer, Cristian Bravo-Lillo, Lorrie Cranor, and Elli Fragkaki. 2013. *Warning design guidelines*. Technical Report. Carnegie Mellon University CyLab. https://www.cylab.cmu.edu/_files/pdfs/tech_reports/CMUCyLab13002.pdf

[10] Ruha Benjamin. 2019. *Race After Technology: Abolitionist Tools for the New Jim Code*. John Wiley & Sons, Medford, MA, USA.

[11] Richard Berk. 2012. *Criminal justice forecasts of risk: A machine learning approach*. Springer Science & Business Media, Berlin, Germany.

[12] Thérèse M Craine Bertsch. 2012. *The standpoint of homeless single mothers on recurrent episodes of homelessness*. Ph.D. Dissertation. Adelphi University School of Social Work. https://www.proquest.com/docview/1318618421

[13] Andrea Blanch, Beth Filson, Darby Penney, and Cathy Cave. 2012. *Engaging women in trauma-informed peer support: A guidebook*. Technical Report. National Center for Trauma-Informed Care. https://nicic.gov/engaging-women-trauma-informed-peer-support-guidebook

[14] Danielle Blunt, Emily Coombes, Shanelle Mullin, and Ariel Wolf. 2020. Posting Into the Void: Studying the Impact of Shadowbanning on Sex Workers and Activists. Retrieved September 6, 2021 from https://hackinghustling.org/posting-into-the-void-content-moderation/

[15] Christoph Bösch, Benjamin Erb, Frank Kargl, Henning Kopp, and Stefan Pfattheicher. 2016. Tales from the Dark Side: Privacy Dark Strategies and Privacy Dark Patterns. *Proceedings on Privacy Enhancing Technologies* 2016, 4 (2016), 237–254. https://doi.org/10.1515/popets-2016-0038

[16] Elizabeth A. Bowen and Nadine Shaanta Murshid. 2016. Trauma-Informed Social Policy: A Conceptual Framework for Policy Analysis and Advocacy. *American Journal of Public Health* 106, 2 (Feb. 2016), 223–229. https://doi.org/10.2105/AJPH.2015.302970

[17] Gillian Brockell. 2018. Dear tech companies, I don't want to see pregnancy ads after my child was stillborn. Retrieved August 28, 2021 from https://www.seattletimes.com/life/dear-tech-companies-i-dont-want-to-see-pregnancy-ads-after-my-child-was-stillborn/

[18] Vivian Barnett Brown, Maxine Harris, and Roger Fallot. 2013. Moving toward Trauma-Informed Practice in Addiction Treatment: A Collaborative Model of Agency Assessment. *Journal of Psychoactive Drugs* 45, 5 (2013), 386–393.

