Computers in Human Behavior 173 (2025) 108794

Contents lists available at ScienceDirect

Computers in Human Behavior

journal homepage: www.elsevier.com/locate/comphumbeh

From mistrust to confidence: How NeuroTech improves privacy for mistrusted digital environments in a formerly incarcerated population

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

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

ARTICLE INFO

Handling Editor: Dr. Bjorn de Koning

Keywords:
Privacy
Biometric authentication
Biometric access control systems
Incarcerated population

ABSTRACT

As digital platforms increasingly mediate everyday life, privacy-preserving technologies must account for the lived experiences of marginalized users. This study investigates how formerly incarcerated individuals, who often face heightened mistrust and feelings of surveillance with technologies, respond to Biometric Access Systems as a solution for privacy concerns. In Study 1, qualitative findings revealed TikTok, Meta, and video conferencing were the most mistrusted digital platforms, with respondents citing persistent surveillance and a lack of control when engaging with these platforms. In Study 2, we evaluated a novel Biometric Access System – NeuroTech – which uses neuro-vibrational patterns for local authentication. Results showed that NeuroTech significantly reduced privacy concerns and increased user engagement, especially among formerly incarcerated users. The strength of NeuroTech comes from its design, which minimizes surveillance by avoiding facial recognition and eliminates data transmission by granting users local, body-based control over their data. Although formerly incarcerated populations may be skeptical of existing systems, they may be receptive to solutions that empower autonomy, especially if implemented with respect.

1. Introduction

1.1. Importance of privacy

For nearly half a century, scholars have voiced serious concern over the protection of one's informational privacy (Beke et al., 2018; Mason, 1986; Stone et al., 1983). Privacy as a concept can be diverse and complex, including various philosophical and legal theories, and is understood to include numerous attributes including non-intrusion, seclusion, limitation, and control of information about the self. This is commonly referred to as the restricted access/limited control theory of privacy (Tavani, 2007). Tavani (2007) defined privacy as a situation in which one has protection from intrusion and can control one's information by restricting others' access to it.

Our ability to shield private information from intrusion, as well as control information by restricting others' access, is especially relevant in digital environments. Engaging with digital environments is ubiquitous, no longer a luxury but a necessity to participate in modern society. We are no longer limited to desktop computers for internet access; now smartphones, wearable technology, and smart home devices (to name a few) are integral in connecting individuals to the internet anywhere, anytime. Although each of these technologies provide value to people's lives, each also collects private information – whether it is private messages on a smartphone, location on a smartwatch, or voice-activated commands on a smart home device – this data collection can be detrimental to privacy if misused.

As the tracking of daily activities has become widely accessible in a digital world, it is becoming essential that all individuals have adequate protection when engaging with digital environments. Companies now take our personal information and have turned it into the nearly $350 billion business of Big Data that is growing exponentially each year ("Big data analytics market sizeshare & industry analysis, 2024). Nearly every day, we hear about hacks and the mishandling of data, leading to over a billion stolen records as of August 12, 2024, with numbers still rising (Whittaker, 2024). Therefore, it is crucial to discover new strategies to protect personal information that does not rely solely on companies and their cloud-based systems because when privacy is invaded and data are mishandled, the consequences, including the emotional ramifications, extend beyond the online space and into the offline world (Durnell et al., 2020).

* Corresponding author.
E-mail address: eric@aermob.com (E. Durnell).

https://doi.org/10.1016/j.chb.2025.108794
Received 9 February 2025; Received in revised form 9 August 2025; Accepted 7 September 2025
Available online 8 September 2025

1.2. Mistrusted digital environments

Over time, privacy concerns with digital environments have gotten stronger, as users are continuously experiencing largescale data malpractices and data breaches. For example, in 2019, Facebook was sued for allowing Cambridge Analytica to collect data on Facebook, even among those who did not consent to their data being harvested (US v. FB). In 2024, AT&T had a massive data breach leading to nearly 90 million AT&T customers' data, such as text message details, call log history, and personal information, to be stolen (Cybersecurity & Infrastructure Security Agency, 2024).

Beyond the average data breach or the harvesting of one's data without their consent, there is concern about technological discrimination. There has been increasing discussion on the impact of "bad data" and "racist algorithmic models," leading to flawed predictions of marginalized groups and results that are not representative of a diverse population (Peña Gangadharan & Niklas, 2019). Unfortunately, research has demonstrated that this discrimination is pervasive in many areas of life. For example, research has demonstrated that women are not being shown STEM career ads at the same levels as men were, reinforcing the gender gap in STEM (Lambrecht & Tucker, 2019). A study of the accuracy of facial recognition models found that the algorithms performed worse at identifying darker-skinned females than any other group (Raji & Buolamwini, 2019). Whether it is due to data malpractices, data breaches, or discriminatory data practices, there are many reasons why individuals would mistrust digital environments of various types. Thus, this study aims to understand how to improve trust and reduce privacy concerns with 'mistrusted digital environments,' which we define as any technology that, due to privacy concerns, evokes apprehension, hesitation, or refusal to use among users.

One important reason for reducing privacy concerns with mistrusted digital environments is because of the crucial role that digital environments play in modern life, whereby mistrust towards a certain digital environment may pose a barrier to effective daily life or lead to social exclusion. That is, while some digital environments may be mistrusted, avoiding them entirely is often impractical. For instance, an individual may feel wary of Facebook but it's the only method they can use to remain connected with distant family members, making avoidance unrealistic. Similarly, TikTok or Instagram might be essential for staying current with trends in a marketing or communications role, or a platform like ChatGPT may be invaluable for productivity, but many may still struggle due to strong concerns over data collection. Thus, mistrust does not mean a digital environment is inherently negative or should be abandoned completely. In fact, many mistrusted digital environments offer significant benefits, including social connection, collaboration, and rapid access to information. Importantly, these digital environments were initially created with specific functions—such as fostering social interaction or providing information—rather than focusing on privacy protection, which explains their limitations in safeguarding user privacy. Therefore, a key goal of this research is to find ways for individuals, to continue using beneficial digital environments with added privacy protections.

To achieve this goal, users will need to adopt additional measures to secure their private information, establishing a strategy specifically aimed at privacy protection. Because these digital environments like Facebook or Zoom were not necessarily created with privacy in mind, one strategy to build privacy protections is to use an external tool and we propose that leveraging NeuroTech, a novel physiological biometric authentication method, may be a successful strategy to enhance privacy, trust, and digital technology usability.

1.3. Introducing NeuroTech: A biometric access control system

Biometric access control systems, which use biometric data such as fingerprints, facial scans, or iris recognition, to provide both biometric authentication and point-of-access control have gained popularity, with Facial Recognition being especially widespread (Melzi et al., 2024). Although Facial Recognition as a biometric authentication method has been used by many digital technologies and environments, one important drawback is that they exacerbate discrimination against marginalized populations, widening the discrimination gap (Bacchini & Lorusso, 2019). For example, the Detroit Police Department has faced criticism for wrongful arrests of African American individuals based on Facial Recognition, underscoring the risks of using this technology in real-world settings (R. Williams, 2024). Furthermore, research has demonstrated that Facial Recognition security could be bypassed using less than $500 by spoofing users' faces (Yan & Yang, 2023). Although recent policies aim to prevent profiling based on Facial Recognition alone (Ha, 2024), additional protective measures are essential to approach privacy and security tools thoughtfully to address these groups' unique challenges (McDonald, 2022).

To address the discriminatory challenges seen with Facial Recognition and tackle a solution to the seemingly never ending cycle of hacking into "secure" systems, this study investigates the potential of a brand new biometric access control system called NeuroTech, which employs unique physiological authentication to enhance security (Alsaadi, 2015; Lucier et al., 2023). Unlike other biometric authentication methods used today, NeuroTech use neural tapping to translate brain-linked signals from the micro-vibrations in the hands while holding a device, like a smartphone, to authenticate an individual (Lucier et al., 2023; Sodhro et al., 2022). NeuroTech is also functionally very easy to integrate with a digital technology, as the micro-vibrations are assessed using the technology already available within one's smartphone, serving as a biometric access point, ensuring that only the authorized user, via their neuro-vibrations, can log in or initiate a transaction, for example. Importantly, because every individual has their own unique neuro-vibration, agnostic of race, ethnicity, or gender, there is no concern for discrimination like Facial Recognition is subject to.

Additionally, to ensure that data is not stored on the cloud, where nefarious individuals can hack and gain access to massive amounts of user data, NeuroTech ensures that users' personal information is stored locally on the users' phone. Because NeuroTech operates via device-side verification and local storage, no biometric data is ever shared with the digital platform provider, thus eliminating cloud exposure risks, and allowing users to keep their own data safely in the palm of their hand. For example, an individual engaging in online banking could access their account without the risk of their private information being obtrusively harvested. In essence, NeuroTech wraps around the platform's existing process and secures it without altering any internal structure. This also provides formerly incarcerated individuals with more control over their data, which may make interacting with mistrusted digital environments less negative.

NeuroTech is an alternative biometric approach specifically designed to mitigate the privacy vulnerabilities common in biometric systems. Our research highlights two key advantages of NeuroTech.

1. Enhanced Biometric Authentication: NeuroTech rely on micro-vibrations unique to each individual, making them impervious to spoofing. As such, NeuroTech eliminates the discriminatory biases often observed in Facial Recognition systems, providing a more equitable solution for marginalized populations.
2. Data Remains Local: Unlike Facial Recognition, this approach does not store personal data in cloud systems, significantly reducing vulnerability to cyberattacks. Instead, data is securely stored on users' devices, ensuring privacy remains literally in their hands.

1.4. Mistrusted digital environments among formerly-incarcerated individuals

This research will compare the impact of the most common biometric authentication method, Facial Recognition, with NeuroTech to identify whether NeuroTech is a viable soluation to improve trust in mistrusted

digital environments among formerly incarcerated individuals. Although privacy concerns are universal, their implications are particularly pronounced for marginalized groups, such as formerly incarcerated individuals (Anderson et al., 2020; DeVeaux, 2013; Wolff et al., 2014), whose past experiences and societal vulnerabilities amplify the stakes of feeling a lack of trust and security (Eubanks, 2018; Lynskey, 2019; Molitorisz, 2020; Seo et al., 2022).

An incredibly relevant traumatic privacy-related experience that all formerly incarcerated individuals endured is the lack of autonomy and control over their lives while incarcerated (Driessen et al., 2023). Inmates are required to undergo cavity searches to prevent contraband, are constantly monitored via video surveillance in restrooms and sleeping quarters, have restricted movement requiring written permission, and may only receive visits under staff supervision with no physical contact allowed. Although the average individual may sacrifice privacy to engage with digital environments, formerly incarcerated individuals may feel these privacy intrusions more intensely due their past trauma, which would disproportionally impact the way they interact with mistrusted digital environments by being more hypervigilant, distrustful, and suspicious of any potential privacy threat (Chen et al., 2022; Haney, 2002; Rennie & Crewe, 2023a; Sannon & Forte, 2022; Turnbull & Hannah-Moffat, 2009; Werth, 2012), potentially leading to disengagement, emotional distress, or risky privacy-related behaviors.

