

“The System Will Choose Security Over Humanity Every Time”: Understanding Security and Privacy for U.S. Incarcerated Users

Yael Eiger¹, Nino Migineishvili¹, Emi Yoshikawa¹, Liza Nadtochiy¹, Kentrell Owens², and Franziska Roesner¹

¹University of Washington

²Max Planck Institute for Security and Privacy

Abstract—Digital devices like tablets, media players, and kiosks are increasingly deployed in U.S. prisons. These technologies can enable incarcerated people to access education, communicate with loved ones, and develop vital reentry skills. However, they can also introduce new privacy and security risks for incarcerated people who have little agency over their usage and contracts, and are currently carved out of many consumer protection safeguards. To investigate these issues, we conducted focus groups and interviews with system-impacted people, i.e., those formerly incarcerated and their relatives (N=17), revealing experiences with device-related security and privacy vulnerabilities and the power dynamics that affect their use. Our participants described pervasive surveillance, censorship, and usability problems with the technology available to them, including shifting and seemingly arbitrary usage policies. These policies strain relationships both inside and outside prisons and contribute to negative downstream effects for incarcerated users. We recommend ways to better balance prison security concerns with privacy-related needs of system-impacted individuals by promoting accountability for technology-related decisions, providing public oversight of digital purchasing and use policies, and designing digital tools with them—the actual end-users—in mind.

I. INTRODUCTION

Tablets, media players, kiosks, and other digital devices are proliferating throughout U.S. prisons and jails [72], [85], [87], [11], enabling incarcerated people to access education and legal services, communicate with loved ones, and learn vital skills for re-entering our increasingly digital society [7], [23], [61]. The use of technology in this context is widespread, directly affecting an estimated 1.9 million currently incarcerated people in the U.S. and another 113 million people (45% of the U.S. population) who have an immediate family member who has been to jail or prison [82]. Collectively, this cohort is defined by the UC Berkeley Underground Scholars Initiative as “system-impacted” people [20].

Prior research has documented security and privacy issues due to other technologies in the carceral system, such as electronic monitoring for people on parole or probation [55]. Others have studied experiences with technology post-release, such as the experiences of formerly incarcerated people navigating their release from prison and re-entering society [61], [53], [54], [67]. One prior work at CHI studied the experiences with surveillance of loved ones communicating with their incarcerated relatives [56]. In this work, we take a broader

perspective, focusing on the experiences of people who directly experienced technology while incarcerated, including technologies they had access to beyond communication.

Closing the public knowledge gap about experiences *while* incarcerated is crucial because incarcerated people have limited agency regarding when, how, and whether they can use digital devices [5], [9]. Their access is determined and restricted by specific prison policies and contracts with digital system purveyors. Further, two companies, ViaPath and Securus, dominate the market supplying prisons and jails with digital devices [24]. Such limited options have been shown to burden and harm a disadvantaged and vulnerable population who already lack legal rights to privacy and the safeguards provided by consumer protection laws [5], [9], [45].

Moreover, policies that govern the use of the digital devices allowed in the carceral system are often driven by concerns about the “security” risks they pose for the prisons [31], [90], [73], [89], [88]. Examples from the 1980s and 1990s, and as recently as 2024, suggest that prison officials often cite unsubstantiated security threats to justify revoking computer access; this is true even when programs demonstrate clear rehabilitative benefits and near-zero recidivism [90], [73], [89].

In this work, we investigate the security and privacy experiences of system-impacted people using digital devices while incarcerated, from their own perspectives. We investigate:

- **RQ1:** What security and privacy threats, risks, and concerns do system-impacted people experience when **utilizing digital devices while incarcerated?**
- **RQ2:** How do system-impacted people perceive security and privacy-related **prison policies and their implementation** by prison officials?
- **RQ3:** What **downstream effects** do system-impacted people experience as a result of these issues?

To that end, we conducted focus groups and interviews with 17 system-impacted participants, including 12 formerly incarcerated people and 5 loved ones.

Our participants reported that they experienced pervasive forms of surveillance and censorship related to available technologies during incarceration. They described shifting and arbitrary technology censorship policies that strained their relationships with outside communities and threaten their

future rehabilitation. They related experiences of living in a “panopticon”¹ of surveillance that exacerbates feelings of dehumanization, self-doubt, and mistrust towards technology and the prison infrastructure. This lack of privacy further caused participants to feel at once powerless to affect and grateful for the scant access to technology they do have, described by one participant as “technology Stockholm syndrome.”²

Our participants also described how prison policies regarding technology use stem, in their view, from incomplete or misguided mental models that prison officials hold about the incarcerated population and their ability to misuse technologies, as well as the technologies themselves. The concerns about prison security raised by these mental models lead in part to the technology restrictions and surveillance (and the downstream harms) that our participants describe.

Beyond giving voice to the experiences of our participants, our findings raise considerations about ways in which normative security and privacy beliefs become replicated and amplified through the medium of digital technologies. Presumptive security and privacy concerns expressed by prison administration can give rise to a real, practical lack of security and privacy for incarcerated people and their loved ones. This finding provokes and aligns with broader questions asked in recent security and privacy research, namely the consideration of marginalized and/or vulnerable populations in threat modeling [14]. In other words: security and privacy *for whom*?

II. BACKGROUND, RELATED WORK, AND MOTIVATION

A. Digital Devices in U.S. Prisons

ViaPath and Securus build and distribute digital devices such as tablets and media players to U.S. prisons. The devices come pre-loaded with their messaging applications “GettingOut”/GTL for Viapath and “JPay,” which became Securus after a 2015 buyout [66]. To send messages, loved ones outside of prison must separately access the GettingOut or JPay/Securus applications by downloading them on their personal devices. The Prison Policy Initiative estimates that these two companies control more than 80% of the market share for carceral communication technology [24], [86], operating in thousands of facilities [65], [81]. In our geographic area, the prisons predominantly contract with Securus; thus, our participants had used JPay and Securus, not Viapath, products.

These technologies and apps are changing rapidly. Over the past decade, for example, telephones have been almost wholly replaced by kiosks (wall-mounted computer screens protected by a steel box) [41]. Kiosks, in turn, are now being supplemented by personal media devices and tablets [41]. Such devices are used for communication purposes

(e.g., messaging), though our participants also described other purposes, such as using the (same) tablets as music/media players and to access legal services.

These technologies, which are available to (some³) incarcerated people – Securus/JPay, ViaPath/GettingOut, and kiosks – make up the scope of this paper, including both their uses for communication with their loved ones in the outside world, and usage for media consumption like those listed in Table II.

B. Security and Privacy Concerns for System-Impacted People

During Incarceration. The privacy and security concerns with technologies available within prisons are not hypothetical. ViaPath and Securus have come under scrutiny for poor privacy practices and over-surveillance of users. For example, in 2018 Securus was sued for collecting and storing location data, audio recordings, and transcripts of phone calls from people in prison, including calls protected by attorney-client privilege [79], [42]. Securus settled the lawsuit and their contract was renewed with the correctional facility [27], [70].

Thus, security, privacy, and related concerns for the system-impacted population exist. But to our knowledge, their own self-reported experiences, and the downstream effects of those concerns, have been understudied: for example, Verbaan et al. [80] notes that the prison context has been largely overlooked in computer science, especially with respect to how system-impacted people experience and use technology.

Previous academic work by Owens et al. [56] considered *the families and loved ones* of currently incarcerated people and their mental models of surveillance when using carceral communication tools. Our findings support and strengthen those of this prior work, as well as add new perspectives. Specifically, we gather the perspectives of *formerly incarcerated people themselves* (in addition to their families or loved ones), and we consider technology use cases beyond communication. Our findings also extend beyond surveillance to other privacy, usability, and consumer protection concerns, as well as downstream impacts.

After Release. After release from prison, system-impacted people continue to experience technology restrictions and associated security and privacy impacts. For example, Owens et al. [55], [57] investigated the technical, legal, and human-centered impacts of electronic monitoring applications used for parole, probation, and immigration restriction.