https://doi.org/10.1080/02791072.2013.844381
[19] Joy Buolamwini and Timnit Gebru. 2018. Gender shades: Intersectional accuracy disparities in commercial gender classification. In *Proceedings of the Conference on Fairness, Accountability and Transparency*. PMLR, New York, NY, USA, 81:77–91. http://proceedings.mlr.press/v81/buolamwini18a.html
[20] Crosby Burns and Jeff Krehely. 2011. Gay and Transgender People Face High Rates of Workplace Discrimination and Harassment. Retrieved August 28, 2021 from https://cdn.americanprogress.org/wp-content/uploads/issues/2011/06/pdf/workplace_discrimination.pdf
[21] Justin Buss, Hayden Le, and Oliver L Haimson. 2021. Transgender identity management across social media platforms. *Media, Culture & Society* 0, 0 (2021), 1–17. https://doi.org/10.1177/01634437211027106
[22] Lisa D Butler, Filomena M Critelli, and Elaine S Rinfrette. 2011. Trauma-informed care and mental health. *Directions in Psychiatry* 31, 3 (2011), 197–212.
[23] Callisto: Tech to Combat Sexual Assault. 2017. Designing trauma-informed and inclusive technology for survivors of sexual assault. Retrieved September 6, 2021 from https://medium.com/@projectcallisto/designing-trauma-informed-and-inclusive-technology-for-survivors-of-sexual-assault-928afb3c579
[24] Matthew Carrasco and Andruid Kerne. 2018. Queer visibility: Supporting LGBT+ selective visibility on social media. In *Proceedings of the Conference on Human Factors in Computing Systems (CHI)*. ACM, New York, NY, USA, 250:1–250:12. https://doi.org/10.1145/3173574.3173824
[25] Center for Substance Abuse Treatment. 2014. *Trauma-Informed Care in Behavioral Health Services*. Substance Abuse and Mental Health Services Administration, Rockville, MD, USA. http://www.ncbi.nlm.nih.gov/books/NBK207201/
[26] Chadwick Trauma-Informed Systems Project. 2013. Creating trauma-informed child welfare systems: A guide for administrators. Retrieved August 29, 2021 from http://communitypact.org/wp-content/uploads/2014/04/CTISPTICWAdminGuide-overview.pdf
[27] Stevie Chancellor, Jessica Annette Pater, Trustin Clear, Eric Gilbert, and Munmun De Choudhury. 2016. # thyghgapp: Instagram content moderation and lexical variation in pro-eating disorder communities. In *Proceedings of the Conference on Computer-Supported Cooperative Work & Social Computing (CSCW)*. ACM, New York, NY, USA, 1201–1213. https://doi.org/10.1145/2818048.2819963
[28] Janet X. Chen, Francesco Vitale, and Joanna McGrenere. 2021. What Happens After Death? Using a Design Workbook to Understand User Expectations for Preparing Their Data. In *Proceedings of the Conference on Human Factors in Computing Systems (CHI)*. ACM, New York, NY, USA, 169:1–169:13. https://doi.org/10.1145/3411764.3445359
[29] Kendra Cherry. September 13, 2020. The Color Psychology of Red. Retrieved August 28, 2021 from https://www.verywellmind.com/the-color-psychology-of-red-2795821
[30] Alexander Cho. 2018. Default publicness: Queer youth of color, social media, and being outed by the machine. *New Media & Society* 20, 9 (2018), 3183–3200. https://doi.org/10.1177/1461444817744784
[31] Sabrina Cipolletta, Riccardo Votadoro, and Elena Faccio. 2017. Online support for transgender people: an analysis of forums and social networks. *Health & Social Care in the Community* 25, 5 (2017), 1542–1551. https://doi.org/10.1111/hsc.12448
[32] Patricia Hill Collins. 2002. *Black feminist thought: Knowledge, consciousness, and the politics of empowerment*. Routledge, Milton Park, Oxfordshire, UK.
[33] Patricia Hill Collins and Sirma Bilge. 2020. *Intersectionality*. John Wiley & Sons, Hoboken, NJ, USA.
[34] Committee on Temporary Shelter. 2018. Trauma-informed design. Retrieved September 6, 2021 from https://cotsonline.org/2018/04/27/trauma-informed-design/
[35] Sasha Costanza-Chock. 2020. *Design justice: Community-led practices to build the worlds we need*. The MIT Press, Cambridge, MA, USA.
[36] Stephanie S Covington. 2008. Women and addiction: A trauma-informed approach. *Journal of psychoactive drugs* 40, sup5 (2008), 377–385. https://doi.org/10.1080/02791072.2008.10400665
[37] Kimberlé Crenshaw. 1989. Demarginalizing the intersection of race and sex: A black feminist critique of antidiscrimination doctrine, feminist theory and antiracist politics. *University of Chicago Legal Forum* 1989, 1 (1989), 139–167. https://chicagounbound.uchicago.edu/uclf/vol1989/iss1/8/
[38] Kimberle Crenshaw. 1990. Mapping the margins: Intersectionality, identity politics, and violence against women of color. *Stanford Law Review* 43, 6 (1990), 1241–1299. https://doi.org/10.2307/1229039
[39] Darren W Davis. 1997. The direction of race of interviewer effects among African-Americans: Donning the black mask. *American Journal of Political Science* 41, 1 (1997), 309–322. https://doi.org/10.2307/2111718
[40] Avery Decker. 2021. To Build Gentler Technology, Practice Trauma-Informed Design. Retrieved January 5, 2022 from https://medium.com/care-code/to-build-gentler-technology-practice-trauma-informed-design-3b4ad34a9f0b
[41] Ashley Deeks. 2019. The judicial demand for explainable artificial intelligence. *Columbia Law Review* 119, 7 (2019), 1829–1850. https://www.jstor.org/stable/26810851
[42] Bessel A. Van der Kolk. 2015. *The Body Keeps the Score: Brain, Mind, and Body in the Healing of Trauma*. Penguin Books, City of Westminster, London, UK.
[43] Megan Rose Dickey. 2019. The future of diversity and inclusion in tech. Retrieved September 6, 2021 from https://techcrunch.com/2019/06/17/the-future-of-diversity-and-inclusion-in-tech/
[44] Sarah Dokkedahl, Robin Niels Kok, Siobhan Murphy, Trine Rønde Kristensen, Ditte Bech-Hansen, and Ask Elklit. 2019. The Psychological Subtype of Intimate Partner Violence and Its Effect on Mental Health: Protocol for a Systematic Review and Meta-Analysis. *Systematic Reviews* 8, 1 (2019), 198. https://doi.org/10.1186/s13643-019-1118-1
[45] Lynn Dombrowski, Ellie Harmon, and Sarah Fox. 2016. Social justice-oriented interaction design: Outlining key design strategies and commitments. In *Proceedings of the Conference on Designing Interactive Systems (DIS)*. ACM, New York, NY, USA, 656–671. https://doi.org/10.1145/2901790.2901861
[46] Brianna Dym, Jed R. Brubaker, Casey Fiesler, and Bryan Semaan. 2019. "Coming Out Okay": Community Narratives for LGBTQ Identity Recovery Work. *Proceedings of the ACM on Human-Computer Interaction* 3, CSCW (2019), 154:1–154:28. https://doi.org/10.1145/3359256
[47] Denise E. Elliott, Paula Bjelajac, Roger D. Fallot, Laurie S. Markoff, and Beth Glover Reed. 2005. Trauma-Informed or Trauma-Denied: Principles and Implementation of Trauma-Informed Services for Women. *Journal of Community Psychology* 33, 4 (2005), 461–477. https://doi.org/10.1002/jcop.20063
[48] Roberto Encarnación, Cesar Collazos, Habib M. Fardoun, and Daniyal Alghazzawi. 2019. Information Architecture in the Development of Virtual Applications for the Rehabilitation of Patients with PTSD: Case: Defense Avoidance and Schok Mechanisms. In *Proceedings of the Workshop on ICTs for Improving Patients Rehabilitation Research Techniques*. ACM, New York, NY, USA, 23–34. https://doi.org/10.1145/3364138.3364146
[49] Sheena Erete, Yolanda A Rankin, and Jakita O Thomas. 2021. I can't breathe: Reflections from black women in CSCW and HCI. *Proceedings of the ACM on Human-Computer Interaction* 4, CSCW3 (2021), 234:1–234:23. https://doi.org/10.1145/3432933
[50] Virginia Eubanks. 2018. *Automating inequality: How high-tech tools profile, police, and punish the poor*. St. Martin's Press, New York, NY, USA.
[51] Hayley Evans, Udaya Lakshmi, Hue Watson, Azra Ismail, Andrew M. Sherrill, Neha Kumar, and Rosa I. Arriaga. 2020. Understanding the Care Ecologies of Veterans with PTSD. In *Proceedings of the Conference on Human Factors in Computing Systems (CHI)*. ACM, New York, NY, USA, 43:1–43:15. https://doi.org/10.1145/3313831.3376170
[52] Facebook. 2021. What are my ad preferences and how can I adjust them on Facebook? Retrieved August 31, 2021 from https://www.facebook.com/help/247395082112892
[53] Roger D. Fallot and Maxine Harris. 2009. *Creating cultures of trauma-informed care (CCTIC): A self-assessment and planning protocol*. Technical Report. Community Connections, Washington DC, USA. https://www.theannainstitute.org/CCTICSELFASSPP.pdf
[54] Casey Fiesler and Nicholas Proferes. 2018. "Participant" Perceptions of Twitter Research Ethics. *Social Media + Society* 4, 1 (2018), 1–14. https://doi.org/10.1177/2056305118763366
[55] Forbrukerrådet. 2018. *Deceived by Design: How tech companies use dark patterns to discourage us from exercising our rights to privacy*. Technical Report. Norwegian Consumer Council. https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf.
[56] 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 Conference on Human Factors in Computing Systems (CHI)*. ACM, New York, NY, USA, 667:1—-667:13. https://doi.org/10.1145/3173574.3174241
[57] Linda Garnets, Gregory M. Herek, and Barrie Levy. 1990. Violence and Victimization of Lesbians and Gay Men: Mental Health Consequences. *Journal of Interpersonal Violence* 5, 3 (1990), 366–383. https://doi.org/10.1177/088626090005003010
[58] Neha Gill. 2019. The Importance Of Trauma-Informed Design. Retrieved September 6, 2021 from https://www.forbes.com/sites/forbesnonprofitcouncil/2019/12/09/the-importance-of-trauma-informed-design
[59] David Glodstein, Susan L Glodstein, and James Fornaro. 2010. Fraud Trauma Syndrome: The Victims of the Bernard Madoff Scandal. *Journal of Forensic Studies in Accounting & Business* 2, 1 (2010), 1–9.
[60] Robyn L. Gobin and Jennifer J. Freyd. 2014. The Impact of Betrayal Trauma on the Tendency to Trust. *Psychological Trauma: Theory, Research, Practice, and Policy* 6, 5 (2014), 505–511. https://doi.org/10.1037/a0032452
[61] Katelyn Golladay and Kristy Holtfreter. 2017. The consequences of identity theft victimization: An examination of emotional and physical health outcomes. *Victims & Offenders* 12, 5 (2017), 741–760. https://doi.org/10.1080/15564886.2016.1177766
[62] Lauren Goode. 2021. I Called Off My Wedding. The Internet Will Never Forget. Retrieved August 29, 2021 from https://www.wired.com/story/weddings-social-media-apps-photos-memories-miscarriage-problem/

[63] Lisa A. Goodman, Leonard Saxe, and Mary Harvey. 1991. Homelessness as psychological trauma: Broadening perspectives. *American Psychologist* 46, 11 (1991), 1219–1225. https://doi.org/10.1037/0003-066X.46.11.1219

[64] Mitchell L Gordon, Kaitlyn Zhou, Kayur Patel, Tatsunori Hashimoto, and Michael S Bernstein. 2021. The disagreement deconvolution: Bringing machine learning performance metrics in line with reality. In *Proceedings of the Conference on Human Factors in Computing Systems (CHI)*. ACM, New York, NY, USA, 388:1–388:14. https://doi.org/10.1145/3411764.3445423

[65] Mary L Gray and Siddharth Suri. 2019. *Ghost work: How to stop Silicon Valley from building a new global underclass*. Mariner Books, New York, NY, USA.