This lack of control extends to interactions with digital environments, where individuals may be forced to sacrifice privacy to meet social or work needs may bring up traumatic memories. For example, individuals may need to allow location-based monitoring for social media interactions with family or comply with mandatory video conferencing during work (Lucier et al., 2023; Okabe-Miyamoto et al., 2021). Research has shown that when some formerly incarcerated individuals (and individuals of the general public) feel that surveillance is inescapable, they choose not using digital technology (Guberek et al., 2018), while others engage in risky behavior due to feeling like they have "nothing to lose" (Driessen et al., 2023; Seo et al., 2022). Therefore, depending on an individual's response to the lack of control, they may either disengage with the digital environment completely (to the detriment of the individual's social connection and work productivity, depending on the digital environment being avoided or to the detriment of the digital environment due to the lack of engagement) or they might make risky decisions with their private information in order to comply (to the detriment of the individual's right to privacy and autonomy).

As such, we believe that individuals with previous incarceration histories would be more susceptible to traumatic emotional and behavioral responses to mistrusted digital environments and thus, be more interested in a solution to protect their privacy.

2. Current study

Given the challenges that mistrusted digital environments face, innovative solutions like NeuroTech offer a promising path forward as it (1) provides enhanced security through unique neuro-vibrational methods that cannot be spoofed, (2) an on-device storage of personal information that is mass hackable like cloud-based solutions and (3) eliminates the discriminatory biases that are inherent in Facial Recognition (Bacchini & Lorusso, 2019) to provide an equitable and inclusive solution to privacy. As such, this study explores a novel using NeuroTech with mistrusted digital environments to potentially reduce privacy concerns and improve use of mistrusted digital environments among the general population as well as formerly incarcerated individuals. Unlike Facial Recognition, which often exacerbates discrimination (Bacchini & Lorusso, 2019), NeuroTech offer a groundbreaking non-discriminatory approach for safeguarding the right to privacy, marking a unique instance of First Amendment protections being upheld through technological coding. Given that formerly incarcerated individuals face an elevated risk of discrimination (Ha, 2024; D. P. Williams, 2020; R. Williams, 2024), we are also interested in identifying whether NeuroTech may be a Biometric Access Control System that might be especially useful among a formerly incarcerated population.

1. What digital environments do people have privacy concerns with?
2. Will using NeuroTech with a mistrusted digital environment improve engagement with the mistrusted digital environment?
3. Will using NeuroTech with a mistrusted digital environment reduce privacy concerns about the mistrusted digital environment?
4. Will using NeuroTech with a mistrusted digital environment improve engagement with the mistrusted Digital environment more effectively than Facial Recognition f?
5. Will using NeuroTech with a mistrusted Digital environment alleviate privacy concerns more effectively than Facial Recognition for formerly incarcerated individuals?
6. After reading about the benefits of NeuroTech, will individuals be willing to adopt NeuroTech?

3. Study 1

3.1. Participants

The primary aim of Study 1 was to identify the types of digital environments that individuals are hesitant to engage with or actively avoid due to privacy concerns (i.e., to answer research question #1). To address this research question, we sought a reasonable sample of both formerly incarcerated individuals and individuals who had never been incarcerated, allowing us to compare their privacy concerns and engagement behaviors with digital environments.

Participants were recruited from two sources: Prolific, an online platform providing access to diverse populations, and San Francisco State University's Project Rebound program, which specifically supports formerly incarcerated individuals in their reintegration through higher education. This dual-sampling approach ensured representation from both populations, aligning with the study's goal of capturing insights into privacy concerns across these two groups.

Importantly, while we did not expect Prolific to yield a large sample of formerly incarcerated individuals, the platform did include participants with self-reported incarceration histories. This allowed us to classify participants into groups regardless of recruitment source. At the end of the survey, all participants were asked: "Have you ever spent time in a jail, prison, or juvenile detention center?" Participants who responded "yes" were categorized as formerly incarcerated, while those who responded "no" were categorized as never incarcerated. This classification enabled a combined analysis of participants from both recruitment sources to address our research question effectively.

A total of 101 participants were recruited for this study and provided informed consent. From the Prolific sample, 76 participants (75 %) reported no history of incarceration, and 6 participants (6 %) reported a history of incarceration. From the Project Rebound sample, 19 participants initially identified as formerly incarcerated, with 17 (89 %) retained after attention check analysis. Combining these two sources resulted in a final sample of 76 (75 %) participants without an incarceration history, 23 (23 %) participants with an incarceration history, and 2 (2 %) participants who did not respond to the incarceration question. This dual-sampling strategy combined the breadth of Prolific with the targeted population of Project Rebound, ensuring alignment with the study's goals and providing insights into privacy concerns and digital environment engagement across both groups.

Participants in Study 1 ($N = 101$) had a mean age of 39.54 years ($SD = 13.18$), with ages ranging from 20 to 72. Gender identification included 51 (50 %) male, 47 (47 %) female, and 3 (3 %) transgender participants. In terms of ethnicity, the sample was predominantly Caucasian/White, with 63 (62 %) participants, followed by 15 (15 %) African American/Black, 10 (10 %) Hispanic/Latinx, 8 (8 %) Asian, and 5 (5 %) Multi-Ethnic participants. Marital status varied, with 52 (51 %) single and never married, 30 (30 %) married or in a domestic

partnership, and smaller proportions widowed 3 (3 %), divorced 14 (14 %), or separated 2 (2 %). Most participants, 70 (69 %), had no children in their household, while 15 (15 %) had one child, and 15 (15 %) had two or more children. Educational attainment was diverse, with 66 (65 %) holding a college degree or higher. Income distribution indicated that 52 (51 %) earned above $60,000 annually. Notably, 23 (23 %) of participants had been incarcerated, and 71 (70 %) expressed privacy concerns related to online activities, which led to hesitancy in engaging online.

3.2. Procedures

Participants first consented to the study then were asked whether they (1) reported having privacy concerns with a digital technology and refused to engage with it, (2) reported having privacy concerns with a digital technology and hesitated to engage with it, and/or (3) reported not having privacy concerns with a digital technology.

For participants reporting privacy concerns with something online and refusing to engage, we asked them to list three digital technologies they avoided, select the one of greatest concern, and explain why. We also inquired whether avoiding the technology led to any negative outcomes and if improved privacy protections would increase their likelihood of interaction or improve their attitudes toward the technology. Participants were also asked if there were other reasons, beyond privacy, for avoiding the digital technology. For participants reporting privacy concerns but hesitating to engage, we asked them to list three digital technologies they hesitated to use, select the one of greatest concern, and explain why. They were asked how this hesitation impacted their technology use, their attitudes toward the technology, and why they continued to use it despite privacy concerns. Finally, we asked if better privacy protections would increase their likelihood of use, improve their attitudes, and if non-privacy factors influenced their hesitation.

After these specific questions, participants responded to items about general privacy concerns, digital divide status, and algorithmic awareness. Demographics such as age, gender, ethnicity, marital status, number of children, education, income, and incarceration history were also collected.

3.3. Measures

Hesitation to Use Mistrusted Digital Environment. We asked, "Are there any digital technologies that you are hesitant to engage with (but still do) and/or refuse to engage with because of privacy concerns?" and were told to select all that apply: "Yes, I have privacy concerns with something online, but I still engage with it," "Yes, I have privacy concerns with something online, and I do not engage with it," and "No, I do not have privacy concerns with anything online." In all analyses, we report the percentage of participants who selected each option Note: Participants could endorse more than one "yes" response option (e.g., they may both engage with an refuse digital technologies due to privacy concerns), so these percentages may sum to more than 100 %. The "no privacy concerns" option was mututally exclusive and could not be selected alongside either "yes" response.

Refusal to Use Mistrusted Digital Environment. We asked, "What digital technology do you have privacy concerns with but refuse to engage with?" and had respondents list up to 3 digital technologies. We followed up by asking, "Which of the above do you refuse the MOST to interact with? Please only choose one" allowing participants to report which of the three digital technologies they refused the most to engage with. We ask participants why the refuse to interact with the digital technology using an open-ended text box. We also ask if not engaging with the digital technology ever "lead to negative outcomes?" On a "yes" or "no" scale, we asked participants "other than privacy, are there any other reasons you refuse to interact with digital technology?" If participants answer yes, they explained why in an open-ended text box and explained their feelings when using the mistrusted digital technology. Table 1 reports the percentages of responses to the question regarding privacy concerns with digital technologies across various demographic variables.

Specific Mistrusted Digital Environments. We asked, "What digital technology do you have privacy concerns with but still engage with?" and had respondents list up to 3 digital technologies. We followed up by asking, "Which of the above do you hesitate the MOST to interact with? Please only choose one" allowing participants to report which of the three digital technologies they hesitated the most to interact with. We ask participants to tell us why they hesitate to interact with the digital technology using an open-ended text box. We also ask if their hesitation to use the digital technology ever leads to "not use the digital technology," "use the digital technology less frequently," "doesn't change your habits with the digital technology," or "other". Next, we asked, "how do you feel when you're engaging with the digital technology?" and "why do you still engage with the digital technology when you have privacy concerns?" using open-ended text boxes. On a "yes" or "no" scale, we asked participants "other than privacy, are there any other reasons you hesitate to interact with digital technology?" If

Table 1
Engagement with digital technologies despite privacy concerns by demographic group (N = 101).

Category	N	Engage Despite Concerns (%)	Refuse Due to Privacy Concerns (%)	No Concerns (%)
Total Sample	101	79	33	7
Incarceration History				
Yes	23	74	21	8
No	76	80	36	7
Gender				
Male	51	75	33	8
Female	47	83	32	6
Age				
≤29 years	29	79	35	3
30–39 years	30	80	27	13
≥40 years	42	79	36	5
Ethnicity				
African American/ Black	15	80	20	13
Asian	8	75	38	0
Caucasian/White	63	79	35	8
Hispanic/Latinx	10	70	30	0
Education				
High School or less	12	67	25	17
Some College	39	77	39	8
College Degree	25	84	20	4
Graduate Degree	25	84	40	4
Income				
Less than 29K	24	67	33	17
30K–59K	25	84	28	8
60K–99K	27	70	44	3
100K or more	24	96	21	0
Marital Status				
Single, never married	52	81	37	10
Married or domestic partnership	30	80	30	4
Divorced	14	71	36	0
Children in Household				
0	70	81	33	7
1	15	67	40	7
2+	16	81	25	6

Note: Participants were asked if they engage with or avoid digital technologies due to privacy concerns and could select multiple responses. "Engage Despite Concerns" and "Refuse Due to Concerns" are not mutually exclusive and may sum to more than 100 %. However, the "No Concerns" response was mutually exclusive. All percentages are rounded to whole numbers and calculated within each subgroup (row).

participants answer yes, they explained why in an open-ended text box. We analyzed these responses separately for our two primary groups of interest: those with an incarceration history and those without.