Prior work on digital technologies post-release also shows that privacy concerns can lead formerly incarcerated people to avoid or limit their engagement with digital technologies, and many people cite surveillance concerns in particular [53], [67], [56]. For example, Seo et al. [67] examine women transitioning from incarceration and note that post-incarceration discomfort with the internet often stems from its association with the surveillance they experienced in prison. As such, online privacy concerns often make people, in particular

¹The term “panopticon” was popularized by Foucault [25], but the “panopticon” prison was originally designed by Bentham. The panopticon guarantees that incarcerated people are unaware of when or whether they are being watched at a given moment, which in turn creates self-regulation.

²The term our participant used, “Stockholm Syndrome,” refers to the phenomenon of a hostage developing a bond with or even gratitude towards their captor, which has also been described as “a conscious coping strategy that can be understood as a form of adaptive behavior, providing hope for the victim in an otherwise hopeless situation” [35].

³Securus serves thousands of correctional agencies and 1.2 million incarcerated people across North America [65]. ViaPath similarly operates in thousands of facilities across more than 30 state corrections departments and hundreds of county jails [81].

underserved populations, hesitant to acquire new skills and engage with technology [68]. Gurasami et al. [33] coined the term “carceral web” to refer to a lack of agency formerly incarcerated people feel over their privacy, due to the internet’s ability to publicize, archive, and document their crimes.

C. *Notions of “Security” in Carceral Systems*

Prisons have a long history of incorporating and then revoking technology access for the incarcerated. For example, in 1986, incarcerated people at the Washington State Prison in Monroe were allowed to purchase computers and other devices to keep in their cells [90]. According to Paul Wright, founder and director of the Human Rights Defense Center, recidivism rates for these people was “nearly zero” [90], [89], [73]. A later director terminated the program, citing it as a “security issue,” even though he acknowledged under oath that no threat had arisen due to the program [90], [89].

The policies that govern the use, and often revocation, of digital devices continue to be justified with notions of “security” risks [31], [90], [73], [89], [88] for the prisons. As recently as 2024, officials restricted access to the ironically named “Securebook 5” computers for incarcerated students based on amorphous security concerns [88].

In the prison context, the considerations of “security” are inextricably linked with the practices of privacy. For instance, a new AI system called Verus was deployed across correctional facilities in eight states to monitor calls between incarcerated people and their loved ones; the system monitored 2.5 million calls during a 2021 year-long pilot in Suffolk County, New York alone [6]. The stakeholders, this time governing the introduction of a new technology that accentuated surveillance while diminishing user privacy, were once again correctional facilities aiming to detect “security threats” [6].

These digital technologies are designed with prisons as the main stakeholders. Prisons hold the authority to determine how to implement and deploy technologies within their facilities based on their unique security and privacy conceptions. Their motivations and viewpoints are well-documented in prior work [48], [43], [78]. In contrast, our paper focuses on a different stakeholder: system-impacted people as the direct end-users of these technologies. For instance, when looking at the Verus system from the perspective of the actual end-user, we see privacy breaches: Verus flagged conversations of system-impacted people referencing the Spanish word for “lawyer” and conversations concerning COVID-19 cover-ups in detention facilities [6]. Viewing Verus from the perspective of the incarcerated reveals a different notion of “security and privacy,” one where safety, health and right to confidential communication with legal counsel are jeopardized.

III. METHODOLOGY

A. *Positionality*

As researchers, our experiences and worldviews alter the perspectives we bring to our work [84], [44]. Thus, we describe our identities and positionality here. The research

team included people with varied ethnicities and races, socioeconomic, geographic, and educational backgrounds, as well as a diverse set of experiences with policing and the carceral system. Multiple authors have spent years teaching classes in prisons and working closely with re-entry organizations. Significantly impacting our perspective, however, is the fact that no researcher on our team has personally been incarcerated.

B. *Recruitment*

Participants were recruited through advocacy organizations that we have community partnerships with. These organizations are led by, include, and maintain established, trusted relationships with the communities we sought to engage. In addition to supporting recruitment, these partnerships provided a foundation for more sustained support for participants beyond the study itself and offered a continuity of care and resources rather than a one-time interaction. The authors also continue to nurture and give back to these community partnerships, subsequently co-organizing and co-designing workshops and events together.

After identifying and enrolling the first few participants through these organizations, we employed snowball sampling [64], [12] to expand our participant pool. This method leveraged participants’ existing social networks. Our fliers asked if participants had any experience with carceral technology such as JPay or Securus, but it did not reveal other research questions we planned to study.

Participants were subsequently asked to fill out a screening survey, which we used to verify their eligibility. Participants had to be over 18, have firsthand experience using JPay/Securus or GettingOut, and be formerly incarcerated or loved one of someone who is currently incarcerated. We chose not to directly interview currently incarcerated people to minimize potential risks to that population (see Section III-G).

For confidentiality reasons, we chose not to collect or report demographics, including race and socioeconomic status, which historically has a strong impact on over-policing and incarceration rates. To ensure we captured these experiences but did not risk participant privacy, we intentionally recruited from organizations that represent and advocate for these historically over-incarcerated identity groups, including an advocacy group for incarcerated Black people, an advocacy group for incarcerated Native American & Indigenous people, and a group working on the overlap of incarceration and housing insecurity.

C. *Participants*

In total, we conducted 4 focus groups and 5 one-on-one interviews, with a total of 17 participants. We offered the option of focus groups to all participants, in part because prior research indicates that vulnerable groups may feel more comfortable sharing their experiences in group settings [59], [58] and when participants are already acquainted. Thus, based on participant preferences, we conducted some focus groups among participants who already knew each other (i.e., with their family members or social connections that were also

	Session	Status	Access To
P1	Focus Group 1	Formerly Incarcerated	JPay, Kiosk
P2	Focus Group 1	Formerly Incarcerated	JPay, Kiosk
P3	Focus Group 1	Formerly Incarcerated	JPay, Kiosk
P4	Focus Group 2	Formerly Incarcerated	JPay, Kiosk, Securus
P5	Focus Group 2	Formerly Incarcerated	JPay, Kiosk, Securus
F1	Focus Group 2	Family member	JPay, Securus
P6	Focus Group 3	Formerly Incarcerated	JPay, Kiosk
P7	Focus Group 3	Formerly Incarcerated	JPay, Kiosk
F2	Interview 1	Family member	JPay, Securus
P8	Interview 2	Formerly Incarcerated	JPay, Kiosk, Securus
P9	Interview 3	Formerly Incarcerated	JPay, Kiosk, Securus
F3	Focus Group 4	Family member*	JPay, Securus
F4	Focus Group 4	Family member*	JPay, Securus
F5	Focus Group 4	Family member*	JPay, Securus
P10	Focus Group 4	Formerly Incarcerated	JPay, Kiosk, Securus
P11	Interview 4	Formerly Incarcerated	JPay, Kiosk
P12	Interview 5	Formerly Incarcerated	JPay, Kiosk, Securus

TABLE I: **Focus Group and Interview Participants.** In total, we recruited 17 participants, 12 of whom are formerly incarcerated (denoted by the letter “P” followed by the participant number) and 5 of whom were family members of currently or formerly incarcerated individuals (denoted by the letter “F” followed by the participant number, and marked visually with a colored background). Family members of formerly (rather than currently) incarcerated individuals are denoted with an asterisk. Participants’ access to technologies depended on when and where they were incarcerated.

eligible for our study) as well as some individual interviews. Spanning these focus groups and interviews, twelve participants were formerly incarcerated, and five were family members of currently incarcerated people or formerly incarcerated people (see Table I). Specifically, the family member in Focus Group 2 (F1) is both family to their currently incarcerated spouse, and family to the formerly incarcerated people in their focus group (P4, P5). The Family member in Interview 1 (F2) has a currently incarcerated spouse. The family members of Focus Group 4 (F3, F4, F5) are family members of the formerly incarcerated participant in their focus group (P10).

We iteratively analyzed data as we collected it. We reached thematic saturation, i.e., no new themes emerged, after 11 participants, although we continued with our scheduled focus groups and interviews until we reached 17 total participants. The codebook continued to remain unchanged throughout these final interviews, so we stopped recruiting for more participants after completing all scheduled sessions. A link to our full codebook and interview protocol can be found at [this OSF directory](#).