[66] Stephanie Greer, Danielle Ramo, Yin-Juei Chang, Michael Fu, Judith Moskowitz, and Jana Haritatos. 2019. Use of the chatbot "vivibot" to deliver positive psychology skills and promote well-being among young people after cancer treatment: randomized controlled feasibility trial. *JMIR Mhealth Uhealth* 7, 10 (2019), e15018. https://doi.org/10.2196/15018

[67] Linda J Griffith and S David Leonard. 1997. Association of colors with warning signal words. *International Journal of Industrial Ergonomics* 20, 4 (1997), 317–325. https://doi.org/10.1016/S0169-8141(96)00062-5

[68] Hana Habib, Sarah Pearman, Jiamin Wang, Yixin Zou, Alessandro Acquisti, Lorrie Faith Cranor, Norman Sadeh, and Florian Schaub. 2020. "It's a scavenger hunt": Usability of Websites' Opt-Out and Data Deletion Choices. In *Proceedings of the Conference on Human Factors in Computing Systems (CHI)*. ACM, New York, NY, USA, 384:1–384:12. https://doi.org/10.1145/3313831.3376511

[69] Oliver Haimson, Daniel Delmonaco, Peipei Nie, and Andrea Wegner. 2021. Disproportionate Removals and Differing Content Moderation Experiences for Conservative, Transgender, and Black Social Media Users: Marginalization and Moderation Gray Areas. *Proceedings of the ACM on Human-Computer Interaction* 5, CSCW2 (2021), 466:1–466:35.

[70] 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 Conference on Computer Supported Cooperative Work & Social Computing (CSCW)*. ACM, New York, NY, USA, 1176–1190. https://doi.org/10.1145/2675133.2675152

[71] Oliver L Haimson, Justin Buss, Zu Weinger, Denny L Starks, Dykee Gorrell, and Briar Sweetbriar Baron. 2020. Trans Time: Safety, Privacy, and Content Warnings on a Transgender-Specific Social Media Site. *Proceedings of the ACM on Human-Computer Interaction* 4, CSCW2 (2020), 124:1–124:27. https://doi.org/10.1145/3415195

[72] Rochelle F. Hanson and Jason Lang. 2016. A Critical Look At Trauma-Informed Care Among Agencies and Systems Serving Maltreated Youth and Their Families. *Child Maltreatment* 21, 2 (2016), 95–100. https://doi.org/10.1177/1077559516635274

[73] Erika Harrell. 2021. *Victims of identity theft, 2018*. Technical Report. U.S. Department of Justice. https://bjs.ojp.gov/content/pub/pdf/vit18.pdf

[74] Maxine Harris and Roger D. Fallot. 2001. Designing Trauma-Informed Addictions Services. *New Directions for Mental Health Services* 2001, 89 (2001), 57–73. https://doi.org/10.1002/yd.23320018907

[75] Steve Harrison, Phoebe Sengers, and Deborah Tatar. 2011. Making epistemological trouble: Third-paradigm HCI as successor science. *Interacting with computers* 23, 5 (2011), 385–392. https://doi.org/10.1016/j.intcom.2011.03.005

[76] Morit Heitzler. 2013. Broken boundaries, invaded territories: The challenges of containment in trauma work. *International Body Psychotherapy Journal* 12, 1 (2013), 28–41. https://www.ibpj.org/issues/articles/Heitzler%20-%20Broken%20Boundaries%20Invaded%20Territories.pdf

[77] Tad Hirsch, Kritzia Merced, Shrikanth Narayanan, Zac E Imel, and David C Atkins. 2017. Designing contestability: Interaction design, machine learning, and mental health. In *Proceedings of the Conference on Designing Interactive Systems (DIS)*. ACM, New York, NY, USA, 95–99. https://doi.org/10.1145/3064663.3064703

[78] Esther Howe, Paola Pedrelli, Robert Morris, Maren Nyer, David Mischoulon, and Rosalind Picard. 2017. Feasibility of an Automated System Counselor for Survivors of Sexual Assault. *Iproceedings* 3, 1 (2017), e8585. https://doi.org/10.2196/iproc.8585

[79] Matthew Hutson. 2021. The opacity of artificial intelligence makes it hard to tell when decision-making is biased. *IEEE Spectrum* 58, 2 (2021), 40–45. https://doi.org/10.1109/MSPEC.2021.9340114

[80] Identity Theft Resource Center. 2018. *The Aftermath: The Non-Economic Impacts of Identity Theft*. Technical Report. Identity Theft Resource Center. https://www.idtheftcenter.org/aftermath2018/

[81] Identity Theft Resource Center. 2021. *Consumer Aftermath Report: How Identity Crimes Impact Victims, their Families, Friends and Workplaces*. Technical Report. Identity Theft Resource Center. https://www.idtheftcenter.org/identity-theft-aftermath-study/

[82] Jane Im, Jill Dimond, Melody Berton, Una Lee, Katherine Mustelier, Mark S Ackerman, and Eric Gilbert. 2021. Yes: Affirmative Consent as a Theoretical Framework for Understanding and Imagining Social Platforms. In *Proceedings of the Conference on Human Factors in Computing Systems (CHI)*. ACM, New York, NY, USA, 403:1–403:18. https://doi.org/10.1145/3411764.3445778

[83] Lilly Irani, Janet Vertesi, Paul Dourish, Kavita Philip, and Rebecca E Grinter. 2010. Postcolonial computing: a lens on design and development. In *Proceedings of the Conference on Human Factors in Computing Systems (CHI)*. ACM, New York, NY, USA, 1311–1320. https://doi.org/10.1145/1753326.1753522

[84] Sandy E. James, Jody L Herman, Susan Rankin, Mara Keisling, LIsa Mottet, and Ma'ayan Anafi. 2016. *The Report of the 2015 U.S. Transgender Survey*. Technical Report. National Center for Transgender Equality. http://www.transequality.org/sites/default/files/docs/USTS-Full-Report-FINAL.PDF

[85] Elizabeth K Hopper, Ellen L Bassuk, and Jeffrey Olivet. 2010. Shelter from the storm: Trauma-informed care in homelessness services settings. *The Open Health Services and Policy Journal* 3, 1 (2010), 80–100. https://doi.org/10.2174/1874924001003010080

[86] Gunnur Karakurt, Douglas Smith, and Jason Whiting. 2014. Impact of Intimate Partner Violence on Women's Mental Health. *Journal of Family Violence* 29, 7 (2014), 693–702. https://doi.org/10.1007/s10896-014-9633-2

[87] Nancy Kassam-Adams, Susan Rzucidlo, Marie Campbell, Grace Good, Erin Bonifacio, Kimberly Slouf, Stephanie Schneider, Christine McKenna, Carol A. Hanson, and Donna Grather. 2015. Nurses' Views and Current Practice of Trauma-Informed Pediatric Nursing Care. *Journal of Pediatric Nursing* 30, 3 (2015), 478–484. https://doi.org/10.1016/j.pedn.2014.11.008