The listed technologies were categorized into key groups: AI (artificial intelligence technologies), SA (shopping and retail-related apps and sites), FB (banking and financial services), CT (communication and social interaction tools), SE (search engines and browsing tools), EM (email-related technologies), SM (social media platforms), and MI (miscellaneous or other technologies). This categorization allowed for a systematic analysis and comparison of the frequency and types of digital technologies that participants from both groups hesitated to use due to privacy concerns.

Privacy Protection and Engagement, Attitudes, and Emotions with Mistrusted Digital Environments. For both those that refuse and hesitate to use digital technology, we ask whether "having privacy protection (would) increase your likelihood to interaction with the digital technology," if "having privacy protection (would) improve your attitude toward the digital technology," and if "having privacy protection (would) lead to more positive feelings while using the digital technology" all on a "yes" or "no" scaling.

3.4. Results

Refusal and Hesitation to Use Mistrusted Digital Environments. We examined how privacy concerns impacted engagement with digital technologies, referred to as "mistrusted digital environments." Participants with an incarceration history were slightly less likely to engage with technologies despite privacy concerns, with 17 of 23 (74 %) doing so, compared to 61 of 76 (80 %) of those without such a history. They were also less likely to refuse engagement due to privacy concerns, with 5 of 23 (21 %) declining to engage compared to 27 of 76 (36 %). Demographic differences were also explored. Gender comparisons indicated that 39 of 47 (83 %) female participants engaged with technologies despite privacy concerns, compared to 38 of 51 (75 %) male participants. Engagement increased with educational attainment: 42 of 50 (84 %) participants with a graduate or college degree engaged despite privacy concerns, while only 8 of 12 (67 %) of those with a high school education did so. Income followed a similar trend, with 23 of 24 (96 %) participants earning $100,000 or more continuing to engage with digital technologies despite privacy concerns. Detailed engagement across demographics is presented in Table 1.

Mistrusted Digital Environments. Next, we explored which mistrusted digital environments were most prevalent among individuals. The categorization of these technologies was informed by participants' responses to the two prompts (refuse, hesitate) asking respondents to report on the digital technologies that they had privacy concerns with. We developed a coding scheme to categorize these digital technologies into eight categories: AI (artificial intelligence technologies), SA (shopping and retail-related apps and sites), FB (banking and financial services), CT (communication and social interaction tools), SE (search engines and browsing tools), EM (email-related technologies), SM (social media platforms), and MI (miscellaneous or other technologies).

The coding process involved reviewing participants' open-ended responses to identify and categorize the digital technologies they mentioned. Frequency counts for each category allowed us to analyze how privacy concerns manifested differently between participants with and without an incarceration history. Among formerly incarcerated participants, social media platforms accounted for 38 % of responses, with TikTok and Meta platforms mentioned most frequently. In contrast, social media accounted for 29 % of responses among non-incarcerated participants, who also primarily cited TikTok. Communication and social interaction tools (e.g., Zoom) were the second most common concern among formerly incarcerated individuals, representing 14 % of responses. Concerns about email technologies and banking or financial services each accounted for 6 %, while shopping and retail-related apps made up 4 %. In the non-incarcerated group, communication and social interaction tools were cited in 24 % of responses, followed by search engines and browsing tools at 14 %, shopping and retail-related apps at 7 %, banking and financial services at 7 %, and AI technologies at 6 %. Table 2 provides a systematic overview of the digital technologies that participants hesitated to engage with due to privacy concerns.

These findings address our first research question, revealing that formerly incarcerated individuals commonly mistrust TikTok, Meta platforms (e.g., Instagram, Facebook), and video conferencing software; similarly, non-incarcerated participants reported social media as their primary concern. In Study 2, we will focus on these three digital technologies to assess whether a Biometric Access Control System may mitigate privacy concerns.

These differences address Q1, revealing that formerly incarcerated individuals commonly mistrust TikTok, Meta platforms (e.g., Instagram, Facebook), and video conferencing software; similarly, those without a history of incarceration also reported social media as commonly mistrusted digital environments. As such, in Study 2, we will focus on these three digital technologies to assess whether a Biometric Access Control System may mitigate privacy concerns.

Thematic Analysis of Reasons for Refusal and Hesitation to Use Mistrusted Digital Environments. We also conducted a qualitative analysis of participants' open-ended responses regarding their hesitations, feelings, and motivations for engaging with mistrusted digital environments to understand respondents' experiences and thoughts. The analysis involved thematic coding of respondents' experiences and thoughts, leading to three primary themes: Privacy Concerns, Emotional Responses, and Reasons for Engagement. Subcategories within each theme captured nuanced insights, including data harvesting, trust issues, and the necessity of technology for social connections. Table 3 summarizes the frequency of responses for each theme and subtheme, with illustrative quotes from participants. This overview highlights the

Table 2
Frequency and distribution of privacy concerns by digital technology type.

Sample	Incarcerated (n = 50)		Non-Incarcerated (n = 180)	
Category	Frequency	% of Responses	Frequency	% of Responses
AI-powered services and tools	0	0	11	6 %
Communication platforms (e.g., Zoom)	7	14 %	43	24 %
Email services	3	6 %	13	7 %
Online banking and financial services	3	6 %	12	7 %
Other digital technologies	8	16 %	9	5 %
E-commerce platforms and apps	4	8 %	13	7 %
Web search and browsing tools	6	12 %	26	14 %
Social media platforms	19	38 %	53	29 %
Total	50	100 %	180	100 %

Note. Participants were asked to identify digital technologies they hesitate to engage with or refuse to use due to privacy concerns. Responses were open-ended and coded into eight categories based on function and user-facing service. Frequencies reflect the number of individual concerns coded from each group. Percentages are based on the total number of coded responses per group (non-incarcerated = 50; incarcerated = 180). Participants were asked to identify digital technologies they were hesitant to engage with or refused to use due to privacy concerns. Percentages are calculated out of the total number of coded responses within each group. The coding scheme categorizes the reported technologies into seven groups: AI-powered services and tools (AI), e-commerce platforms and apps (E-COM), online banking and financial services (BF), communication platforms (CT), web search and browsing tools (SE), email services (EM), social media platforms (SM), and miscellaneous or other technologies (MI). Frequencies for each category reflect the number of responses indicating concerns. All percentages are rounded to whole numbers.

Table 3
Themes and Frequencies of participant responses regarding mistrusted digital environments.

Theme	Subtheme	Example Quote	Frequency
Privacy Concerns	Data Harvesting	"I don't want my data harvested, and I am concerned with all the leaks."	8
	Trust Issues	"I do not trust Elon Musk."	5
Emotional Responses	Feeling Uncertain	"I feel drained of energy."	6
	Feeling Intrusive	"It feels intrusive."	7
Reasons for Engagement	Necessity	"I need to use it to reach out to certain colleagues."	9
	Keeping Connections	"I use it for keeping up with family and friends."	10

Note. The table presents the frequency and percentage of privacy concerns reported by participants in two groups: those with an incarceration history (marginalized sample) and those without (non-marginalized sample). Participants were asked to identify digital technologies they were hesitant to engage with or refused to use due to privacy concerns. The coding scheme categorizes the reported technologies into seven groups: AI-powered services and tools (AI), e-commerce platforms and apps (E-COM), online banking and financial services (BF), communication platforms (CT), web search and browsing tools (SE), email services (EM), social media platforms (SM), and miscellaneous or other technologies (MI). Frequencies for each category reflect the number of responses indicating concerns.

nuanced privacy concerns respondents have regarding mistrusted digital environments and underscores the potential need for a Biometric Access Control System to protect privacy, suggesting further research is necessary to identify strategies for alleviating privacy concerns.

There were notable visceral experiences that the formerly incarcerated participants mentioned about the mistrusted digital technology they mentioned. For example, one formerly incarcerated individual noted that their most mistrusted technology was Google because "they track literally everything" but continue to use it because it's "practically needed," but it feels like they are "selling their soul" while using it. Another formerly incarcerated individual said that they most mistrust Facebook "because of the amount of information that is taken and stored without (their) expressed permission. They force an interaction out of necessity or requirement, then harvest the information to use as a resource to garnish capital in the form of finance." Despite this, the individual continues to use Facebook "because it is the platform where my friends and family are all located. A … location that allows me to see the people I trust (and) love. I just hate that I have to give up a large part of my privacy in order to feel connected with the people I love." As mentioned, the theme of surveillance is pervasive among formerly incarcerated individuals (Haney, 2002; Molitorisz, 2020; D. P. Williams, 2020), which is likely why this feeling is particularly salient to this respondent as they mentioned that they feel "like all communication and even my location is being tracked. They mention it as convenience, but it feels a lot like surveillance." As such, formerly incarcerated participants' narratives revealed that privacy concerns with digital platforms like Facebook and Google stemmed from perceived surveillance, tracking, and a complete loss of control, echoing their traumatic experiences of being constantly monitored and deprived of autonomy.

Engagement Behaviors with Mistrusted Digital Environments. Given the prevalence of mistrusted digital environments, we further explored how privacy concerns affect engagement behaviors. Participants who reported hesitations with mistrusted digital environments were asked, "Does your hesitation with your 'mistrusted digital environment' ever lead you to … (Please select all that apply): (1) Not use this digital technology, (2) Use this digital technology less frequently, (3) Continue to use this digital technology without changing your habits, or (4) Other (please explain)." Due to small sample sizes, responses from the 80 participants reporting hesitation were summarized in Table 1. Among these 80 participants, 12 (15 %) indicated that their hesitation led them to avoid using their mistrusted digital environment altogether, while 52 (65 %) used it less frequently, and 19 (24 %) reported no change in habits. An additional 8 (10 %) selected "other," with several explaining that they limited usage to secure devices (e.g., home computers) or avoided sharing personal information online. Some also noted a general decline in their usage of such technologies over time due to rising privacy concerns.

When comparing responses by incarceration status, the following trends emerged: (1) Among formerly incarcerated individuals, 18 % reported avoiding the mistrusted digital environment, 59 % used it less frequently, and 18 % reported no change in habits. (2) In contrast, non-incarcerated participants reported slightly avoidance (13 %), higher rates of usage (69 %), and 25 % reported no change in habits. These findings suggest that privacy concerns meaningfully shape technology engagement behaviors, with variations between formerly incarcerated and non-incarcerated populations.