D. Interview Logistics and Protocol

Interviews lasted approximately one hour and were conducted either in-person or remotely, depending on the participant’s preference and comfort level. One to three researchers were present during these sessions. While we reserved private rooms on campus for in-person interviews, we recognized that some participants might feel uneasy or uncomfortable coming to a university setting. Additionally, we acknowledged that many participants live in rural or suburban areas where the commute to the university can be prohibitively long or expensive. To reduce barriers to participation and increase

accessibility, we offered to meet participants at community-based locations such as public libraries or community centers closer to where they live. Participants were compensated \$35 USD per hour in a prepaid VISA gift card in addition to commuting and parking costs.

Participants gave informed consent twice: before scheduling interviews/focus groups, and again verbally at the start of the session. Sessions were audio recorded with consent.

After establishing that everyone was comfortable, and asking some icebreaker, intro, and rapport building questions, we asked participants about their in-prison or outside experience with technology. Since different prisons contracted with different technology vendors, we asked them to clarify which technologies (e.g., JPay, Securus, GTL) they used and when. We also asked about other technology used in the prison. We then prompted participants to discuss their security and privacy concerns and what factors influenced their experiences. We asked how these practices impacted relationships and dynamics inside and outside the prison. We closed by asking participants to share their aspirations for change. The interview protocol between formerly incarcerated people and the loved ones of currently incarcerated people contained no differences except for slight variations in wording (e.g., “Where and when were you incarcerated?” vs “Where and when is/was your loved one incarcerated?”).

Because we believed the interviews might contain sensitive information, we manually transcribed the recordings rather than using a third-party transcription service, stored all transcripts in directories only viewable by the research team, and used encrypted messaging tools to schedule the interviews.

E. Ethical Considerations

Our study was approved by our Institutional Review Board (IRB). Given the sensitive nature of incarceration, we took proactive measures to ensure that the research environment remained kind, safe, and participant-centered.

We collected identifiable information including participants’ full name, email address, and phone number solely to administer participant compensation, as mandated by our institution. This information was stored in a separate spreadsheet not linked to research data, where participants were identified only by unique identifiers (e.g., “P1”). All data was stored in a password-protected Google Drive only accessible to the research team. Each participant was also assigned a unique participant identifier (e.g., “P1”), which was used throughout the research documentation and analysis. Audio recordings were transcribed fully manually and no third-party service was used. All quoted material was de-identified.

We did not ask participants about their criminal charges, sentencing, or details of their incarceration. Anticipating that some topics might provoke discomfort, we designed interviews with built-in breaks and flexibility. While no participants chose to pause or end the interview early, we remained vigilant and prepared to accommodate such needs. Participants were reminded throughout that they could skip questions or retroactively request the removal of content.

Category	Code
Communication Tech.	Mail CorrLinks Messaging (Securus/JPay/GTL) Kiosk
Media & Education	Laptops Legal/policy library eBooks Television Music
Benefits	Faster communication Training for re-entry Cultural touchstone
Harms	Usability problems Censorship Scarcity Expensive Bargaining chip Adaptation Insufficient knowledge Loss of social connections Apathy Surveillance
Policies	Funding Daily technology use Communication Costs
Stakeholders	Department of Corrections staff Technicians Government officials

TABLE II: Overview of the high-level themes surfaced in our qualitative codebook. The full codebook can be found in [our OSF directory](#).

The final manuscript was sent to participants via email two weeks before submission, so that they could highlight any areas they felt misrepresented their experiences or felt sensitive. The feedback we received from participants was positive and no one requested a removal of their quotes.

F. Data Analysis

Data analysis was conducted in multiple stages. Initially, we used a collaborative, qualitative open coding technique [74], where researchers separately examined two different interviews and/or focus groups and drew up initial codes. These codes were then combined and further refined collaboratively. This led to the creation of a codebook that encapsulated codes relating to (1) technologies used by system-impacted people and (2) the benefits and harms of these technologies. We repeated this process with two additional interviews and/or focus groups by two researchers. This resulted in the creation of a new code addressing (3) prison policies, people or parties that govern the use of technologies, and security & privacy concerns. Finally, two researchers applied the established codebook to all transcripts. Our final codebook is in Table II.

We then used inductive thematic analysis [13] to uncover overarching themes. Three authors independently derived themes from the transcripts. The themes were later converged through open discussion among all researchers.

G. Limitations

Our study focused on persons incarcerated in state and federal prisons in the Puget Sound region to surface findings in a context that we understood well. As such, our results should not (and, like much qualitative research, are not intended to) be interpreted as generalizing beyond this. We focused on technology that people use while incarcerated, rather than things like prison surveillance cameras, which incarcerated people do not use but are subjected to.

We also acknowledge the limitation in recruiting via snowball sampling and that people who know each other may hold similar views that are not generalizable at scale.

To minimize the amount of personal information collected, we did not gather individual demographic data (e.g., race, age, ethnicity, sentence duration, sentence dates, etc.). As a result, we are unable to analyze our findings in relation to these demographic factors.

We also acknowledge the limitation of focusing only on formerly incarcerated people and their loved ones while excluding currently incarcerated people. Though it is possible to do research ethically with currently incarcerated people, we recognize that working with a more vulnerable group carries additional risks that we did not need to impose to answer our research questions. Following best practice, we thus interviewed proxies for this vulnerable population [8].

Moreover, we did not include many other key stakeholders in the carceral system. For instance, we did not interview technology developers, Department of Corrections officials and staff, technology company representatives, police officers, or lawyers. We felt there was a gap in understanding the perspectives of system-impacted people specifically, while the opinions and stances of prison officials regarding technology have been well-studied and documented [36], [15], [49]. Our choice to study the opinions of a marginalized population is in line with prior work that focuses on electronic monitoring subjects [55], undocumented immigrants [32], or survivors of stalkerware [26] without including the viewpoints of technology developers and deployers.

IV. FINDINGS

We organize our findings using the classic Alice and Bob communication model. Here, Alice is an incarcerated person attempting to communicate (e.g., via Securus), and Bob is a loved one outside of prison on his regular mobile device. We discuss the digital security and privacy experiences of Alice and Bob, the role of prisons as a “man in the middle”, and the downstream negative impacts for Alice and Bob.

A. Security & Privacy Experiences of System-Impacted People

In the initial stage of the Alice and Bob communication model, Alice attempts to send a message to Bob using prison-provided communication tools. This section describes the security and privacy concerns that emerge for Alice and Bob in this direct communication line. Participants described this step as rife with involuntary and stringent censorship (Sections IV-A to IV-A) that delay communication (Section IV-A).

Following the naming conventions in Table I, quotes from formerly incarcerated Participants are denoted with “—P” e.g., “—P1” and quotes from Family members are denoted with “—F” e.g., “—F1”.

Censorship Is Overwhelming. All participants commented that digital censorship is prevalent, e.g., F2: “Everything is monitored. Everything is censored.” The censorship extends both to the person that a system-impacted individual is allowed to communicate with and to the words and messages allowed to be exchanged between them. P1 summarized:

“There’s so much censorship around all of that. Right, because you’re not allowed to talk to other prisoners. You’re censored in that...Even with the people that you do talk with, you guys could talk...but only about certain things.” —P1

Participants perceived censorship as extending beyond communication, attributing limited availability of educational materials on the devices to deliberate censorship decisions:

“They censor the books that we’re able to get in...They censor the music. They censor the motivational speeches.” —P1

The apparatus that enables this vast censorship is surveillance. P6 explained that “[the Department of Corrections, DOC] tracks everything. Everything gets recorded.” P9 further perceived that underpinning censorship was a system of “surveillance of the video call and text system; every message was ‘reviewed’ by somebody.” This constant, unrelenting prevalence of surveillance and censorship had downstream effects, as we describe in Section IV-C.

Consent Is Involuntary. Participants reported that surveillance and censorship breached their privacy. As F2 observed:

“It really is an invasion of privacy. Because before that letter gets in [loved one’s] hand...how many people have already looked at it and sorted through it? I don’t really like that feeling.” —F2

However, system-impacted people have no option but to continue utilizing and depending on the digital devices that are available. P7 noted that in prison:

“You give consent by being there. Nobody asks you for any kind of consent. Do you want a phone call? Do you want an email? Do you want music? Consent is implied...if you want any of that.”