[88] Os Keyes. 2018. The Misgendering Machines: Trans/HCI Implications of Automatic Gender Recognition. *Proceedings of the ACM on Human-Computer Interaction* 2, CSCW (2018), 88:1–88:22. https://doi.org/10.1145/3274357

[89] Vanessa Kitzie. 2018. "I pretended to be a boy on the Internet": Navigating affordances and constraints of social networking sites and search engines for LGBTQ+ identity work. *First Monday* 23, 7 (2018), 1. https://doi.org/10.5210/fm.v23i7.9264

[90] Bran Knowles, Mark Rouncefield, Mike Harding, Nigel Davies, Lynne Blair, James Hannon, John Walden, and Ding Wang. 2015. Models and patterns of trust. In *Proceedings of the Conference on Computer Supported Cooperative Work & Social Computing*. ACM, New York, NY, USA, 328–338. https://doi.org/10.1145/2675133.2675154

[91] Amy J. Ko. 2019. 100 hours of name change labor. Retrieved August 29, 2021 from https://medium.com/bits-and-behavior/100-hours-of-name-change-labor-c652c22a89b9

[92] Amy J. Ko. 2020. Taking refuge from the internet. Retrieved August 29, 2021 from https://medium.com/bits-and-behavior/taking-refuge-from-the-internet-9c1c521a5a56

[93] Kyriakos N Kotsoglou and Marion Oswald. 2020. The long arm of the algorithm? Automated Facial Recognition as evidence and trigger for police intervention. *Forensic Science International: Synergy* 2 (2020), 86–89. https://doi.org/10.1016/j.fsisyn.2020.01.002

[94] Shanti Kulkarni. 2019. Intersectional trauma-informed intimate partner violence (IPV) services: Narrowing the gap between IPV service delivery and survivor needs. *Journal of Family Violence* 34, 1 (2019), 55–64. https://doi.org/10.1007/s10896-018-0001-5

[95] Jonathan Lazar, Jinjuan Heidi Feng, and Harry Hochheiser. 2017. *Research methods in human-computer interaction*. Morgan Kaufmann, San Francisco, CA, USA.

[96] Ada Lerner, Helen Yuxun He, Anna Kawakami, Silvia Catherine Zeamer, and Roberto Hoyle. 2020. Privacy and Activism in the Transgender Community. In *Proceedings of the Conference on Human Factors in Computing Systems (CHI)*. ACM, New York, NY, USA, 212:1–212:13. https://doi.org/10.1145/3313831.3376339

[97] Jill Levenson. 2017. Trauma-Informed Social Work Practice. *Social Work* 62, 2 (April 2017), 105–113. https://doi.org/10.1093/sw/swx001

[98] Yuan Li, Adel Yazdanmehr, Jingguo Wang, and H Raghav Rao. 2019. Responding to identity theft: A victimization perspective. *Decision Support Systems* 121 (2019), 13–24. https://doi.org/10.1016/j.dss.2019.04.002

[99] Calvin A Liang, Sean A Munson, and Julie A Kientz. 2021. Embracing Four Tensions in Human-Computer Interaction Research with Marginalized People. *ACM Transactions on Computer-Human Interaction* 28, 2 (2021), 1–47. https://doi.org/10.1145/3443686

[100] Ann Light. 2011. HCI as heterodoxy: Technologies of identity and the queering of interaction with computers. *Interacting with computers* 23, 5 (2011), 430–438. https://doi.org/10.1016/j.intcom.2011.02.002

[101] Bingjie Liu and S Shyam Sundar. 2018. Should machines express sympathy and empathy? Experiments with a health advice chatbot. *Cyberpsychology, Behavior, and Social Networking* 21, 10 (2018), 625–636. https://doi.org/10.1089/cyber.2018.0110

[102] 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. https://doi.org/10.1300/J082v42n01_05

[103] Steven H Lopez, Randy Hodson, and Vincent J Roscigno. 2009. Power, status, and abuse at work: General and sexual harassment compared. *The Sociological Quarterly* 50, 1 (2009), 3–27. https://www.jstor.org/stable/40220119

[104] Gale M Lucas, Albert Rizzo, Jonathan Gratch, Stefan Scherer, Giota Stratou, Jill Boberg, and Louis-Philippe Morency. 2017. Reporting Mental Health Symptoms: Breaking Down Barriers to Care with Virtual Human Interviewers. *Frontiers in Robotics and AI* 4 (2017), 51:1–51:9. https://doi.org/10.3389/frobt.2017.00051

[105] Meghan L Marsac, Nancy Kassam-Adams, Aimee K Hildenbrand, Elizabeth Nicholls, Flaura K Winston, Stephen S Leff, and Joel Fein. 2016. Implementing a trauma-informed approach in pediatric health care networks. *JAMA Pediatrics* 170, 1 (2016), 70–77. https://doi.org/10.1001/jamapediatrics.2015.2206

[106] Sandra L Martin, Olivia Silber Ashley, LeBretia White, Sarah Axelson, Marc Clark, and Barri Burrus. 2017. Incorporating trauma-informed care into school-based programs. *Journal of School Health* 87, 12 (2017), 958–967. https://doi.org/10.1111/josh.12568

[107] Michael Massimi and Ronald M. Baecker. 2011. Dealing with Death in Design: Developing Systems for the Bereaved. In *Proceedings of the Conference on Human Factors in Computing Systems (CHI)*. ACM, New York, NY, USA, 1001–1010. https://doi.org/10.1145/1978942.1979092

[108] Arunesh Mathur, Josefine Engel, Sonam Sobti, Victoria Chang, and Marshini Chetty. 2016. "They Keep Coming Back Like Zombies": Improving Software Updating Interfaces. In *Symposium on Usable Privacy and Security*. USENIX Association, Berkeley, CA, USA, 43–58. https://www.usenix.org/system/files/conference/soups2016/soups2016-paper-mathur.pdf

[109] 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 Conference on Human Factors in Computing Systems (CHI)*. ACM, New York, NY, USA, 2189–2201. https://doi.org/10.1145/3025453.3025875

[110] Frank H. McCourt. 2021. The Internet Is Beyond Repair. It's Time to Stop Trying to Fix It. Retrieved January 5, 2022 from https://www.barrons.com/articles/big-tech-has-broken-the-internet-dont-fix-it-rebuild-51637318700

[111] Allison McDonald, Catherine Barwulor, Michelle L Mazurek, Florian Schaub, and Elissa M Redmiles. 2021. "It's stressful having all these phones": Investigating Sex Workers' Safety Goals, Risks, and Practices Online. In *USENIX Security Symposium*. USENIX Association, Berkeley, CA, USA, 375–392. https://www.usenix.org/system/files/sec21-mcdonald.pdf

[112] Carolyn McKay. 2020. Predicting risk in criminal procedure: actuarial tools, algorithms, AI and judicial decision-making. *Current Issues in Criminal Justice* 32, 1 (2020), 22–39. https://doi.org/10.1080/10345329.2019.1658694

[113] D. Harrison Mcknight and Norman L. Chervany. 1996. The Meanings of Trust. Retrieved August 29, 2021 from http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.155.1213

[114] Christopher Menschner and Alexandra Maul. 2016. *Key ingredients for successful trauma-informed care implementation.* Technical Report. Center for Health Care Strategies, Trenton, NJ, USA. https://www.samhsa.gov/sites/default/files/programs_campaigns/childrens_mental_health/atc-whitepaper-040616.pdf