Engagement Behaviors with Mistrusted Digital Environments with Added Privacy Protection. One of the main goals of this manuscript is to explore solutions to help individuals feel that their privacy is protected when using mistrusted digital environments, which could promote engagement and improve attitudes towards mistrusted digital environments. To that end, we investigated whether improved privacy protection would influence participants' likelihood to engage with mistrusted digital environments. A substantial majority (86 %) indicated that better privacy protection would increase their likelihood of interacting with mistrusted digital environments, while 87 % believed it would improve their attitudes toward them. Furthermore, 90 % of participants reported that enhanced privacy protection would lead to more positive feelings while using their mistrusted digital environments.

These findings highlight the critical role of privacy protection in fostering favorable attitudes and encouraging interaction with mistrusted digital environments. Notably, only minor differences emerged between formerly incarcerated individuals and non-formerly incarcerated participants. Among the formerly incarcerated group, 82 % indicated that better privacy protection would increase their likelihood of interacting with their mistrusted digital environment, and 82 % believed it would improve their attitudes. In contrast, 90 % of the non-formerly incarcerated population indicated that improved privacy protection would lead to greater interaction with mistrusted digital environments, and 92 % believed it would improve their attitudes. These findings address Q2 and Q3 by suggesting that stronger privacy protections could foster increased engagement, more positive attitudes, and improved emotional experiences with mistrusted digital environments, even within incarcerated populations. Accordingly, Study 2 will examine whether using a Biometric Access Control System with a mistrusted digital environment may help increase engagement and reduce privacy concerns with mistrusted digital environments.

3.5. *Brief discussion*

Results from Study 1 indicate that there are specific mistrusted digital environments that many formerly incarcerated individuals have privacy concerns with, namely TikTok, Meta platforms, and video conferencing software, while non-formerly incarcerated individuals also reported concerns with social media, addressing Q1. These privacy concerns lead to formerly incarcerated individuals using mistrusted digital environments less or fully refusing to use them, enforcing the need for solutions that enhance privacy protection among this specific population. Addressing Q2 and Q3, we found that stronger privacy protections could foster increased engagement, positive attitudes, and emotions towards mistrusted digital environments, providing evidence that NeuroTech may be a strong tool to protect privacy and improve usage of mistrusted digital environments. Therefore, in Study 2, we plan to introduce NeuroTech as a solution to reduce privacy concerns with mistrusted digital environments, which may in turn improve engagement.

4. Study 2

Having established that privacy concerns exist for specific types of mistrusted digital environments, which in turn impact engagement, we next explored potential strategies to reduce these concerns, with the goal of enhancing engagement, attitudes, and emotional responses toward these useful, yet mistrusted, digital environments.

4.1. Participants

A total of 2947 participants were recruited through a data vendor and provided informed consent. Due to the complexity of the study, we implemented strict inclusionary criteria. To be included in Study 2, participants had to express privacy concerns with our key mistrusted digital environments (Meta platforms, TikTok, and video conferencing software). As a result, 37 % of participants who did not express concerns with these mistrusted digital environments were excluded. In addition, if participants had privacy concerns with our key mistrusted digital environments but this concern did not impact their engagement, they were also excluded, leading to an additional 17 % being removed. As a result, 1149 were qualified for our study.

Next, we implemented a series of attention check questions to ensure data quality. First, we had participants read about one of two Biometric Access Control Systems: The novel NeuroTech and the traditional Facial Recognition. As an attention check, we asked participants to accurately identify the they had just read about NeuroTech and facial reecognition, leading to an additional 44 % of the sample being removed. Finally, we had a final attention check that asked respondents to select "Never" in a 5-point "Never" to "Often" scale, leading to an additional 23 % being removed. After removing those that did not complete the survey, our final sample consisted of 589 participants who were included in all Study 2 analyses.

Among our sample of 589 participants, most were female (53 %), Caucasian (76 %), and ranged in age: 18–24 (6 %), 25–34 (15 %), 35–44 (19 %), 45–54 (20 %), 55-55 (18 %), 65 or older (23 %). All 589 participants responded to the income item. The most common income brackets were 46K–55K (16 %), 13K–25K (12 %), and 26K–35K (11 %). A small number of participants (2 %) preferred not to answer. Most participants also earned a household income that exceeds $35,000 (79 %) and a majority have completed some college or trade school (49 %). Most participants reported having no children in the household (64 %), married (47 %), and single and never married (30 %). Participants were scattered across the United States: Southeast (35 %), Midwest (29 %), northeast (21 %), and west (14 %). A majority of participants lived in suburban areas (48 %) compared to urban (27 %) and rural areas (25 %).

To better understand socioeconomic status and personal experiences, we asked a battery of questions. Unless otherwise noted, all percentages reflect valid responses. Due to occasional non-response or skip patterns, some item-level Ns differ slightly from the total sample (N = 589), as indicated in the text or tables. Of the full sample (N = 589), 44 % reported growing up in a low-income or poverty-stricken household, 11 % reported currently living in one, and 45 % reported never having experienced poverty. Conversely, 45 % of our sample stated that they had never experienced low-income or poverty-stricken situations. We also asked about health conditions, of the 589 participants, 42 % reported chronic health conditions or disabilities, but 58 % reporting no such conditions. Participants also responded to questions about their employment stability, among 588 valid respondents, 39 % reported previous long-term unemployment or difficulty securing stable employment, 13 % reported currently experiencing it, and 47 % reported never having faced such challenges. Additionally, among all participants (N = 589), 39 % reported past housing instability or homelessness, 6 % reported current instability, and 55 % reported never experiencing such issues. Importantly, because the goal of our research is to explore the experiences of previously incarcerated individuals, 143 of 588 valid respondents (1 participant did not answer) 24 % reported experiencing incarceration in the past.

4.2. Procedures

We first asked participants a set of questions involving their socioeconomic status, including poverty status, disability status, unemployment status, and homelessness, to understand their vulnerabilities. Importantly, we asked about previous incarceration history as this population was our population of interest. We then defined the term "privacy concerns" as any concern towards the possible misuse of personal information. Next, because of our inclusionary criteria, we asked whether participants refused to or were hesitant to interact with any of the following three digital environments (TikTok, Meta products, and/or video conferencing software) due to privacy concerns. Based on which mistrusted digital environment they chose, we then asked our "pre-intervention questions" regarding their usage frequency and the level of privacy concern they had with the mistrusted digital environment.

Next, to identify whether using NeuroTech or Facial Recognition with a mistrusted digital environment improves engagement and reduces privacy concerns, we randomly assigned respondents to one of two different Biometric Access Control System conditions: NeuroTech (experimental condition) or Facial Recognition (control condition). In each condition, participants read a description of each Biometric Access Control System. The NeuroTech condition read the following: "You told us you had privacy concerns with [Meta/Video Conferencing Software/TikTok]. We would like to introduce you to a new physiological biometric technology, which can greatly improve your mobile device security. This new biometric technology uses the micro-vibrations in your hand while you are holding your smartphone to confirm that only you, the legitimate user, can unlock your smartphone. To create your unique biometric authentication profile, you simply hold your phone for 3–4 s and an algorithm, along with existing sensors in your smartphone, will capture the nearly invisible microscopic movements in your hand. This new physiological biometric technology, using the micro-vibrations in your hand, would pair with [Meta/Video Conferencing Software/TikTok] to protect your privacy. Whenever you are logging in, sending your private information, spending money, or creating a new profile, this new technology protects your privacy by improving authentication through physiology-based encryption. This means that hackers are unable to steal your password or pretend to be you because your body becomes your unique password–which is unhackable." The Facial Recognition condition (control) condition read the following: You told us you had privacy concerns with [Meta/Video Conferencing Software/TikTok]. A biometric technology that can improve your mobile device's security is Facial Recognition. This technology is present in many mobile devices, such as the iPhone and Samsung Galaxy. Facial Recognition maps users' facial features from multiple angles to capture a full-range image of the users' face. Each time you hold your mobile device up to your face, the facial data collected is used to unlock your device or grant access to an app. Although Facial Recognition protects privacy, hackers may still be able to create spoofs of users' faces, based on publicly available images and Facial Recognition may not always recognize user faces due to factors like lighting, glasses, or ethnicity. However, Facial Recognition is a simple and easy strategy to protect one's private information. Facial Recognition would pair with [Meta/Video Conferencing Software/TikTok] to protect your privacy. Whenever you are logging in, sending your private information, spending money, or creating a new profile, this new technology protects your privacy by ensuring that only you, verified by your face, can use the mobile device or app."

Then, they saw a question that read: "Remember, the content above described using (the mistrusted digital environment) with a …" and for those in the NeuroTech condition had to select "physiological biometric technology using the micro-vibrations in my hand" and those in the Facial Recognition condition had to select "Facial Recognition". Then we had another attention check question that asked, "from the

description you just read, the (condition) would …" and participants had to accurately define their condition to continue on.

After reading about NeuroTech or Facial Recognition, we then asked our "post-intervention questions" such as how using the with their mistrusted digital environment impacted their privacy concerns with digital environments, their feelings of refusal or hesitancy to use the mistrusted digital environment, how much they thought that it would cost, whether they believe the using would better protect their privacy, how frequently they would use the mistrusted digital environment with this using, how confident they were that the using would protect their privacy and security, their trust that the using would protect their privacy, and whether they'd be willing to adopt NeuroTech or Facial Recognition to enhance their security.

4.3. Measures

Mistrusted Digital Environments. To be eligible for the study, participants must be hesitant or refuse to use one of our three mistrusted digital environments. To measure this, we asked the question "Are you ever hesitant or refuse to use any of the following digital technologies due to privacy concerns? If you hesitate or refuse to use multiple digital technologies, choose the one that you have the most privacy concerns with" and provided the answer choices of "Meta (e.g., Facebook, Instagram, WhatsApp)", "Video Conferencing Software (e.g., Zoom, Skype)", "TikTok", and "I do not hesitate or refuse to use any of these." If participants chose one of the three mistrusted digital environments, they were then asked if they "refused to use it", "hesitated to use it", or "use it without refusal or hesitation."

Engagement with Mistrusted Digital Environments. Before we show the using prompt, we asked "how often do you use [Meta/Video Conferencing Software/TikTok]" with answer choices "never", "once or twice a month", "once or twice a week", "every day", or "a few times a day". After reading the using prompt, we asked, "If [Meta/Video Conferencing Software/TikTok] was paired with [NeuroTech/Facial Recognition], how often would you use [Meta/Video Conferencing Software/TikTok]?" with answer choices "never", "once or twice a month", "once or twice a week", "every day", or "a few times a day".