P8 asked: “When it’s the only option, what else do I do?” We discuss how this lack of free choice about what technology and provider they choose to use (if any), leads to a sense of apathy and reluctant acceptance in Section IV-C.

Technology Changes Increase Surveillance. All participants mentioned initially using physical mail and wall-mounted phone to communicate with their loved ones outside the prison. This changed over time; many described the introduction of JPay devices as a means to communicate with loved ones.

Following a 2015 buyout of JPay by Securus [66], many participants’ JPay devices were replaced with Securus tablets.

Updates and changes in technology did not necessarily lead to the improvements participants hoped for. For example, the changeover from JPay to Securus after the buyout led to a decline in quality and usability of the technology:

“Once it switched over to Securus—can’t believe we’re gonna say this—that we actually miss JPay. Securus just seems like it has, they both have their own set of problems, but it just seems like the technology has not gotten better, it’s gotten worse, with Securus.” —F2

The changeovers negatively affected usability and increased surveillance and censorship, leading to more stringent restrictions for participants. P6, for instance, described how communication had become more restrictive:

“Nowadays, it being Securus and the changes that they’ve made, people on the outside are not allowed to initiate contact...You used to be able to send emails out; you could talk to them if you knew their email address; there’s no option for that anymore.”

The perception of increasing censorship was also felt with new technology. F2 described: “With JPay, [it’s] more censored, even more so.” Despite the outside world advancing technologically, our participants felt their technology was regressing; P9 described how “it was really fascinating to watch backward technology while [time] was going forward.”

Surveillance Leads to Communication Delays. Because messages are surveilled for content, participants experienced long delays in their communication being sent and received, if they are received at all. Moreover, participants lacked information about whether their messages were censored, and how. As P1 described:

“Even if you message on JPay but you said the wrong thing on there...Your messages may come through slower...or they won’t come through at all. Sometimes, they don’t even let [you] know that.”

The delays and drops in message exchange due to censorship belie the idea of seamless communication through technology according to some participants. As P8 reflected:

“...you think, ‘Oh, I can write this email’ and...send it off into the ether; it could sit in the mailroom for days if it had something in it that alerted [the prison officials]. And then you wouldn’t even know that your email didn’t go out, let alone why you weren’t getting a response, or if it did go out, but now they’re watching you.” —P8

We elaborate more on the working of censorship through technology surveillance in Section IV-C.

Other Consumer Protection and Autonomy Issues: Usability Challenges and Financial Burdens. The monopolies of few companies on the market for digital devices in U.S. prisons, combined with the technology access restrictions that stem (at least apparently) in part from prison security concerns, also led to serious usability and financial challenges.

Both were such pervasive and taxing issues that all of our participants brought them up without being prompted.

In terms of hardware usability, the tablets were prone to easy breakage. P5 described that: “one of the worst things that would happen would be the battery swelling...it’d swell up and crack the screen.” The constant hardware problems forced participants and families to pay for devices anew, which, as P4 implies, benefits Securus: “Tablets would break because they’re poor quality. They always broke because then we would have to re-buy them.”

Participants further experienced software issues whereby their applications often froze, their purchased data was lost, or telecommunication features worked poorly. F2, a family member, described: “we deal with this almost every day—sometimes, he’ll call, and it will be dead air. Or he’ll have to call back. And I don’t realize. On his end, he’s probably trying 20 or 50 times to try to get through.”

Finally, the physical implementations of devices caused discomfort. F1 described the physical contortions that their incarcerated spouse had to undergo when video calling at a poorly designed kiosk with a payphone handset attached to a cord that is only 12 inches long: “We typically won’t even go like the full 30 minutes at the call because his neck, like you can see how uncomfortable it is, holding that.”

All participants, without being prompted, also mentioned the costly pricing and hidden fees when using prison technologies. This was particularly worrisome for participants given that, generally in the non-prison environment, the same services (such as email) are free. P4 described how these exorbitant costs compared to their low wages, observing:

“[Sending a message costs] 50 cents, and if you do that everyday, then of course that’s like 15 dollars a month, and in a place where they pay you, I think it’s 18 cents an hour, 21 cents an hour ... So I mean those things balance poorly.”

P11 similarly expressed that “They cost more than what we are paid. For no reason at all.” The costs and fees also burdened the loved ones of incarcerated people, who often used these technologies to send money. P8 explained that:

“When I was first incarcerated, if you got money sent in, it was 35% taken out, and it changed to 55% within a couple years of my incarceration. Which means if you get 100 bucks sent in, you’re only getting 45 out of it ... it’s really hard to justify that to a family...already struggling.”

As such, participants were financially burdened by both the fees charged by Securus, and the taxation policies of DOC. President Biden attempted to put a cap on these fees [17], although President Trump reversed this in 2025 [19].

B. Prison as the “Man” in the Middle

Before Bob receives Alice’s message, it is intercepted by Department of Corrections (DOC) staff, i.e., the “man in the middle” who exerts technical and bureaucratic control over the communication channel. Participants perceive this interception as a symptom of power asymmetry wherein power is

unilaterally exercised by staff (Section IV-B); their perspective was that that staff often operate from misinformed or overly punitive threat models (Section IV-B).

Power in the Hands of Officers. The extent to which participants can access technology, and how they are surveilled and censored, depends on the discretion of the staff and officers overseeing them. P4 observed that: “The power dynamic that exists within the carceral circumstance is one that entirely leaves it up to the whim of whatever staff member it is.” This power dynamic fosters feelings of scarcity and competition around technology. P1 described this in the context of the kiosks, saying: “Oftentimes, [the kiosks] were so overloaded that one of them would be down.” They noted that this scarcity led to conflict: “There were so many altercations, so many fights, so many assaults, just because of that.”

The increase in altercations as a result of device scarcity, rule-setting, and restriction can be seen as ironic given that the justification for these restrictions is often “safety” and “security.” P1 hypothesized that the scarcity was engineered since officers profited from the chaos, underscoring the lack of trust between incarcerated people and prison staff:

“They [the Department of Corrections officers] run up the fights, they run up the infractions, and they say, ‘Oh well, we need this much more in the budget because we need to hire this many more people for security or the guards need to work overtime.’ ”

These power dynamics also apply to censorship. Officials have discretion about whom and what they censor, and are perceived as wielding this power with prejudice, as P1 explained: “There’s one individual who for some weird reason, may just dislike you. And that’s the thing about it, there is no recourse. So yeah, so they are more likely...to listen to our calls.”

Thus, participants felt that technology was often weaponized against them to restrict their privacy and increase officers’ power. They observed that securing against digital threats seemed more important to prison staff than incarcerated people having the ability to communicate with their loved ones, lawyers, or community members. P2 summed this up as: “the system will choose security over humanity every time.”

Censorship Feels Arbitrary. The power of individual officials to control censorship was combined with a sense of inconsistent policies; the decision about who was censored and how seemed arbitrary to participants. For example, P4, in a focus group with P5, said “[P5] and I can send the exact same image to two different people, and one will get it on the exact same day, and the other will get it rejected.”

F1 also recounted a time they tried to communicate with their incarcerated spouse, and the message was censored:

“I mean this was like a very basic email that I had sent my husband, like nothing suggestive. Like, ‘Call me at whatever time’ or something like that. And [officers] sent [me] this thing that there was like, obscene whatever...it was just nuts.” —F1

Such seemingly arbitrary decisions contribute to further power disparities, allowing officers to control what people can see

and when. They can, with little warning or recourse, restrict communication with loved ones or legal counsel. For instance, P4 explained that:

“[My spouse] would send legal work that I was working on; she’d take pictures of it so that I could edit it. [A]nd there came a point where [an officer said] said, ‘Yeah, we’re rejecting this, it’s too much text to review.’ ” —P4

Prison Staff May Hold Inaccurate Threat Models. Staff and officers wield power and use technology as another means to exert it. Participants felt that prison staff’s misconceptions about technology may exacerbate these issues. P8 explained that they did not think prison officials had a factual understanding of the technology, and, because of this, took away access to it, saying: “They slowly were like ‘Okay, wait a second, we think something tech-y is happening here, but we don’t know what. So we’re gonna take away all these things.’”