[115] Peter Mertin and Philip B. Mohr. 2001. A Follow-Up Study of Posttraumatic Stress Disorder, Anxiety, and Depression in Australian Victims of Domestic Violence. *Violence and Victims* 16, 6 (2001), 645–54. https://www.proquest.com/docview/808559022/abstract/E7A11D1417BB42BAPQ/1

[116] Microsoft. 2016. Microsoft's AI vision, rooted in research, conversations. Retrieved August 30, 2021 from https://news.microsoft.com/features/microsofts-ai-vision-rooted-in-research-conversations/

[117] Niki A. Miller and Lisa M. Najavits. 2012. Creating Trauma-Informed Correctional Care: A Balance of Goals and Environment. *European Journal of Psychotraumatology* 3, s1 (May 2012), 17246. https://doi.org/10.3402/ejpt.v3i0.17246

[118] Jessica Minahan. 2019. Trauma-informed teaching strategies. Retrieved August 29, 2021 from https://www.ascd.org/el/articles/trauma-informed-teaching-strategies

[119] Dinesh Mittal, Karen L. Drummond, Dean Blevins, Geoffrey Curran, Patrick Corrigan, and Greer Sullivan. 2013. Stigma Associated with PTSD: Perceptions of Treatment Seeking Combat Veterans. *Psychiatric Rehabilitation Journal* 36, 2 (2013), 86–92. https://doi.org/10.1037/h0094976

[120] Lauren Mizock and Thomas K. Lewis. 2008. Trauma in Transgender Populations: Risk, Resilience, and Clinical Care. *Journal of Emotional Abuse* 8, 3 (2008), 335–354. https://doi.org/10.1080/10926790802262523

[121] Mainack Mondal, Johnnatan Messias, Saptarshi Ghosh, Krishna P Gummadi, and Aniket Kate. 2016. Forgetting in social media: Understanding and controlling longitudinal exposure of socially shared data. In *Symposium on Usable Privacy and Security*. USENIX Association, Berkeley, CA, USA, 287–299. https://www.usenix.org/system/files/conference/soups2016/soups2016-paper-mondal.pdf

[122] Carol Moser, Sarita Y Schoenebeck, and Paul Resnick. 2019. Impulse buying: Design practices and consumer needs. In *Proceedings of the Conference on Human Factors in Computing Systems (CHI)*. ACM, New York, NY, USA, 242:1–242:15. https://doi.org/10.1145/3290605.3300472

[123] Roberto Encarnación Mosquera, Habib M Fardoun, Daniyal Alghazzawi, Cesar Collazos, and Víctor M Ruiz Penichet. 2018. Design guidelines for the implementation of an interactive virtual reality application that supports the rehabilitation of amputees of lower limbs patients with post-traumatic stress disorder (PTSD). In *HCI International 2018 – Posters' Extended Abstracts*. Springer, New York, NY, USA, 17–31. https://doi.org/10.1007/978-3-319-92279-9_3

[124] Nasim Motalebi and Saeed Abdullah. 2018. Conversational agents to provide couple therapy for patients with PTSD. In *Proceedings of the International Conference on Pervasive Computing Technologies for Healthcare*. ACM, New York, NY, USA, 347–351. https://doi.org/10.1145/3240925.3240933

[125] Deirdre K Mulligan, Daniel Kluttz, and Nitin Kohli. 2019. Shaping our tools: Contestability as a means to promote responsible algorithmic decision making in the professions. Retrieved September 6, 2021 from http://dx.doi.org/10.2139/ssrn.3311894

[126] Coral Muskett. 2014. Trauma-Informed Care in Inpatient Mental Health Settings: A Review of the Literature. *International Journal of Mental Health Nursing* 23, 1 (2014), 51–59. https://doi.org/10.1111/inm.12012

[127] National Women's Law Center. 2018. *Out of the Shadows: An Analysis of Sexual Harassment Charges Filed by Working Women.* Technical Report. National Women's Law Center. https://nwlc.org/wp-content/uploads/2018/08/SexualHarassmentReport.pdf.

[128] Yuval Neria, Evelyn J. Bromet, Sylvia Sievers, Janet Lavelle, and Laura J. Fochtmann. 2002. Trauma Exposure and Posttraumatic Stress Disorder in Psychosis: Findings from a First-Admission Cohort. *Journal of Consulting and Clinical Psychology* 70, 1 (2002), 246–251. https://doi.org/10.1037/0022-006X.70.1.246

[129] Jakob Nielsen and Rolf Molich. 1990. Heuristic Evaluation of User Interfaces. In *Proceedings of the Conference on Human Factors in Computing Systems (CHI)*. ACM, New York, NY, USA, 249–256. https://doi.org/10.1145/97243.97281

[130] Ihudiya Finda Ogbonnaya-Ogburu, Angela DR Smith, Alexandra To, and Kentaro Toyama. 2020. Critical race theory for HCI. In *Proceedings of the Conference on Human Factors in Computing Systems (CHI)*. ACM, New York, NY, USA, 265:1–265:16. https://doi.org/10.1145/3313831.3376392

[131] Kathleen O'Leary, Arpita Bhattacharya, Sean A Munson, Jacob O Wobbrock, and Wanda Pratt. 2017. Design opportunities for mental health peer support technologies. In *Proceedings of the Conference on Computer Supported Cooperative Work & Social Computing*. ACM, New York, NY, USA, 1470–1484. https://doi.org/10.1145/2998181.2998349

[132] Resmiye Oral, Marizen Ramirez, Carol Coohey, Stephanie Nakada, Amy Walz, Angela Kuntz, Jenna Benoit, and Corinne Peek-Asa. 2016. Adverse Childhood Experiences and Trauma Informed Care: The Future of Health Care. *Pediatric Research* 79, 1 (2016), 227–233. https://doi.org/10.1038/pr.2015.197

[133] World Health Organization and Pan American Health Organization. 2012. *Understanding and addressing violence against women: intimate partner violence.* Technical Report. World Health Organization. https://apps.who.int/iris/handle/10665/77432

[134] Kentrell Owens, Camille Cobb, and Lorrie Cranor. 2021. "You Gotta Watch What You Say": Surveillance of Communication with Incarcerated People. In *Proceedings of the Conference on Human Factors in Computing Systems (CHI)*. ACM, New York, NY, USA, 62:1–62:18. https://doi.org/10.1145/3411764.3445055

[135] Nirmita Panchal, Rabah Kamal, Cynthia Cox, and Rachel Garfield. 2021. The Implications of COVID-19 for Mental Health and Substance Use. Retrieved September 6, 2021 from https://www.kff.org/coronavirus-covid-19/issue-brief/the-implications-of-covid-19-for-mental-health-and-substance-use/

[136] Deuk Hee Park, Hyea Kyeong Kim, Il Young Choi, and Jae Kyeong Kim. 2012. A literature review and classification of recommender systems research. *Expert systems with applications* 39, 11 (2012), 10059–10072. https://doi.org/10.1016/j.eswa.2012.02.038

[137] Sarah M. Peitzmeier, Mannat Malik, Shanna K. Kattari, Elliot Marrow, Rob Stephenson, Madina Agénor, and Sari L. Reisner. 2020. Intimate Partner Violence in Transgender Populations: Systematic Review and Meta-Analysis of Prevalence and Correlates. *American Journal of Public Health* 110, 9 (2020), e1–e14. https://doi.org/10.2105/AJPH.2020.305774