Privacy Concerns with Mistrusted Digital Environments. Before reading the using prompt, we asked, "How would you rate your privacy concerns with [Meta/Video Conferencing Software/TikTok]?" on a scale of "not at all concerned", "somewhat concerned", "concerned", "very concerned", to "extremely concerned." After reading the using prompt, we then asked, "If [Meta/Video Conferencing Software/TikTok] was paired with [NeuroTech/Facial Recognition], how would you rate your privacy concerns with [Meta/Video Conferencing Software/TikTok]?" on a scale of "not at all concerned", "somewhat concerned", "concerned", "very concerned", to "extremely concerned."

Refuse/Hesitate to Use Digital environment. After reading the using prompt, we asked, "If [Meta/Video Conferencing Software/TikTok] was paired with [NeuroTech/Facial Recognition], which of the following would describe your use of [Meta/Video Conferencing Software/TikTok]?" with answer choices "I would refuse to use it", "I would hesitate to use it", or "I would use it without refusal or hesitation."

Cost of. After reading the using prompt, we asked, "How much do you think it will cost to pair [Meta/Video Conferencing Software/TikTok] with [NeuroTech/Facial Recognition]?" with an open-ended text box to indicate cost in dollars.

Privacy of NeuroTech. After reading the using prompt, we asked, "I believe that [NeuroTech/Facial Recognition] would pair with [Meta/Video Conferencing Software/TikTok] to protect my privacy better than [Meta/Video Conferencing Software/TikTok] alone can" on a "strongly agree", "somewhat agree", "neither agree nor disagree", "somewhat disagree", to "strongly disagree" scale. We also asked, "How confident are you that [NeuroTech/Facial Recognition] can enhance privacy and security when using [Meta/Video Conferencing Software/TikTok]?" on a "not at all confident", "slightly confident", "moderately confident", "very confident" to "extremely confident" scale.

Trusting NeuroTech. After reading the using prompt, we asked, "To what extent do you trust the effectiveness of the [NeuroTech/Facial Recognition] to protect your privacy?" on a "I do not trust it at all", "I slightly trust it", "I moderately trust it", "I trust it very much", to "I trust it completely" scale.

Adopting NeuroTech. After reading the using prompt, we asked, "Would you be willing to adopt [NeuroTech/Facial Recognition] to enhance the security of [Meta/Video Conferencing Software/TikTok]?" on a "definitely not", "probably not", "neutral", "probably yes", to "definitely yes" scale.

4.4. Results

Mistrusted Digital Environments. Among the three presented mistrusted digital environments (TikTok, Meta platforms, and video conferencing software), a majority of participants selected TikTok as their primary privacy concern (61 %), followed by Meta platforms (26 %) and video conferencing software (13 %). Among the formerly incarcerated group (n = 143 of 588 valid respondents), the majority reported TikTok as their primary privacy concern (58 %), followed by Meta platforms (28 %) and video conferencing software (14 %). A similar pattern was observed in the non-incarcerated group (n = 445), with 62 % selecting TikTok, 25 % Meta platforms, and 14 % video conferencing software.

A chi-square test of independence was conducted to examine whether formerly incarcerated individuals and those without incarceration experience differed in their primary privacy concerns related to Meta platforms (e.g., Facebook, Instagram, WhatsApp), TikTok, and video conferencing software (e.g., Zoom, Skype). The chi-square test was not statistically significant, $\chi^2(2, N = 588) = 0.629$, $p = .73$, indicating no significant association between incarceration history and the type of digital technology of most concern for privacy. These results provide insight into Q1, suggesting that privacy concerns across the three platforms are broadly shared, with no meaningful differences between formerly incarcerated and non-incarcerated individuals.

Engagement with Mistrusted Digital Environments. To assess engagement with mistrusted digital environments on devices before the introduction of using these devices with NeuroTech or Facial Recognition, a *t*-test was conducted. Participants were asked: (1) "How often do you use this (mistrusted) digital environment?" (response options ranged from Never = 1 to A few times a day = 5) prior to the introduction of the Biometric Access Control System conditions. Prior to reading about NeuroTech or Facial Recognition, there were no significant differences between those who were formerly incarcerated ($M = 1.93$, $SD = 0.10$) and their non-formerly incarcerated counterparts ($M = 1.82$, $SD = 0.06$).

After reading the vignette for their assigned, participants were asked to rate their engagement when their mistrusted digital environment was paired with their assigned. This assessment measured *changes* in engagement after learning about the potential security benefits of NeuroTech or Facial Recognition. A mixed factorial ANOVA was conducted to examine engagement with mistrusted digital environment devices before and after the introduction of NeuroTech or Facial Recognition, comparing formerly incarcerated individuals to non-incarcerated individuals. The mixed factorial ANOVA revealed a significant main effect of time, $F(1, 586) = 51.585$, $p < .001$, indicating that participants reported higher engagement with mistrusted digital environment devices after the introduction of NeuroTech or Facial Recognition ($M = 2.06$, $SE = 0.04$) compared to before the introduction ($M = 1.88$, $SE = 0.04$).

Additionally, a significant interaction was found between incarceration status and time, $F(1, 586) = 3.73$, $p = .05$. Estimated marginal means indicated that formerly incarcerated individuals reported significantly greater engagement post-vignette ($M = 2.33$, $SE = 0.11$) compared to pre-vignette ($M = 1.93$, $SE = 0.10$), while non-incarcerated

individuals also showed a smaller increase from pre-vignette ($M = 1.81$, $SE = 0.06$) to post-vignette ($M = 2.04$, $SE = 0.06$). Pairwise comparisons revealed that formerly incarcerated individuals exhibited a significant increase in engagement from pre-to post-vignette ($p = .02$), whereas non-incarcerated individuals did not show a significant difference ($p = .309$). These results provide insight into Q2, indicating that the introduction of NeuroTech or Facial Recognition leads to stronger engagement habits among formerly incarcerated individuals compared to their non-incarcerated counterparts.

However, the critical three-way interaction between engagement, experimental condition, and incarceration status was not significant, $F(1, 584) = 1.536$, $p = .216$. This suggests that while engagement was higher in the NeuroTech condition ($M = 0.445$) compared to Facial Recognition condition ($M = 0.187$), incarceration status did not significantly alter the engagement changes across conditions, see Fig. 1. Thus, while NeuroTech led to a larger increase in engagement, incarceration status did not have a moderating effect on this change, providing further support for Q2 and insight into Q4.

Privacy Concerns with Mistrusted Digital Environments. We also assessed privacy concerns with mistrusted digital environments before using NeuroTech or Facial Recognition among formerly incarcerated individuals ($M = 3.83$, $SE = 0.10$) and non-formerly incarcerated individuals ($M = 3.78$, $SE = 0.06$), however, these differences were not significant ($p = .67$). After reading about using NeuroTech or Facial Recognition with the mistrusted digital environment, participants were asked about their privacy concerns once more and individuals with a history of incarceration reported lower concern ($M = 3.074$, $SE = 0.11$) compared to those without such history ($M = 3.251$, $SE = 0.063$), however, again, this difference was not statistically significant, ($p = .17$).

Next, a mixed factorial ANOVA was conducted to assess the effect of concern on participants' responses from before using NeuroTech or Facial Recognition with their mistrusted digital environment to after. The analysis revealed a significant main effect of concern, $F(1,583) = 141.99$, $p < .001$, indicating that participants expressed significantly less concern regarding the mistrusted digital environment after their using NeuroTech or Facial Recognition. Specifically, the mean concern level prior to using NeuroTech or Facial Recognition with their mistrusted digital environment was higher ($M = 3.81$, $SE = 0.06$, 95 % CI [3.70, 3.92]) compared to the mean concern level after using NeuroTech or Facial Recognition with their mistrusted digital environment ($M = 3.16$, $SE = 0.06$, 95 % CI [3.04, 3.29]). Additionally, significant interaction

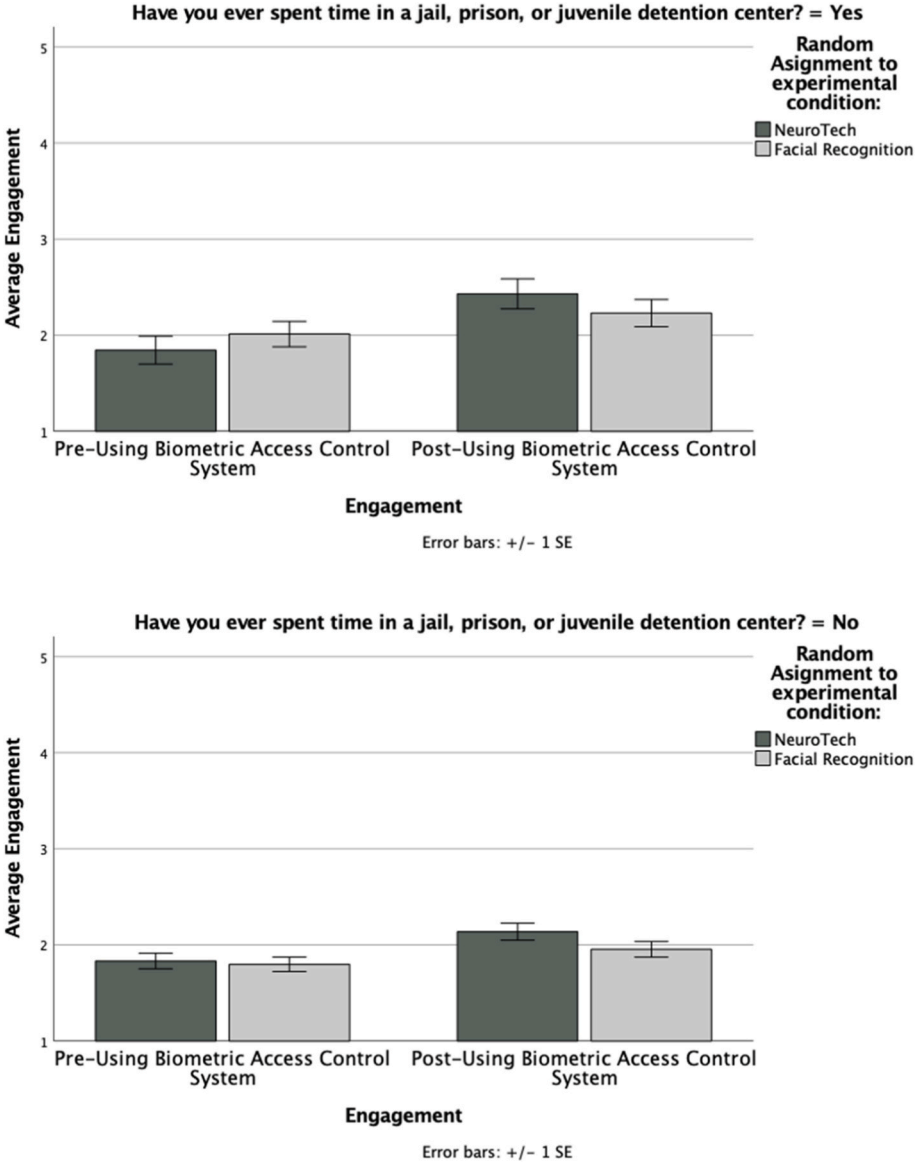

Fig. 1. Engagement pre- and post-using NeuroTech or Facial Recognition among formerly incarcerated (top) and not formerly incarcerated (bottom) individuals.

effects were observed between concern and incarceration status F (1,583) = 4.28, $p = .04$, as well as between concern and experimental condition F(1,583) = 14.58, $p < .001$. However, the three-way interaction involving concern, incarceration, and experimental condition was not significant, F(1,583) = 0.88, $p = .35$.