P8 continued by explaining how the officers are taught to restrict the digital rights and access of incarcerated people due to security fears while actively violating the security and privacy of incarcerated people:

“So the officers actually have all the access to everything that could hurt us. And yet they are taught to be afraid of us. . . . They’re literally thinking, ‘You might get my login for something; you might see my password; you might see the information that’s in my employee account’ . . . They’re not thinking of you getting a hold of somebody’s piece of mail; they’re literally thinking of their digital identity.” —P8

Finally, technology is perceived as both overwhelmingly powerful and yet simultaneously fragile and easily compromised by any unsupervised incarcerated person. This lack of understanding may contribute to staff responding with fear:

“Two staff members. . . talking about moving everything to Wi-Fi. They said, ‘Well gosh, now they’re gonna be getting onto the Internet, they’re gonna be hacking. . . and doing a bunch of identity theft’ . . . like they’re making this whole scenario about things that inmates are going to be doing on a secure platform. . . the staff’s ignorance about the technology is counter to the benefit of it.” —P5

C. Downstream Impacts

Finally, we consider the subsequent effects of the staff’s decisions to censor or block Alice’s message. These decisions, described by participants as often arbitrary and unpredictable, have profound downstream consequences that threaten core aspects of personal well-being: engendering self-doubt, eroding community ties, hindering rehabilitation, and feelings of resignation and powerlessness in the face of technology access.

Internalized Threats of Self. Participants shared that the system of censorship within prisons conveys a clear message: technology use by incarcerated people is inherently dangerous

and untrustworthy, necessitating surveillance. This narrative is further reinforced when officers can revoke technology access under the guise of mitigating security risks. P8 described how:

“I sent an email, but that email didn’t actually go somewhere; it goes to the mailroom. It goes to somebody else’s inbox, for them to look at it first. And for them to determine if they think it’s okay to be sent out. And so you don’t even have that kind of instant gratification of like, okay I sent that thing. You don’t even know if it goes, and that breeds that distrust. Both of self, because it’s like, okay, did I do that, right? And then of the tech, because it’s, ‘Okay, is the tech malfunctioning?’, and how will I know if it’s doing the right thing?” —P8

These fears became so internalized that they remained even after P8’s release:

“So when I was getting on the Internet and searching things when I first got out [of prison], I was like ‘Oh, should I do this?’ Like I just was instantly thinking, I’m self-monitoring. And I was really afraid to get on social media because what if I’m not allowed on here?” —P8

Other participants also reflected on self-censorship and how the incessant psychological double-think lingers:

“Landing here in my reintegration journey, there has been [psychological] overrides due to developmentally being arrested through incarceration. There’s. . . an override to show up, speak up, be seen, do these things, and this is part of the threat of us being censored from just being human.” —P2

P2 likened the “psychological trauma that’s being taken out on our bodies” to that of “treading water” and “drowning.” In P8’s words, censorship created “the panopticon. . . at its finest.”

Threats to Community. Surveillance and censorship of communication technologies inhibits participants from fostering their intimate, human relationships. P2 expressed that:

“Yeah, I would just highlight the censorship of like, I was married while I was inside. There’s a whole process to even get correspondence with my wife. And then, to speak about intimate things, our mail was rejected. And it’s like, I’m human, and I have a wife, and they stopped that.” —P2

According to P10, the prevailing expectation from Securus and DOC is that: “10 minutes is enough to build a relationship, right? But it’s not” (P10). The consequences if they chose not to use this technology, or if their access was restricted or revoked, was grave: “My body was being affected by how much anxiety and fear [I had] and [I was] so scared that my boys weren’t gonna remember me” (P10).

Surveillance and censorship further prohibited those seeking outside legal council or support. P5 voiced described how censorship prevented him from seeking the legal council he required, observing that his friend sent him “a picture from the. . . attorney general’s website of this year’s people who were

on the clemency list for 2024. They [prison officials] rejected it as third-party information.”

Threats to Rehabilitation. Participants expressed that the exposure to surveillance and censorship, in addition to arbitrary technology restrictions, leads to a lack of digital literacy within and beyond prisons. This does not adequately prepare them for the technological world once released [52], [53], [54].

This digital disadvantage is partially due to the loss of privacy and agency that system-impacted people experience since their life stories and their pasts are forever documented online, accessible to the public (echoing [33]). The fear of being discovered as formerly incarcerated relates to participants experiencing difficulties in using technologies once released. As P8 recounts, the lack of digital literacy created a feeling of “being outed” or “othered,” stating: “That was my reaction to almost everything: They’re gonna know that I was in prison because I don’t know how to do this.”

Participants also perceived that the surveillance and censorship continued, even post-release, to undermine efforts for peaceful reintegration. Echoing Owens et al.’s [55] findings on post-release electronic monitoring, P8 discussed the anxiety induced by post-release electronic monitoring applications:

“I have to submit an entire schedule, and I’m beholden to it. Where it will take me 10 minutes to get from here to here, and then 15 minutes to find parking, and then 30 minutes at a meeting, and then 45 minutes to get back home. ...and that is another way of surveilling, where that gets loaded into the computer... So all these invisible ways, again, that technology, we’re told that it’s for the betterment of our lives and that this will make things easier. And yet when we get surveilled by it, it’s used in this really punitive way.” —P8

The threat of surveillance and censorship leads participants to fear and second-guess their actions. It prevents them from adapting to technologies, since they perceive them as means to continue the cycle of surveillance and censorship experienced in prison. P8, for instance, explains how easy it was to be taken advantage of on social media since they had no prior experience with and were afraid of technology:

“I ended up getting trolled, really bad actually, on Facebook. So I don’t use Facebook anymore... One, I feel like I shouldn’t be doing this, and then it’s reinforced because the reaction I end up getting [is] like, ‘Oh, you did it wrong.’” —P8

This lack of access and fear of technology can thus deepen the digital divide for system-impacted people and make them more vulnerable to social isolation or even online scams.

Apathy and Resignation. The reluctant acceptance of technologies stems from a belief that it is unlikely that problems will be adequately fixed. Participants felt powerless in the face of persistent usability issues and appeals of censorship that offered them no resolution. P4, for instance, described the process they went through to address an issue, noting that:

“You find yourself back in this place where you’re completely defeated, you’ve found no recourse, nobody is accountable, it’s never anybody’s fault.” P10 was told their were unable to appeal the decision to revoke their communication with their family: “I sent complaints and everything. Then I found out that I couldn’t even appeal it.” P2 also felt that complaining or raising injustices inside the prison only left them feeling depressed, articulating that, for the incarcerated person: “If he stops too long to gripe... then he drowns.”

This feeling of powerlessness paradoxically left participants feeling grateful and appreciative for the same technologies that harm them, a phenomenon that P5 dubbed “technology Stockholm syndrome.” P4 explained:

“So, all of these hurdles, all of these things just to say if a phone call works well for a full 20 minutes, you just have to kinda consider yourself lucky... like you shouldn’t be grateful that somebody didn’t kick you after they knocked you down.”

With meager expectations, the smallest successes made them feel lucky to have access to anything at all. F1 elaborated, explaining that: “A lot of times I’ll be like, ‘Just be glad for what you get.’” P7 further contextualized how access to technology within prisons is often viewed as a substitute for educational opportunities. Additionally, they connected this access to broader issues of consumerism and technology addiction in the outside world:

“I don’t know that [technology access] prepared anyone specifically, it probably prepared them to be good consumers... I don’t know that it prepared me [for release] in the same way a school would.”

V. DISCUSSION

We now discuss two tensions that surfaced during our investigation, and recommendations for their mitigation, aimed at the research community, policymakers, prison officials, and prison technology vendors.

Although we make recommendations, we believe that no matter how usable, accessible, and modern the technology is inside of prisons, the carceral system is an inherently traumatizing force in U.S. society. We echo Owens et al. [56] vis-a-vis recommendations: “While we can offer design and policy recommendations to make communication easier and more privacy-preserving for [family members of incarcerated people] and their incarcerated relatives, the most effective solution is one that reduces the number of people who are subjected to carceral surveillance in the first place.”