[138] Sarah Perez. 2019. Twitter launches a way to report abusive use of its Lists feature. Retrieved August 29, 2021 from https://techcrunch.com/2019/11/18/twitter-launches-a-way-to-report-abusive-use-of-its-lists-feature/

[139] Diana L. Perry and Monica L. Daniels. 2016. Implementing Trauma—Informed Practices in the School Setting: A Pilot Study. *School Mental Health: A Multidisciplinary Research and Practice Journal* 8, 1 (2016), 177–188. https://doi.org/10.1007/s12310-016-9182-3

[140] Justin Petelka, Yixin Zou, and Florian Schaub. 2019. Put your warning where your link is: Improving and evaluating email phishing warnings. In *Proceedings of the Conference on Human Factors in Computing Systems (CHI)*. ACM, New York, NY, USA, 518:1–518:15. https://doi.org/10.1145/3290605.3300748

[141] Anthony T. Pinter, Morgan Klaus Scheuerman, and Jed R. Brubaker. 2021. Entering Doors, Evading Traps: Benefits and Risks of Visibility During Transgender Coming Outs. *Proceedings of the ACM on Human-Computer Interaction* 4, CSCW3 (2021), 272:1–272:27. https://doi.org/10.1145/3434181

[142] Nicole Leeper Piquero, Mark A Cohen, and Alex R Piquero. 2011. How much is the public willing to pay to be protected from identity theft? *Justice Quarterly* 28, 3 (2011), 437–459. https://doi.org/10.1080/07418825.2010.511245

[143] Thomas Ploug and Søren Holm. 2020. The four dimensions of contestable AI diagnostics-A patient-centric approach to explainable AI. *Artificial Intelligence*

in Medicine 107 (2020), 101901. https://doi.org/10.1016/j.artmed.2020.101901

[144] Nicholas Proferes, Naiyan Jones, Sarah Gilbert, Casey Fiesler, and Michael Zimmer. 2021. Studying Reddit: A Systematic Overview of Disciplines, Approaches, Methods, and Ethics. *Social Media+ Society* 7, 2 (2021), 1–14. https://doi.org/10.1177/20563051211019004

[145] Public Health Agency of Canada. 2018. Trauma and Violence-Informed Approaches to Policy and Practice. Retrieved August 29, 2021 from https://www.canada.ca/en/public-health/services/publications/health-risks-safety/trauma-violence-informed-approaches-policy-practice.html

[146] Hawra Rabaan. 2021. Exploring Transformative Justice Principles to Inform Survivor-Centered Design for Muslim Women in the United States. In *Companion Publication of the Conference on Computer Supported Cooperative Work and Social Computing*. ACM, New York, NY, USA, 291–294. https://doi.org/10.1145/3462204.3481797

[147] Sheela Raja, Memoona Hasnain, Michelle Hoersch, Stephanie Gove-Yin, and Chelsea Rajagopalan. 2015. Trauma informed care in medicine. *Family & community health* 38, 3 (2015), 216–226. https://doi.org/10.1097/FCH.0000000000000071

[148] Inioluwa Deborah Raji, Timnit Gebru, Margaret Mitchell, Joy Buolamwini, Joonseok Lee, and Emily Denton. 2020. Saving face: Investigating the ethical concerns of facial recognition auditing. In *Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society*. ACM, New York, NY, USA, 145–151. https://doi.org/10.1145/3375627.3375820

[149] Ryan Randa and Bradford W Reyns. 2020. The physical and emotional toll of identity theft victimization: A situational and demographic analysis of the National Crime Victimization Survey. *Deviant Behavior* 41, 10 (2020), 1290–1304. https://doi.org/10.1080/01639625.2019.1612980

[150] Usha Ranji, Brittni Frederiksen, Alina Salganicoff, and Michelle Long. 2021. *Women, Work, and Family During COVID-19: Findings from the KFF Women's Health Survey*. Technical Report. Kaiser Family Foundation. https://www.kff.org/womens-health-policy/issue-brief/women-work-and-family-during-covid-19-findings-from-the-kff-womens-health-survey/

[151] Yolanda A Rankin and Jakita O Thomas. 2019. Straighten up and fly right: Rethinking intersectionality in HCI research. *Interactions* 26, 6 (2019), 64–68. https://doi.org/10.1145/3363033

[152] Elizabeth Reeves. 2015. A Synthesis of the Literature on Trauma-Informed Care. *Issues in Mental Health Nursing* 36, 9 (Sept. 2015), 698–709. https://doi.org/10.3109/01612840.2015.1025319

[153] Carrie W Rishel, Jiyoung K Tabone, Helen P Hartnett, and Kathy F Szafran. 2019. Trauma-Informed Elementary Schools: Evaluation of School-Based Early Intervention for Young Children. *Children & Schools* 41, 4 (2019), 239–248. https://doi.org/10.1093/cs/cdz017

[154] Sarah T Roberts. 2019. *Behind the Screen: Content Moderation in the Shadows of Social Media*. Yale University Press, New Haven, CT, USA.

[155] Heather Rosoff, Jinshu Cui, and Richard John. 2014. Behavioral experiments exploring victims' response to cyber-based financial fraud and identity theft scenario simulations. In *Symposium On Usable Privacy and Security*. USENIX Association, Berkeley, CA, USA, 175–186. https://www.usenix.org/system/files/conference/soups2014/soups14-paper-rosoff.pdf

[156] Cynthia Rudin. 2019. Stop explaining black box machine learning models for high stakes decisions and use interpretable models instead. *Nature Machine Intelligence* 1, 5 (2019), 206–215. https://www.nature.com/articles/s42256-019-0048-x

[157] Jo Rycroft-Malone, Christopher Burton, Joyce E Wilkinson, Gill Harvey, Brendan McCormack, Richard Baker, Sue Dopson, Ian Graham, Sophie Staniszewska, Carl Thompson, et al. 2015. *Collective action for knowledge moblisation: a realist evaluation of the collaborations for leadership in applied Health Research and care*. Technical Report. National Institute for Health Research. https://www.ncbi.nlm.nih.gov/books/NBK332950/

[158] Christian Sandvig, Kevin Hamilton, Karrie Karahalios, and Cedric Langbort. 2014. Auditing algorithms: Research methods for detecting discrimination on internet platforms. In *Data and Discrimination: Converting Critical Concerns into Productive Inquiry*. International Communication Association, Seattle, WA, USA, 1–23. https://social.cs.uiuc.edu/papers/pdfs/ICA2014-Sandvig.pdf

[159] Brenda K Savage. 2016. Race-of-interviewer effects and survey questions about police violence. *Sociological Spectrum* 36, 3 (2016), 142–157. https://doi.org/10.1080/02732173.2015.1110508

[160] Devansh Saxena, Karla Badillo-Urquiola, Pamela J Wisniewski, and Shion Guha. 2020. A Human-Centered Review of Algorithms used within the US Child Welfare System. In *Proceedings of the Conference on Human Factors in Computing Systems (CHI)*. ACM, New York, NY, USA, 102:1–102:15. https://doi.org/10.1145/3313831.3376229

[161] Scamwatch. 2021. Identity theft: I lost $6028 when scammers stole my identity. Retrieved August 29, 2021 from https://www.scamwatch.gov.au/get-help/real-life-stories/scam-victims-tell-us-their-stories/identity-theft-i-lost-6028-when-scammers-stole-my-identity

[162] Florian Schaub and Lorrie Faith Cranor. 2020. Usable and Useful Privacy Interfaces. In *An Introduction to Privacy for Technology Professionals*, Travis D Breaux (Ed.). International Association of Privacy Professionals, Portsmouth, NH, USA, 176–238. https://iapp.org/media/pdf/certification/IAPP-Intro-to-Privacy-for-Tech-Prof-SAMPLE.pdf.