Importantly, we conducted a mixed factorial ANOVA with privacy concerns as the dependent variable and included both experimental condition (NeuroTech vs. Facial Recognition) and incarceration status (yes vs. no). The results revealed a significant change in privacy concerns from pre to post using NeuroTech or Facial Recognition with their mistrusted digital environment, F(1, 584) = 141.996, $p < .001$, indicating that privacy concerns decreased significantly once used with a Biometric Access Control System. A significant interaction between Facial Recognition and NeuroTech with incarceration status was seen, F (1, 584) = 4.275, $p = .039$, suggesting that formerly incarcerated individuals and those without incarceration histories responded differently to the two experimental conditions. Post hoc tests showed that privacy concerns did not significantly differ between the conditions for formerly incarcerated participants (Mean Difference = −0.106, $p = .566$), but for non-incarcerated participants, privacy concerns were marginally lower in the NeuroTech condition (Mean Difference = −0.197, $p = .061$). Despite this, the three-way interaction between experimental condition, incarceration status, and privacy concerns was not significant, F(1, 584) = 0.88, $p = .349$, see Fig. 2. These findings suggest that NeuroTech reduced privacy concerns more effectively than Facial Recognition, but the moderating role of incarceration status was not significant, providing insight for both Q3 and Q5.

Willingness to Adopt NeuroTech. Finally, participants were asked about their willingness to adopt NeuroTech or Facial Recognition to enhance the security of the mistrusted digital environment using a five-point scale ranging from 1 ("definitely not") to 5 ("definitely yes"), with higher scores indicating a greater willingness to adopt the. Participants in the NeuroTech condition ($M = 2.87$, $SE = 0.10$) were more willing to adopt NeuroTech while those in the Facial Recognition condition were less willing to adopt Facial Recognition ($M = 2.61$, $SE = 0.09$), F(1, 583) = 3.96, $p = .047$. Additionally, previously incarcerated individuals ($M = 2.97$, $SE = 0.11$) demonstrated a higher willingness to adopt a Biometric Access Control System compared to non-formerly incarcerated individuals ($M = 2.50$, $SE = 0.07$), F(1, 584) = 12.65, $p < .001$. However, there was no significant interaction effect between condition and

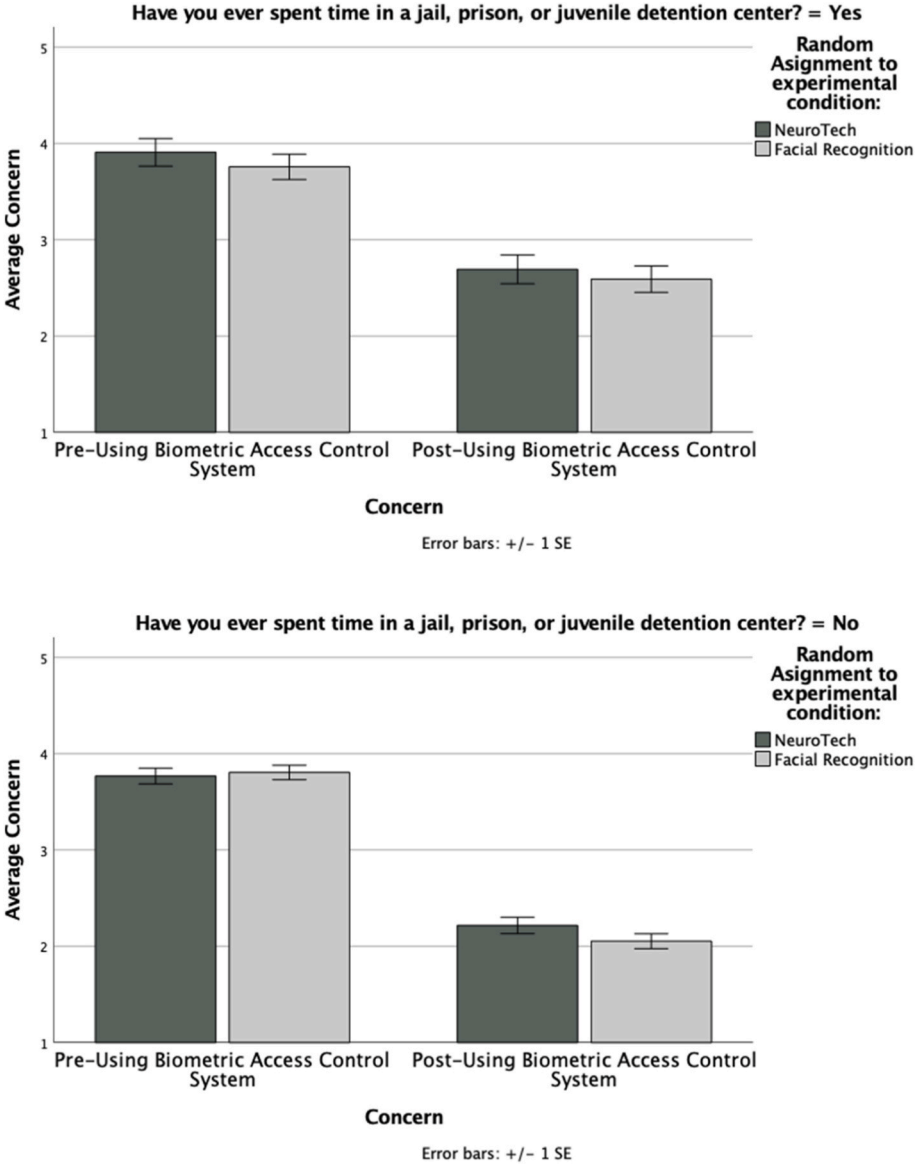

Fig. 2. Privacy concerns pre- and post-using NeuroTech or Facial Recognition with their mistrusted digital environment among formerly incarcerated (top) and not formerly incarcerated (bottom) individuals.

former incarceration status, F(1, 584) = 0.12, $p = .91$, see Fig. 3. This suggests that all individuals were more likely to adopt NeuroTech or Facial Recognition (whichever condition they were assigned to), regardless of the participants' incarceration status, providing insight into Q6.

5. Discussion

This study is one of the first to examine NeuroTech as a solution to reduce privacy concerns and improve use of mistrusted digital environments, as well as is uniquely tackling long-standing discriminatory practices seen with current practices like Facial Recognition. Furthermore, our findings provide important insights into the specific digital environments that formerly incarcerated individuals distrust, as well as the potential for NeuroTech being a non-discriminatory solution to mitigate these concerns and increase user engagement with mistrusted digital environments.

Using a qualitative approach in Study 1, we found that TikTok, Meta platforms, and video conferencing software were identified as the most mistrusted technologies among both formerly incarcerated and non-formerly incarcerated groups. While previous research has highlighted privacy concerns with digital environments, including among populations who have been historically discriminated against by digital environments and biometric authentication systems (Edelman et al., 2017; Edelman & Luca, 2014), this study is the first to specifically explore and identify the types of mistrusted digital environments that are popular among formerly incarcerated individuals. Past research has established that incarceration is highly traumatic, with constant surveillance and a complete lack of autonomy (Anderson et al., 2020; DeVeaux, 2013; Driessen et al., 2023; Wolff et al., 2014).

Based on qualitative narratives from formerly incarcerated individuals in Study 1, such as feeling a lack of control over what data is harvested with platforms like Google or feeling surveilled on Facebook just to be able to connect with distant loved ones, these experiences are contributing to the mistrust of technologies, as these technologies require individuals to give up something (whether it be one's name, browsing history, location, etc.) in order to have access to what are now "basic necessities" (Lucier et al., 2023; Okabe-Miyamoto et al., 2021, 2022). This is a critical step, as digital environments are increasingly integrated into daily life, and their impact on marginalized populations, such as those with an incarceration history, remains underexplored. Understanding which digital environments are particularly mistrusted by populations that are historically mistrusting and discriminated against is essential for ensuring that technological interventions are designed with their specific needs and concerns in mind.

In Study 1, we found that formerly incarcerated individuals were more likely to engage with mistrusted digital environments if they were provided with greater privacy protections. This finding underscores the importance of designing Biometric Access Control Systems that align with users' expectations for security and control over their personal data. Because Study 1 identified that greater privacy protections would lead to positive outcomes, in Study 2 we introduced NeuroTech and Facial Recognition. Respondents read about the functionality of NeuroTech or Facial Recognition (depending on random assignment), giving respondents an understanding of how NeuroTech works to protect one's privacy, specifically through the use of neuro-vibrational biometrics for authentication and localized data storage for reduced hacking opportunities. Explaining that NeuroTech provides a privacy mechanism that restores as sense of agency was of particular interest to formerly incarcerated populations, aligning with the control-related concerns that were expressed in the qualitative narratives in Study 1 and mirroring previous research on feelings of the lack of control among formerly incarcerated individuals (Haney, 2002; Molitorisz, 2020; Seo et al., 2022; D. P. Williams, 2020; Wolff et al., 2014).

After learning about the functionality of NeuroTech versus Facial Recognition, Study 2 tested the effectiveness of using NeuroTech with mistrusted digital environments, revealing that NeuroTech significantly improved engagement and reduced privacy concerns. These results suggest that NeuroTech, with its neuro-biometric authentication, localized data storage, and First Amendment rights integrated into the code, offers a promising solution to mitigate privacy concerns and increase comfort with digital environments, regardless of previous incarceration status. The favorability of NeuroTech versus Facial Recognition are likely due to two reasons: First, facial recognition is easy to spoof and is not as well trained with non-Caucasian faces (Anderson et al., 2020; DeVeaux, 2013; Driessen et al., 2023; Wolff et al., 2014), but using the neuro-biometric authentication from NeuroTech provides a biometric solution that does not have the same spoofing concerns. Furthermore, NeuroTech's neuro-vibration authentication, minimizes surveillance by avoiding facial recognition and the storage of one's facial features. Second, Facial Recognition often stores images of one's face within the cloud, leading to hacking concerns during major data breaches. NeuroTech does not have this flaw, as all data is stored locally on device and is not subject to mass data breaches.