A. Observed Tension: Harms from No Technology versus Harms from Technology

As explored extensively in prior work [61], [54], [67], [52], [62], [30], [4], system-impacted people face a significant uphill battle when adapting to a rapidly changing digital world. This is especially true if they have been incarcerated over the last three decades, as digital devices became necessary for navigating society. Many of our formerly incarcerated participants mentioned difficulties post-release interfacing with

technologies: from creating an e-mail address, to using QR codes at restaurants, to procuring housing or establishing bank accounts. Prior work explores how this lack of access to technologies is deepening the digital divide [54], [67], [62], [30]. Some recent papers [29], [51], [46] and non-profits [1], [76] aim to close this digital divide by co-designing and deploying digital tools for incarcerated people.

We extend this prior work to demonstrate that, while harms from a lack of access to technology exist, other harms from having exposure to technology emerge. Digital devices that system-impacted people can access lead them to experience surveillance and censorship, strain their community ties, and further threaten their rehabilitation. According to study participants, the tools become sites of power contestation and arbitrary and punitive bargaining chips by officers.

In sum, if a technology is introduced into prisons to support incarcerated people and close the digital divide, *we recommend it be accompanied by considerations of its socio-technical context, and in particular, how the (even well-intentioned) technology could be used in harmful ways.*

Recommendation: Free, open, digital and non-digital opportunities. As P7 expressed in Section IV-C, access to technology encouraged consumerism rather than providing meaningful preparation for release. They underlined that a formal education, like a school, would have better prepared them. Technology access was not a reprieve from consumerism, financial stress, coercive choice, or a replacement for real educational opportunity. We therefore recommend that *digital opportunities should be provided in addition to non-digital educational opportunities. Information should also be made available about the harms of technology*, from technology addiction and consumerism to privacy vulnerabilities, scams, phishing, and the like. Moreover, after release, system-impacted people remain under surveillance of their social media, location, browsing activity, and community ties [55], [50], [28], [60], [63], [83], [37]. Developing a stronger awareness of their security and privacy vulnerabilities can help them navigate these risks and support successful reentry.

We also believe *educational opportunities, notably threat modeling, could be beneficial for prison staff.* In Section IV-B, we note how participants often felt that prison officials held misconceptions about their potential use of technology. Yet, as noted in Section IV-B, staff are the ones responsible for enforcing its use. We believe education for prison officials could be useful to explore the capabilities and limitations of certain technologies, including dispelling common misconceptions about the misuse of technology inside prisons. Indeed, some prior work has shown that educating staff about technology can foster greater support and reduce the stigma for incarcerated people’s use of technology [21], [40], [3], [75].

Regarding pricing, prior work also highlighted the financial burden that technologies place on already struggling system-impacted families [22], [71], [18]. This is particularly concerning given that poverty is a predictor of incarceration, and also increasingly an outcome, in part due to such exploitative

pricing schemes [82], [22]. We believe that making this technology free and/or affordable is not an unrealistic expectation: the San Francisco Public Library recently adopted a new no-hidden-costs, completely free tablet program for all locally incarcerated people [69]; in September 2022, California joined Connecticut as the second state to make phone calls free in state prisons [16]; and in July 2024 the FCC approved new caps on prison phone call prices and banned some kickback schemes in response to the Martha Wright-Reed Just and Reasonable Communications Act of 2022 [10], [17], although President Trump revoked these bans/caps in 2025 [19].

B. Observed Tension: The Customer Is Not the End-User

Our interviews suggested that prison policies and regulations are subject to the whims of officers (Section IV-B) and that interviewees felt there was no accountability for or recourse to change usability problems and censorship (Section IV-C). Under the current incentive structure, prison officials enter into contracts with technology companies, making the companies accountable to the officials and staff, not to actual system end-users; end-users are the incarcerated people and their families, whom Owens et al. describe as “both literally and figuratively a captive audience” [56]. Our findings reveal how this arrangement intensifies censorship and financial burdens (e.g., having to pay to resend a message after it is censored), benefiting both the prison officials and the contracted technology companies but not end-users.

Recommendation: Transparency and accountability to the actual end-users. We previously noted how users are often not notified about whether their messages have been censored (Section IV-A). Though transparency regarding block-lists of words that trigger censorship could help reduce the financial burdens faced by incarcerated people (from not having to pay to resend messages), we recognize that this approach may not be desirable for prison staff due to concerns about circumventing censorship. Nevertheless, we believe that *incarcerated people should be told whether and why their messages were censored.* We also recommend *establishing clear guidelines for disallowed language* to ensure that prison officials’ decisions are not arbitrary. Furthermore, we call for more research to verify the claims of prison officials that censorship prevents illegal or otherwise harmful activity; *more research is needed to understand if the censorship accomplishes its claimed benefits, and does not just prevent system-impacted people from openly speaking with their loved ones and lawyers.*

Security experts have long argued that “security through obscurity” is a weak strategy [2], [47], [39], [38], [34]. In that vein, we recommend that both the aforementioned censorship guidelines, and *Privacy Impact Assessments (PIAs)* — which every U.S. federal agency must fill out regarding personal data collection and privacy — *be required for prisons and their contractors and made publicly available* [77]. We also recommend that these assessments extend beyond the scope of personal privacy, *including all potential harms and risks the technology may impose.* This could include financial and

social harms our participants described.

We further recommend that prison contracts with private companies be subject to a mandatory public comment period before a private company's bid is chosen. These contracts should incorporate input from system-impacted community members and be awarded in part based on robust research about the potential harms of the technology to its end-users.

Recommendation: Consider and audit more carefully the use of “security” and “safety” for the carceral institution as a justification to violate the security, privacy, and safety incarcerated people. Finally, we noted the repeated reference to “security” and “safety” threats to prisons when asking participants why they believed their own security, privacy, and safety were violated. These violations ranged from officials searching their belongings and messages, intense surveillance and restriction on device use, as well as coercion, competition from manufactured scarcity, and lack of autonomy over their personal information and documents. However, the underlying prison security concerns may not be founded in actual data about real threats, and moreover the implied threat model creates opportunities and excuses for abuses of power.

If prisons intend to reduce tension and violence inside their walls, we worry that such intense restriction, power contestation, and competition over the very technology that connects people to their support systems is not helpful. Such frustration, isolation, lack of autonomy, and scarcity could, in fact, be detrimental to the prison's stated goals of maintaining a peaceful environment, as we discussed in Section IV-B.

In sum, we believe that work is needed to address the privacy, security, usability, and financial issues stemming from technology available to incarcerated people, and we believe that this work can take many achievable forms: including educational reforms, consumer protection safeguards, policy implementations, technical solutions, bug fixes, and more.

VI. CONCLUSION

To explore the security, privacy, and associated impacts of technology inside the carceral system, we conducted focus groups and interviews with 17 formerly incarcerated people and relatives. Our findings show that participants experience pervasive forms of surveillance and censorship related to the available technologies. They describe shifting and arbitrary technology censorship policies that strain their relationships with their communities and threaten their future rehabilitation; these challenges exacerbated feelings of dehumanization, self-doubt, and mistrust towards technology. We end by recommending ways to modify these technologies and policies to better serve incarcerated people and their loved ones, and thereby ultimately for society as a whole.

ACKNOWLEDGEMENTS

The authors would like to thank all of our user study participants, and members of the UW Security and Privacy Lab who gave feedback on earlier versions of the paper. This work was supported in part by the U.S. National Science Foundation under Award #2205171.