[163] 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 (2018), 155:1–155:27. https://doi.org/10.1145/3274424

[164] Dawn Schlecht. 2021. A Step-By-Step Guide To User Experience (UX) Patterns. Retrieved August 29, 2021 from https://careerfoundry.com/en/blog/ux-design/ux-patterns-why-use-them/

[165] Ari Schlesinger, W Keith Edwards, and Rebecca E Grinter. 2017. Intersectional HCI: Engaging identity through gender, race, and class. In *Proceedings of the Conference on Human Factors in Computing Systems (CHI)*. ACM, New York, NY, USA, 5412–5427. https://doi.org/10.1145/3025453.3025766

[166] Sarita Schoenebeck, Oliver L Haimson, and Lisa Nakamura. 2021. Drawing from justice theories to support targets of online harassment. *New Media & Society* 23, 5 (2021), 1278–1300. https://doi.org/10.1177/1461444820913122 arXiv:https://doi.org/10.1177/1461444820913122

[167] Sarita Schoenebeck, Carol F. Scott, Emma Grace Hurley, Tammy Chang, and Ellen Selkie. 2021. Youth Trust in Social Media Companies and Expectations of Justice: Accountability and Repair After Online Harassment. *Proc. ACM Hum.-Comput. Interact.* 5, CSCW1, Article 2 (apr 2021), 18 pages. https://doi.org/10.1145/3449076

[168] Farhana Shahid, Wasifur Rahman, M. Saifur Rahman, Sharmin Akther Purabi, Ayesha Seddiqa, Moin Mostakim, Farhan Feroz, Tanjir Rashid Soron, Fahmida Hossain, Nabila Khan, Anika Binte Islam, Nipi Paul, Ehsan Hoque, and A. B. M. Alim Al Islam. 2020. Leveraging Free-Hand Sketches for Potential Screening of PTSD. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 4, 3 (2020), 94:1–94:22. https://doi.org/10.1145/3411835

[169] Ruth Shillair, Shelia R Cotten, Hsin-Yi Sandy Tsai, Saleem Alhabash, Robert LaRose, and Nora J Rifon. 2015. Online safety begins with you and me: Convincing Internet users to protect themselves. *Computers in Human Behavior* 48 (2015), 199–207. https://doi.org/10.1016/j.chb.2015.01.046

[170] Donghee Shin. 2020. User perceptions of algorithmic decisions in the personalized AI system: perceptual evaluation of fairness, accountability, transparency, and explainability. *Journal of Broadcasting & Electronic Media* 64, 4 (2020), 541–565. https://doi.org/10.1080/08838151.2020.1843357

[171] Emrys Shoemaker, Gudrun Svava Kristinsdottir, Tanuj Ahuja, Dina Baslan, Bryan Pon, Paul Currion, Pius Gumisizira, and Nicola Dell. 2019. Identity at the Margins: Examining Refugee Experiences with Digital Identity Systems in Lebanon, Jordan, and Uganda. In *Proceedings of the Conference on Computing and Sustainable Societies*. ACM, New York, NY, USA, 206–217. https://doi.org/10.1145/3314344.3332486

[172] Lucy Simko, Ada Lerner, Samia Ibtasam, Franziska Roesner, and Tadayoshi Kohno. 2018. Computer Security and Privacy for Refugees in the United States. In *Symposium on Security and Privacy*. IEEE, New York, NY, USA, 409–423. https://doi.org/10.1109/SP.2018.00023

[173] Ellen Simpson and Bryan Semaan. 2021. For You, or For"You"? Everyday LGBTQ+ Encounters with TikTok. *Proceedings of the ACM on Human-Computer Interaction* 4, CSCW3 (2021), 252:1–252:34. https://doi.org/10.1145/3432951

[174] Julia Slupska and Leonie Maria Tanczer. 2021. Threat Modeling Intimate Partner Violence: Tech Abuse as a Cybersecurity Challenge in the Internet of Things. In *The Emerald International Handbook of Technology Facilitated Violence and Abuse*, Jane Bailey, Asher Flynn, and Nicola Henry (Eds.). Emerald Publishing Limited, Bingley, West Yorkshire, UK, 663–688. https://doi.org/10.1108/978-1-83982-848-520211049

[175] Sharon G Smith, Xinjian Zhang, Kathleen C Basile, Melissa T Merrick, Jing Wang, Marcie-jo Kresnow, and Jieru Chen. 2018. *The National Intimate Partner and Sexual Violence Survey : 2015 Data Brief – Updated Release*. Technical Report. Centers for Disease Control and Prevention. https://stacks.cdc.gov/view/cdc/60893

[176] Katta Spiel, Oliver L Haimson, and Danielle Lottridge. 2019. How to do better with gender on surveys: a guide for HCI researchers. *Interactions* 26, 4 (2019), 62–65. https://doi.org/10.1145/3338283

[177] Katta Spiel, Os Keyes, Ashley Marie Walker, Michael A DeVito, Jeremy Birnholtz, Emeline Brulé, Ann Light, Pınar Barlas, Jean Hardy, Alex Ahmed, et al. 2019. Queer(ing) HCI: Moving forward in theory and practice. In *Extended Abstracts of the Conference on Human Factors in Computing Systems (CHI)*. ACM, New York, NY, USA, 11:1–11:4. https://doi.org/10.1145/3290607.3311750

[178] Miriah Steiger, Timir J Bharucha, Sukrit Venkatagiri, Martin J. Riedl, and Matthew Lease. 2021. The Psychological Well-Being of Content Moderators: The Emotional Labor of Commercial Moderation and Avenues for Improving Support. In *Proceedings of the Conference on Human Factors in Computing Systems (CHI)*. ACM, New York, NY, USA, 341:1–341:14. https://doi.org/10.1145/3411764.3445092

[179] Rock Stevens, Daniel Votipka, Elissa M Redmiles, Colin Ahern, and Michelle L Mazurek. 2019. Applied Digital Threat Modeling: It Works. *IEEE Security & Privacy* 17, 4 (2019), 35–42. https://doi.org/10.1109/MSEC.2019.2909714

[180] Yolande Strengers, Jathan Sadowski, Zhuying Li, Anna Shimshak, and Florian 'Floyd'Mueller. 2021. What Can HCI Learn from Sexual Consent? A Feminist Process of Embodied Consent for Interactions with Emerging Technologies. In *Proceedings of the Conference on Human Factors in Computing Systems (CHI)*. ACM, New York, NY, USA, 405:1–405:13. https://doi.org/10.1145/3411764.3445107

[181] Angelika Strohmayer, Jenn Clamen, and Mary Laing. 2019. Technologies for Social Justice: Lessons from Sex Workers on the Front Lines. In *Proceedings of the Conference on Human Factors in Computing Systems (CHI)*. ACM, New York, NY, USA, 652:1–652:14. https://doi.org/10.1145/3290605.3300882