Importantly, our research demonstrated that NeuroTech outperformed Facial Recognition in improving privacy concerns and

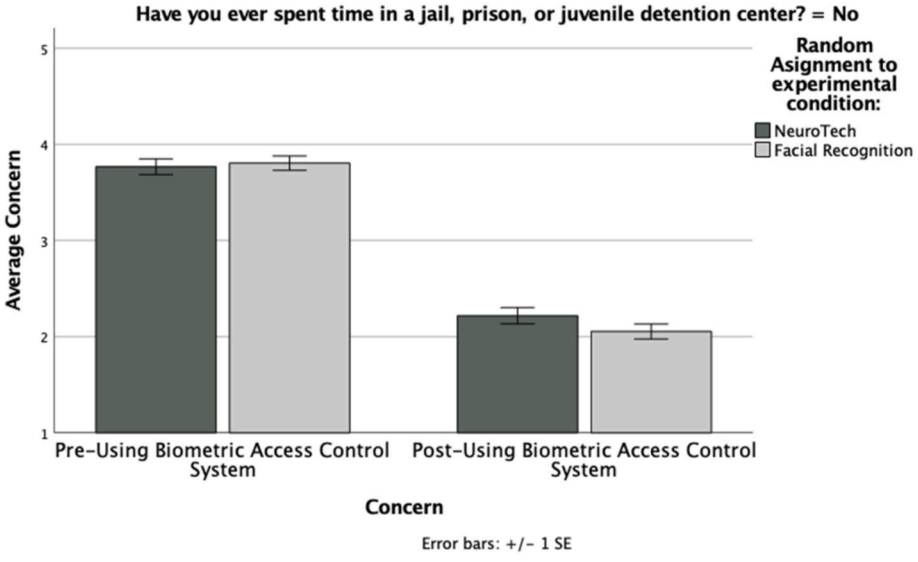

Fig. 3. Willingness to adopt the NeuroTech or Facial Recognition among formerly incarcerated and non-formerly incarcerated individuals.

encouraging engagement with mistrusted digital environments. This falls in line with previous research, as NeuroTech also improved privacy concerns and engagement with a mobile ID (Lucier et al., 2023). However, in our research, this effect was not moderated by incarceration status, indicating that NeuroTech is a broadly effective tool for improving privacy perceptions and engagement with digital environments across different populations. This finding suggests that the privacy features of NeuroTech, such as the focus on untraceable and unbreachable protection through localized data storage as well as neuro-based biometric authentication, are universally appealing to users, regardless of individuals' backgrounds or past experiences with privacy violations.

Interestingly, we found that incarcerated individuals expressed a greater likelihood of adopting privacy protection in general, both Biometric Access Control Systems and Facial Recognition, compared to non-incarcerated individuals. This is understandable because literature often highlights how formerly incarcerated populations have experienced significant breaches of privacy and control over personal information (Eubanks, 2018; Lynskey, 2019; Molitorisz, 2020; Seo et al., 2022), leading them to want stronger privacy protections. Given the history of marginalized groups being surveilled and discriminated against (Anderson et al., 2020; Driessen et al., 2023; Wolff et al., 2014), with individuals in Study 1 explicitly expressing that they feel surveilled and controlled by these digital technologies, it is unsurprising that formerly incarcerated individuals may find Biometric Access Control Systems particularly appealing as a means of reclaiming control over their privacy. This demonstrates the potential for Biometric Access Control Systems like NeuroTech to serve as a tool for empowerment among individuals who have been marginalized by the criminal justice system and demonstrates that formerly incarcerated individuals respond favorably when offered privacy systems that respect autonomy and minimize surveillance.

A key contribution of this research is its use of qualitative methods to capture the nuances of privacy concerns, such as the distinction between feeling uncertain about privacy versus feeling that privacy has been intruded upon. Privacy is not a monolithic concept; rather, it is multifaceted and context-dependent. By using qualitative approaches, we were able to gain a deeper understanding of how formerly incarcerated individuals experience and interpret privacy concerns. This highlights the importance of integrating qualitative research into quantitative studies of privacy, especially when exploring the experiences of marginalized populations whose voices are often left out of quantitative studies.

Despite these promising findings, the goal identifying equitable privacy technologies is far from complete. The digital landscape continues to evolve, and marginalized groups remain disproportionately vulnerable to privacy invasions and surveillance. To address these systemic disparities, we urge researchers, policymakers, and technology developers to prioritize the creation and adoption of privacy-enhancing solutions that are accessible, ethical, and inclusive. That is, our findings lay the groundwork for future research into the intersection of privacy concerns and technology use among marginalized populations, particularly formerly incarcerated individuals. Some researchers in Human-Computer Interactions (HCI) have begun to lay the foundation for valuable work among marginalized population (Hardy et al., 2019; Harrington et al., 2019; Taylor et al., 2024), however there is much more work to be done in the intersection of social justice and HCI (Chordia et al., 2024; Sannon & Forte, 2022).

Although respondents favored Neurotech to Facial Recognition, it is important to note that micro-vibrational signals like NeuroTech may be impacted by physiological variations seen between skin texture or moisture, which may also be impacted by external variations such as temperature or humidity. As a result, there is a concern for false rejection rates (FRR), which may be frustrating for users who may question the system's reliability. However, these drawbacks are present in many options, including Facial Recognition, and should be carefully considered when assessing user acceptance. Future research may benefit from prototype studies that include projected FRR, to understand how users feel about the frequency of FRR and any dissent behaviors that may occur as a result. Addressing the stability and usability challenges in future iterations of this research will be essential to ensuring that Biometric Access Control Systems like NeuroTech can reliably serve high-sensitivity populations like formerly incarcerated individuals.

Future studies should expand upon our findings by expanding beyond self-reported hypothetical data and conducting real-world experiments that allow participants to physically interact with NeuroTech when engaging with mistrusted digital environments. While our study provides valuable insights into participants' willingness to adopt NeuroTech, real-world testing is essential to understand how NeuroTech performs in practical, everyday settings. To tackle this, a prototype of this Biometric Access Control System can be created and used with users to assess real-time engagement, emotions, and adoptability. Additionally, larger sample sizes are needed to validate our findings and ensure that our conclusions can be generalized to a broader population of formerly incarcerated individuals. Importantly, this research provides novel exploration of using NeuroTech with mistrusted digital environments among a marginalized population. Although there is great work in this space, there is more work to be done to explore strategies that are specific to a marginalized population, rather than combining many marginalized groups together. As such, this study may serve as a framework for future research to explore further using Neurotech with other marginalized groups.

We acknowledge the limitations in using Prolific as a recruitment platform. While Prolific provides access to participants who self-report a history of incarceration, it does not guarantee a representative sample of formerly incarcerated individuals in terms of demographic diversity, socioeconomic status, or geographic distribution. However, our dual-recruitment approach mitigated this limitation by including participants from Project Rebound, a program that supports the integration of formerly incarcerated individuals into higher education. Additionally, Prolific's sample was instrumental in ensuring we could recruit sufficient numbers of participants for both groups, allowing for meaningful comparative analyses. This approach aligns with the exploratory nature of Study 1, which wanted to establish a list of mistrusted digital environments among our two populations of interest. Future studies may further refine this approach by incorporating additional recruitment sources to enhance the representativeness of the formerly incarcerated population.

Limitations in sample size and the use of hypothetical scenarios in Study 2 warrant caution in the interpretation of our results. While the findings are promising, further research with a larger, more diverse sample of formerly incarcerated individuals is necessary to fully understand the effectiveness of NeuroTech in addressing privacy concerns and improving engagement with mistrusted digital environments. Given the unique vulnerabilities of this population, especially the lack of control and privacy they face on a daily basis (Rennie & Crewe, 2023b; Turnbull & Hannah-Moffat, 2009; Werth, 2012), ensuring that this populate has access to privacy protection tools that align with their needs is a critical step in advancing equitable privacy protections in the digital age.

Finally, it is important to acknowledge that there are many reasons why formerly incarcerated individuals might not trust certain digital environments or privacy solutions. For example, moral values towards the collection of bodily data may impact trust with digital environments. Moreover, being unfamiliar with new technologies and psychological factors can also combine to influence adoption. As such, even if there is trust with NeuroTech, there may still be resistance among marginalized communities. Therefore, understanding the whole person, including their personality, knowledge of technology, or moral views would be important external factors to assess in future research.

6. Conclusion

As digital technologies become imbedded in daily life, addressing privacy concerns with mistrusted digital environments is essential, especially among marginalized populations like formerly incarcerated individuals (Cho et al., 2020; Liu et al., 2022). This study introduces NeuroTech, a novel and non-discriminatory Biometric Access Control System, and demonstrates its potential to reduce privacy concerns, instill feelings of control, and increase engagement with mistrusted digital systems.

NeuroTech outperformed traditional facial recognition by eliminating visual surveillance and discriminatory biases inherent in facial recognition, offering a more equitable and autonomy-enhancing approach to authentication and access control. NeuroTech minimizes surveillance be avoiding facial recognition and eliminates data transmission by offering users, local control over their data. Although formerly incarcerated populations may have concerns with existing systems, they may be open to solutions like NeuroTech that empower their autonomy—especially if implemented with respect.

By integrating qualitative narratives with quantitative outcomes, we show that NeuroTech directly addresses participants' fear of surveillance and loss of control. Our findings highlight the need for Biometric Access Control System designs that align with users' lived experiences and restore agency. To achieve this goal, technologists, policymakers, and researchers must work together to create inclusive privacy tools tailored to underserved and vulnerable communities. Future research must test these systems in real-world contexts using prototypes to better serve marginalized populations (including, but not limited to formerly incarcerated individuals), to advance digital equity in privacy protection.

CRediT authorship contribution statement

Eric Durnell: Writing – review & editing, Writing – original draft, Project administration, Conceptualization. **Ryan T. Howell:** Writing – original draft, Visualization, Formal analysis, Data curation. **Karynna Okabe-Miyamoto:** Writing – original draft, Project administration, Methodology. **Martin Zizi:** Supervision.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

Data will be made available on request.

References

Alsaadi, I. M. (2015). Physiological biometric authentication systems, advantages, disadvantages, and future development: A review. *International Journal of Scientific & Technology Research, 4*(12), 285–289.

Anderson, J. D., Pitner, R. O., & Wooten, N. R. (2020). A gender-specific model of trauma and victimization in incarcerated women. *Journal of Human Behavior in the Social Environment, 30*(2), 191–212. https://doi.org/10.1080/10911359.2019.1673272

Bacchini, F., & Lorusso, L. (2019). Race, again: How face recognition technology reinforces racial discrimination. *Journal of Information, Communication and Ethics in Society, 17*(3), 321–335. https://doi.org/10.1108/JICES-05-2018-0050

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

Big data analytics market size, share & industry analysis. (2024). *Fortune Business Insights*. https://www.fortunebusinessinsights.com/big-data-analytics-market-106179.