REFERENCES

- [1] Ameelio. Ameelio. <https://www.ameelio.org/>.
- [2] R. Anderson. Why cryptosystems fail. In *ACM Conference on Computer and Communications Security*, 1993.
- [3] D. Antojado and N. Ryan. The future of prison visits? An autoethnographic perspective on the developments of the digitisation of prison visits during COVID-19. *Journal of Criminology*, 2024.
- [4] O. Anuyah, K. Badillo-Urquiola, and R. Metoyer. Characterizing the technology needs of vulnerable populations for participation in research and design by adopting Maslow's hierarchy of needs. In *CHI Conf. on Human Factors in Computing Systems*, 2023.
- [5] P. Arguelles and I. Ortiz-Luis. Bars behind bars: Digital technology in the prison system. *SSRN Electronic Journal*, 2021.
- [6] A. Asher-Schapiro and D. Sherfinski. AI surveillance Takes U.S. Prisons by Storm, 2021. <https://www.context.news/surveillance/ai-surveillance-takes-us-prisons-by-storm>.
- [7] C. Barabas, C. Doyle, J. Rubinovitz, and K. Dinakar. Studying up: reorienting the study of algorithmic fairness around issues of power. In *Conf. on Fairness, Accountability, and Transparency*, 2020.
- [8] R. Bellini, E. Tseng, N. Warford, A. Daffalla, T. Matthews, S. Consolvo, J. Woelfer, P. Kelley, M. Mazurek, D. Cuomo, N. Dell, and T. Ristenpart. Sok: Safer digital-safety research involving at-risk users. In *IEEE Symposium on Security & Privacy*, 2024.
- [9] W. Bertram. The law is supposed to protect consumers from exploitation, but it's not protecting people in prisons and jails. *Prison Policy Initiative*, 2019. <https://www.prisonpolicy.org/blog/2019/11/14/consumerlaw/>.
- [10] W. Bertram. FCC votes to slash prison and jail calling rates and ban corporate kickbacks. *Prison Policy Initiative*, 2024. <https://www.prisonpolicy.org/blog/2024/07/18/fcc-vote/>.
- [11] W. Bertram and P. Wagner. State of phone justice 2022: The problem, the progress, and what's next. *Prison Policy Initiative*, 2022. https://www.prisonpolicy.org/phones/state_of_phone_justice_2022.html.
- [12] P. Biernacki and D. Waldorf. Snowball sampling: Problems and techniques of chain referral sampling. *Sociological methods & research*, 10(2):141–163, 1981.
- [13] V. Braun and V. Clarke. Using thematic analysis in Psychology. *Qualitative research in psychology*, 3(2):77–101, 2006.
- [14] K. Butler, K. Hugenberg, A. K. Eakta Jain, T. Kohno, E. M. Redmiles, F. Roesner, M. Sim, P. Traynor, and H. Barakat. Extending the Heilmeier Catechism to Evaluate Security & Privacy Systems: Who is Left Out? *IEEE Security & Privacy Magazine*, 2025.
- [15] W. C. Galloway. Use of technology in the corrections field. <https://www.fdle.state.fl.us/FCJEI/Programs/SLP/Documents/Full-Text/Galloway,-William-final.aspx>.
- [16] California Department of Corrections and Rehabilitation, Family & Friends Services. Tablets and Telephones. *California Department of Corrections and Rehabilitation*, 2024. <https://www.cdcr.ca.gov/family-resources/tablets/>.
- [17] Congress.gov. Martha Wright-Reed Just and Reasonable Communications Act of 2022, 2022. <https://www.congress.gov/bill/117th-congress/senate-bill/1541/text>.
- [18] H. Cortina. “I Want to Do More than Sit in that Cell and Wait to Die” *The Modernized Pains of Tablets in Prison*. Univ. of Delaware Dissertation, 2022.
- [19] R. Crosby and N. Sims. Trump's FCC scraps ban on prison phone price gouging, a gift to some of his big donors. *Mother Jones*, 2025. <https://www.motherjones.com/politics/2025/07/trumps-fcc-scraps-ban-on-prison-phone-price-gouging-a-gift-to-some-of-his-top-donors/>.
- [20] S. Czifra, A. Galindo, J. Mason, C. Ricks, A. Zohrabi, et al. Analyzing reentry services for formerly incarcerated californians in higher education. *The Urban Institute*, 2022. https://www.urban.org/sites/default/files/2022-03/analyzing-the-landscape-of-reentry-services-for-formerly-incarcerated-californians-in-higher-education_0.pdf.
- [21] G. Davies, J. Ward, S. Elison, S. Weston, S. Dugdale, and J. Weekes. Implementation and evaluation of the Breaking Free Online and Pillars of Recovery treatment programs for substance-involved offenders. *Advancing Corrections*, 3:95–113, 2017.
- [22] S. deVuono Powell, C. Schweidler, A. Walters, and A. Zohrabi. Who pays? the true cost of incarceration on families. *Ella Baker Center, Forward Together, Research Action Design*. Accessed July, 23(2021):221–43, 2015.