[182] Chloe Rose Stuart-Ulin. 2018. Microsoft's politically correct chatbot is even worse than its racist one. Retrieved August 30, 2021 from https://qz.com/1340990/microsofts-politically-correct-chat-bot-is-even-worse-than-its-racist-one/

[183] Substance Abuse and Mental Health Services Administration. 2014. SAMHSA's Concept of Trauma and Guidance for a Trauma-Informed Approach. Retrieved August 28, 2021 from https://ncsacw.samhsa.gov/userfiles/files/SAMHSA_Trauma.pdf

[184] Substance Abuse and Mental Health Services Administration. 2016. DSM-IV to DSM-5 Acute Stress Disorder Comparison. Retrieved August 29, 2021 from https://www.ncbi.nlm.nih.gov/books/NBK519704/table/ch3.t30/

[185] Joshua Sunshine, Serge Egelman, Hazim Almuhimedi, Neha Atri, Lorrie Faith Cranor, and Crying Wolf. 2009. An Empirical Study of SSL Warning Effectiveness. In *Usenix Security Symposium*. USENIX Association, Berkeley, CA, USA, 10–14. https://www.usenix.org/legacy/event/sec09/tech/full_papers/sunshine.pdf

[186] Latanya Sweeney. 2013. Discrimination in online ad delivery. *Commun. ACM* 56, 5 (2013), 44–54. https://doi.org/10.1145/2447976.2447990

[187] Yoshimitsu Takahashi, Chiyoko Uchida, Koichi Miyaki, Michi Sakai, Takuro Shimbo, and Takeo Nakayama. 2009. Potential benefits and harms of a peer support social network service on the internet for people with depressive tendencies: qualitative content analysis and social network analysis. *Journal of medical Internet research* 11, 3 (2009), e29. https://doi.org/10.2196/jmir.1142

[188] Jonathan Taplin. 2017. *Move fast and break things: How Facebook, Google, and Amazon have cornered culture and what it means for all of us*. Little, Brown & Company, New York, NY, USA.

[189] The Combahee River Collective. 1986. *The Combahee River Collective Statement: Black Feminist Organizing in the Seventies and Eighties*. Kitchen Table: Women of Color Press, Albany, NY, USA.

[190] The National Child Traumatic Stress Network. 2015. Secondary Traumatic Stress: A Fact Sheet for Organizations Employing Community Violence Workers. Retrieved August 28, 2021 from https://www.nctsn.org/sites/default/files/resources//secondary_traumatic_stress_community_violence_workers.pdf

[191] K. Thomas, D. Akhawe, M. Bailey, D. Boneh, E. Bursztein, S. Consolvo, N. Dell, Z. Durumeric, P. Kelley, D. Kumar, D. McCoy, S. Meiklejohn, T. Ristenpart, and G. Stringhini. 2021. SoK: Hate, Harassment, and the Changing Landscape of Online Abuse. In *Symposium on Security and Privacy*. IEEE, New York, NY, USA, 247–267. https://doi.org/10.1109/SP40001.2021.00028

[192] Jenifer Tidwell. 2010. *Designing interfaces: Patterns for effective interaction design*. O'Reilly Media, Inc., Sebastopol, CA, USA.

[193] Aaron Tilley. 2021. Slack Backtracks on New Way to Message Over Harassment Concern. Retrieved August 29, 2021 from https://www.wsj.com/articles/slack-backtracks-on-new-way-to-message-over-harassment-concern-11616624282

[194] Alexandra To, Wenxia Sweeney, Jessica Hammer, and Geoff Kaufman. 2020. "They Just Don't Get It": Towards Social Technologies for Coping with Interpersonal Racism. *Proceedings of the ACM on Human-Computer Interaction* 4, CSCW1 (2020), 24:1–24:29. https://doi.org/10.1145/3392828

[195] Emily Tseng, Diana Freed, Kristen Engel, Thomas Ristenpart, and Nicola Dell. 2021. A Digital Safety Dilemma: Analysis of Computer-Mediated Computer Security Interventions for Intimate Partner Violence During COVID-19. In *Proceedings of the Conference on Human Factors in Computing Systems (CHI)*. ACM, New York, NY, USA, 71:1–71:17. https://doi.org/10.1145/3411764.3445589

[196] Gordon J Turnbull. 1998. A review of post-traumatic stress disorder. Part I: Historical development and classification. *Injury* 29, 2 (1998), 87–91. https://doi.org/10.1016/S0020-1383(97)00131-9

[197] Laura Van Dernoot Lipsky. 2010. *Trauma stewardship: An everyday guide to caring for self while caring for others*. Berrett-Koehler Publishers, Oakland, CA, USA.

[198] Laura A Voith, Tyrone Hamler, Meredith W Francis, Hyunjune Lee, and Amy Korsch-Williams. 2020. Using a Trauma-Informed, Socially Just Research Framework with Marginalized Populations: Practices and Barriers to Implementation. *Social Work Research* 44, 3 (2020), 169–181. https://doi.org/10.1093/swr/svaa013

[199] Allison Ward-Lasher, Jill Messing, and Jillian Stein-Seroussi. 2017. Implementation of Trauma-Informed Care in a Housing First Program for Survivors of Intimate Partner Violence: A Case Study. *Advances in Social Work* 18, 1 (2017), 202–216. https://doi.org/10.18060/21313

[200] Rick Wash, Emilee Rader, Kami Vaniea, and Michelle Rizor. 2014. Out of the loop: How automated software updates cause unintended security consequences. In *Symposium On Usable Privacy and Security*. USENIX Association, Berkeley, CA, USA, 89–104. https://www.usenix.org/system/files/soups14-paper-wash.pdf

[201] Jamie White. 2014. The Nightmarish Experiences of an Identity Theft Victim. Retrieved August 29, 2021 from https://www.lifelock.com/learn-identity-theft-resources-nightmarish-experiences-identity-theft-victim.html

[202] Joshua M. Wilson, Jenny E. Fauci, and Lisa A. Goodman. 2015. Bringing Trauma-Informed Practice to Domestic Violence Programs: A Qualitative Analysis of Current Approaches. *American Journal of Orthopsychiatry* 85, 6 (2015), 586–599. https://doi.org/10.1037/ort0000098

[203] Marty J Wolf, Keith W Miller, and Frances S Grodzinsky. 2017. Why We Should Have Seen That Coming: Comments on Microsoft's Tay "Experiment," and Wider Implications. *SIGCAS Computers and Society* 47, 3 (2017), 54–64. https://doi.org/10.1145/3144592.3144598

[204] Rebacca Wong. 2021. Guidelines to Incorporate Trauma-Informed Care Strategies in Qualitative Research. Retrieved September 6, 2021 from https://www.urban.org/urban-wire/guidelines-incorporate-trauma-informed-care-strategies-qualitative-research

[205] Yixin Zou, Allison McDonald, Julia Narakornpichit, Nicola Dell, Thomas Ristenpart, Kevin Roundy, Florian Schaub, and Acar Tamersoy. 2021. The Role of Computer Security Customer Support in Helping Survivors of Intimate Partner Violence. In *USENIX Security Symposium*. USENIX Association, Berkeley, CA, USA, 429–446. https://www.usenix.org/system/files/sec21-zou.pdf