Chen, J. X., McDonald, A., Zou, Y., Tseng, E., Roundy, K. A., Tamersoy, A., Schaub, F., Ristenpart, T., & Dell, N. (2022). Trauma-informed computing: Towards safer technology experiences for all. *Proceedings of the 2022 CHI conference on human factors in computing systems*. https://doi.org/10.1145/3491102.3517475

Cho, H., Li, P., & Goh, Z. H. (2020). Privacy risks, emotions, and social media: A Coping model of online privacy. *ACM Transactions on Computer-Human Interaction, 27*(6). https://doi.org/10.1145/3412367

Chordia, I., Baltaxe-Admony, L. B., Boone, A., Sheehan, A., Dombrowski, L., Le Dantec, C. A., Ringland, K. E., & Smith, A. D. R. (2024). Social justice in HCI: A systematic literature review. *Proceedings of the 2024 CHI conference on human factors in computing systems*. https://doi.org/10.1145/3613904.3642704

Cybersecurity & Infrastructure Security Agency. (2024). AT&T discloses breach of customer data. https://www.cisa.gov/news-events/alerts/2024/07/12/att-discloses-breach-customer-data#:~:text=Release%20Date,Unlawful%20access%20of%20customer%20data.

DeVeaux, M. (2013). The trauma of the incarceration experience. *Harvard Civil Rights - Civil Liberties Law Review, 48*(1), 257–278.

Driessen, J. M. A., Dirkzwager, A. J. E., Harte, J. M., & Aarts, H. (2023). How restrictions of choice affect the sense of agency: The case of personal autonomy in prison. *Journal of Criminal Psychology, 13*(4), 381–393. https://doi.org/10.1108/JCP-12-2022-0035

Durnell, E., Okabe-Miyamoto, K., Howell, R. T., & Zizi, M. (2020). Online privacy breaches, offline consequences: Construction and validation of the concerns with the protection of informational privacy scale. *International Journal of Human-Computer Interaction, 36*(19), 1834–1848. https://doi.org/10.1080/10447318.2020.1794626

Edelman, B., & Luca, M. (2014). Digital discrimination: The case of Airbnb. https://www.benedelman.org/publications/airbnb-011014.pdf.

Edelman, B., Luca, M., & Svirsky, D. (2017). Racial discrimination in the sharing economy: Evidence from a field experiment. *American Economic Journal: Applied Economics, 9*(2), 1–22. https://doi.org/10.1257/app.20160213

Eubanks, V. (2018). *Automating Inequality: How high-tech tools profile, Police, and Punish the poor*. St: Martin's Press, Inc.

Guberek, T., McDonald, A., Simioni, S., Mhaidli, A. H., Toyama, K., & Schaub, F. (2018). Keeping a low profile? Technology, risk and privacy among undocumented immigrants. *Proceedings of the 2018 CHI conference on Human factors in computing systems* (pp. 1–15). https://doi.org/10.1145/3173574.3173688

Ha, A. (2024). *Detroit Police Department agrees to new rules around facial recognition tech. Techcrunch*. Com. https://techcrunch.com/2024/06/29/detroit-police-department-agrees-to-new-rules-around-facial-recognition-tech/.

Haney, C. (2002). *Psychological impact of incarceration: Implications for post-prison Adjustment | Office of justice programs*. US Department of Justice. https://www.ojp.gov/ncjrs/virtual-library/abstracts/psychological-impact-incarceration-implications-post-prison.

Hardy, J., Wyche, S., & Veinot, T. (2019). Rural HCI Research: Definitions, distinctions, methods, and opportunities. *Proc. ACM Hum.-Comput. Interact., 3*(CSCW). https://doi.org/10.1145/3359298

Harrington, C., Erete, S., & Piper, A. M. (2019). Deconstructing community-based collaborative design: Towards more equitable participatory design engagements. *Proc. ACM Hum.-Comput. Interact., 3*(CSCW). https://doi.org/10.1145/3359318

Lambrecht, A., & Tucker, C. (2019). Algorithmic bias? An rmpirical study of apparent gender-based discrimination in the display of STEM career ads. *Management Science, 65*(7), 2966–2981. https://doi.org/10.1287/mnsc.2018.3093

Liu, Z., Wang, X., Li, X., & Liu, J. (2022). Protecting privacy on mobile apps: A Principal–Agent Perspective. *ACM Transactions on Computer-Human Interaction, 29*(1). https://doi.org/10.1145/3475797

Lucier, D. M., Howell, R. T., Okabe-Miyamoto, K., Durnell, E., & Zizi, M. (2023). We make a nice pair: Pairing the mID with a NeuroTechnology privacy enhancing technology improves mID download intentions. *Computers in Human Behavior Reports, 11*, Article 100321. https://doi.org/10.1016/j.chbr.2023.100321

Lynskey, O. (2019). Grappling with "Data Power": Normative nudges from data protection and privacy. https://doi.org/10.1515/til-2019-0007.

Mason, R. O. (1986). Four ethical issues of the information age. *MIS Quarterly, 10*(1), 5–12.

McDonald, A. (2022). *Advancing digital safety for high-risk communities*. The University of Michigan. https://deepblue.lib.umich.edu/bitstream/handle/2027.42/174419/amcdon_1.pdf?sequence=1.

Melzi, P., Rathgeb, C., Tolosana, R., Vera, R., & Busch, C. (2024). An overview of privacy-enhancing technologies in biometric recognition. *ACM Computing Surveys*. https://doi.org/10.1145/3664596

Molitorisz, S. (2020). *Net Privacy: How we can be free in an age of surveillance*. NewSouth.

Okabe-Miyamoto, K., Durnell, E., Howell, R. T., & Zizi, M. (2021). Did Zoom bomb? Negative video conferencing meetings during COVID-19 undermined worker productivity. *Human Behavior and Emerging Technologies*. https://doi.org/10.1002/hbe2.317

Okabe-Miyamoto, K., Durnell, E., Howell, R. T., & Zizi, M. (2022). Video conferencing during emergency distance learning impacted student emotions during COVID-19. *Computers in Human Behavior Reports, 7*, Article 100199. https://doi.org/10.1016/j.chbr.2022.100199

Peña Gangadharan, S., & Niklas, J. (2019). Decentering technology in discourse on discrimination. *Information, Communication & Society, 22*(7), 882–899. https://doi.org/10.1080/1369118X.2019.1593484

Raji, I. D., & Buolamwini, J. (2019). Actionable Auditing: Investigating the impact of publicly naming biased performance results of Commercial AI products. *Proceedings of the 2019 AAAI/ACM conference on AI, Ethics, and society* (pp. 429–435). https://doi.org/10.1145/3306618.3314244

Rennie, A., & Crewe, B. (2023a). 'Tightness', autonomy and release: The anticipated pains of release and life licencing. *British Journal of Criminology, 63*(1), 184–200. https://doi.org/10.1093/bjc/azac008

Rennie, A., & Crewe, B. (2023b). 'Tightness', autonomy and release: The anticipated pains of release and life licencing. *British Journal of Criminology, 63*(1), 184–200. https://doi.org/10.1093/bjc/azac008

Sannon, S., & Forte, A. (2022). Privacy research with marginalized groups: What we know, what's needed, and what's next. *Proc. ACM Hum.-Comput. Interact., 6* (CSCW2). https://doi.org/10.1145/3555556

Seo, H., Britton, H., Ramaswamy, M., Altschwager, D., Blomberg, M., Aromona, S., Schuster, B., Booton, E., Ault, M., & Wickliffe, J. (2022). Returning to the digital world: Digital technology use and privacy management of women transitioning from incarceration. *New Media & Society, 24*(3), 641–666. https://doi.org/10.1177/1461444820966993

Sodhro, A. H., Sennersten, C., & Ahmad, A. (2022). Towards cognitive authentication for amart healthcare applications. *Sensors, 22*(6). https://doi.org/10.3390/s22062101

Stone, E. F., Gueutal, H. G., Gardner, D. G., & McClure, S. (1983). A field experiment comparing information-privacy values, beliefs, and attitudes across several types of organizations. *Journal of Applied Psychology, 68*(3), 459–468.

Tavani, H. T. (2007). Philosophical theories of privacy: Implications for an adequate online privacy policy. *Metaphilosophy, 38*(1), 1–22.

Taylor, J., Deng, W. H., Holstein, K., Fox, S., & Zhu, H. (2024). Carefully unmaking the "Marginalized User:" A diffractive analysis of a gay online community. *ACM Transactions on Computer-Human Interaction*. https://doi.org/10.1145/3673229

Turnbull, S., & Hannah-Moffat, K. (2009). Under these conditions: Gender, parole and the governance of reintegration. *British Journal of Criminology, 49*(4), 532–551. https://doi.org/10.1093/bjc/azp015

United States of America v. Facebook, Inc. (2019). https://www.ftc.gov/system/files/documents/cases/182_3109_facebook_order_filed_7-24-19.pdf.

Werth, R. (2012). I do what I'm told, sort of: Reformed subjects, unruly citizens, and parole. *Theoretical Criminology, 16*(3), 329–346. https://doi.org/10.1177/1362480611410775

Whittaker, Z. (2024). The biggest data breaches in 2024: 1 billion stolen records and rising. Techcrunch.Com. https://techcrunch.com/2024/08/12/2024-in-data-breaches-1-billion-stolen-records-and-rising/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAANaDDexHvecMCIqksUqk9i1-FA3UZZk-W9u008dxX47D-PivitMv95Nz_Vi_RG6OFJvtMvP71MMpvPmtENg0Zn42q0G2mCL644o0Blx9sU1J2-JmuJC_qw2w7wGFv399J5Lw1-msgWcFkRpm2egTR4ziFrLh5VOsC9cW-k3nORtx.

Williams, D. P. (2020). Fitting the description: Historical and sociotechnical elements of facial recognition and anti-black surveillance. *Journal of Responsible Innovation, 7*, 74–83. https://doi.org/10.1080/23299460.2020.1831365

Williams, R. (2024). I was wrongfully arrested because of facial recognition technology. *It Shouldn't Happen to Anyone Else*. Time. https://time.com/6991818/wrongfully-arrested-facial-recognition-technology-essay/.

Wolff, N., Huening, J., Shi, J., & Frueh, B. C. (2014). Trauma exposure and posttraumatic stress disorder among incarcerated men. *Journal of Urban Health, 91*(4), 707–719. https://doi.org/10.1007/s11524-014-9871-x

Yan, Y., & Yang, Z. (2023). Spoofing real-world face authentication systems through optical synthesis. *2023 IEEE Symposium on security and privacy (SP)*. https://doi.org/10.1109/SP46215.2023.10179351