- [23] T. Ertl, S. Taugerbeck, M. Esau, K. Aal, P. Tolmie, and V. Wulf. The social mile: How (psychosocial) ICT can help to promote resocialization and to overcome prison. *ACM Proceedings on Human-Computer Interaction (GROUP)*, 2019.
- [24] D. Floberg and M. McDermott. The slow death of a prison profiteer: How activism brought securus to the brink. *The Appeal*, 2024. <https://theappeal.org/securus-bankruptcy-prison-telecom-industry/>.
- [25] M. Foucault. *Discipline and Punish: The birth of the prison*. Vintage Books, 1979.
- [26] D. Freed, J. Palmer, D. Minchala, K. Levy, T. Ristenpart, and N. Dell. “A Stalker’s Paradise”: How Intimate Partner Abusers Exploit Technology. In *CHI Conference on Human Factors in Computing Systems*, 2018.
- [27] H. Fry. O.C. supervisors extend contract with vendor at center of scandal over jailhouse recordings. *LA Times*, 2018. <https://www.latimes.com/local/lanow/la-me-ln-gtl-contract-extension-20181107-story.html>.
- [28] S. Fussell. Apps are now putting the parole agent in your pocket, 2020. <https://www.wired.com/story/apps-putting-parole-agent-your-pocket/>.
- [29] A. Gautam, K. Gandhi, and J. Sendejo. Enhancing reentry support programs through digital literacy integration. In *ACM Designing Interactive Systems Conference*, 2024.
- [30] M. Grierson, D. Varghese, M. Bolton, and P. Olivier. Design considerations for a digital service to support prison leavers. In *ACM Designing Interactive Systems Conference*, 2022.
- [31] A. Gross. Washington experiments with giving women in prison limited access to the internet. *NPR KNKX*, 2019. <https://www.knkx.org/youth-education/2019-12-16/washington-experiments-with-giving-women-in-prison-limited-access-to-the-internet>.
- [32] T. Guberek, A. McDonald, S. Simioni, A. H. Mhaidli, K. Toyama, and F. Schaub. Keeping a Low Profile? Technology, Risk and Privacy among Undocumented Immigrants. In *CHI Conference on Human Factors in Computing Systems*, 2018.
- [33] S. Gurusami. The carceral web we weave: Carceral citizens’ experiences of digital punishment and solidarity. *Punishment & Society*, 21(4), 2019.
- [34] P. Hall, O. Mundahl, and S. Park. The pitfalls of “security by obscurity” and what they mean for transparent AI. In *Proceedings of the Thirty-Ninth AAAI Conference on Artificial Intelligence and Thirty-Seventh Conference on Innovative Applications of Artificial Intelligence and Fifteenth Symposium on Educational Advances in Artificial Intelligence*, AAAI’25/IAAI’25/EAAI’25. AAAI Press, 2025. <https://doi.org/10.1609/aaai.v39i27.35022>.
- [35] C. Jameson. The “Short Step” from Love to Hypnosis: A Reconsideration of the Stockholm Syndrome. *Journal for Cultural Research*, 14(4):337–355, 2010.
- [36] Joe Russo, Michael J. D. Vermeer, Dulani Woods, Brian A. Jackson. Leveraging technology to support prisoner reentry. *RAND*, 2022. https://www.rand.org/pubs/research_reports/RRA108-12.html.
- [37] Just Future Project. Big Brother on the App Store, 2025. <https://ajustfuture.org/wp-content/uploads/2025/05/Smartphone-Surveillance-and-Sex-Offender-Exceptionalism.pdf>.
- [38] J. Katz and Y. Lindell. *Introduction to modern cryptography: principles and protocols*. Chapman and Hall/CRC, 2007.
- [39] A. Kerckhoffs. La cryptographie militaire. *Journal des Sciences Militaires*, 9, 1883. https://www.petitcolas.net/kerckhoffs/crypto_militaire_1.pdf.
- [40] V. Knight, S. Ross, and M. Wood. Digitalising corrections. *Journal of Criminology*, 57(3):263–274, 2024.
- [41] J. Koebler. A clear plastic tablet for prisoners: The motherboard review. *VICE*, 2024. <https://www.vice.com/en/article/a-clear-plastic-tablet-for-prisoners-the-motherboard-review/>.
- [42] M. Lee and J. Smith. Hack of 70 million prisoner phone calls indicates violations of attorney-client privilege. *The Intercept*, 2015. <https://theintercept.com/2015/11/11/securus-hack-prison-phone-company-exposes-thousands-of-calls-lawyers-and-clients/>.
- [43] A. E. Lerman and J. Page. The state of the job: An embedded work role perspective on prison officer attitudes. *Punishment & Society*, 14(5), 2012.
- [44] C. A. Liang, S. A. Munson, and J. A. Kientz. Embracing Four Tensions in Human-Computer Interaction Research with Marginalized People. *ACM Trans. Comput.-Hum. Interact.*, apr 2021.
- [45] A. Littman. Free-world law behind bars. *Yale Law Journal*, 131, 2022.
- [46] R. Martinez and K. Squire. Engaging recently incarcerated and gang affiliated black and latino/a young adults in designing social collocated applications for mixed reality smart glasses through community-based participatory design workshops. In *Proceedings of the CHI Conference on Human Factors in Computing Systems*, pages 1–17, 2024.
- [47] R. T. Mercuri and P. G. Neumann. Security by obscurity. *Communications of the ACM*, 46(11), Nov. 2003.
- [48] A. Mufarreh, J. Waitkus, and T. A. Booker. Prison official perceptions of technology in prison. *Punishment & Society*, 24(3), 2022.
- [49] National Institute of Justice. New initiatives in correctional technology, 1996. <https://nij.ojp.gov/library/publications/new-initiatives-correctional-technology-final-report>.
- [50] National Reentry Resource Center and the American Probation and Parole Association. Social media in community supervision: Promising practices for policy and implementation, 2020. <https://csgjusticecenter.org/events/social-media-in-community-supervision-promising-practices-for-policy-and-implementation/>.
- [51] M. Nisser, M. Gaetz, A. Fishberg, R. N. Soicher, F. Faruqi, and J. Long. From prisons to programming: Fostering self-efficacy via virtual web design curricula in prisons and jails. In *Proceedings of the CHI Conference on Human Factors in Computing Systems*, pages 1–13, 2024.
- [52] I. F. Ogbonnaya-Ogburu and A. Israni. Supporting the digital aspects of reentry for formerly incarcerated individuals. In *Extended Abstracts of the CHI Conference on Human Factors in Computing Systems*, 2024.
- [53] I. F. Ogbonnaya-Ogburu, K. Toyama, and T. Dillahunt. Returning citizens’ job search and technology use: Preliminary findings. In *Companion of the ACM Conf. on Computer Supported Cooperative Work and Social Computing*, 2018.
- [54] I. F. Ogbonnaya-Ogburu, K. Toyama, and T. R. Dillahunt. Towards an effective digital literacy intervention to assist returning citizens with job search. In *CHI Conf. on Human Factors in Computing Systems*, 2019.
- [55] K. Owens, A. Alem, F. Roesner, and T. Kohno. Electronic monitoring smartphone apps: An analysis of risks from technical, Human-Centered, and legal perspectives. In *USENIX Security Symposium*, 2022.
- [56] K. Owens, C. Cobb, and L. Cranor. “You Gotta Watch What You Say”: Surveillance of communication with incarcerated people. In *CHI Conference on Human Factors in Computing Systems*, 2021.
- [57] K. Owens, Y. Eiger, B. Radka, T. Kohno, and F. Roesner. Understanding experiences with compulsory immigration surveillance in the U.S. In *ACM Conference on Fairness, Accountability, and Transparency*, 2025.
- [58] S. Pollack. Focus-group methodology in research with incarcerated women: Race, power, and collective experience. *Affilia*, 18(4), 2003.
- [59] K. E. Race, D. F. Hotch, and T. Packer. Rehabilitation program evaluation: use of focus groups to empower clients. *Evaluation review*, 18(6):730–740, 1994.
- [60] J. Redden, J. Camello, M. Mecray, M. Osbourne, M. Planty, and J. Russo. Monitoring Technologies for Community Supervision. *U.S. Dept of Justice, Office of Justice Programs*, 2023. <https://www.ojp.gov/library/publications/monitoring-technologies-community-supervision>.
- [61] B. Reisdorf, J. DeCook, M. Foster, J. Cobbina, and A. LaCourse. Digital reentry: uses of and barriers to ICTs in the prisoner reentry process. *Information, Communication & Society*, 25(14):2028–2045, 2022.
- [62] B. Reisdorf and R. Rikard. Digital rehabilitation: A model of reentry into the digital age. *American Behavioral Scientist*, 62(9), 2018.
- [63] J. Russo, M. J. D. Vermeer, D. Woods, and B. A. Jackson. Community Supervision in a Digital World Challenges and Opportunities. *RAND*, 2021. https://www.rand.org/pubs/research_reports/RRA108-10.html.
- [64] G. R. Sadler, H.-C. Lee, R. S.-H. Lim, and J. Fullerton. Research article: Recruitment of hard-to-reach population subgroups via adaptations of the snowball sampling strategy. *Nursing & Health Sciences*, 12(3), 2010.
- [65] Securus. About Us. <https://securustech.net/about-us/index.html>.
- [66] SecurusTechnologies. Securus Technologies, Inc. Completes Transaction to Acquire JPay Inc. . *PR Newswire*, July 2015. <https://www.prnewswire.com/news-releases/securus-technologies-inc-completes-transaction-to-acquire-jpay-inc-300122095.html>.
- [67] H. Seo, H. Britton, M. Ramaswamy, D. Altschwager, M. Blomberg, S. Aromona, B. Schuster, E. Booton, M. Ault, and J. Wickliffe. Returning to the digital world: Digital technology use and privacy management of women transitioning from incarceration. *New Media & Society*, 24(3):641–666, 2022.
- [68] H. Seo, J. Erba, D. Altschwager, and M. Geana. Evidence-based digital literacy class for older, low-income African-American adults. *Journal of Applied Communication Research*, 2019.

- [69] SF Public Library. People over profits: A truly free, no cost tablet program for incarcerated people in San Francisco, 2023. <https://sfgov.org/financialjustice/reports/people-over-profits-truly-free-no-cost-tablet-program-incarcerated-people-san-francisco>.
- [70] J. Smith. Securus settles lawsuit alleging improper recording of privileged inmate calls. *The Intercept*, 2016. <https://theintercept.com/2016/03/16/securus-settles-lawsuit-alleging-improper-recording-of-privileged>.
- [71] N. L. Sobol. Connecting the disconnected communication technologies for the incarcerated. *Wake Forest L. Rev.*, 53:559, 2018.
- [72] V. Surret, A. Corona, E. Weill-Greenberg, R. Samuels, and L. Bonds. The high costs of free prison tablet programs. *The Appeal*, 2024. <https://theappeal.org/the-high-costs-of-free-prison-tablet-programs-books-through-bars/>.
- [73] The Prisoners Computer User Group. "Computing Behind Bars: The Washington State Reformatory Experience: A Three Year Report" prepared by The Prisoners Computer User Group, 1989. <https://cdm16786.contentdm.oclc.org/digital/collection/p16786coll15/id/1406/rec/2>.
- [74] D. R. Thomas. A general inductive approach for analyzing qualitative evaluation data. *American journal of evaluation*, 27(2):237–246, 2006.
- [75] United Nations Interregional Crime and Justice Research Institute (UNICRI). Digital rehabilitation in prisons, 2024. <https://unicri.it/Publication-Digital-Rehabilitation-Prisons>.
- [76] Unlocked Labs. Unlocked labs. <https://unlockedlabs.org/story>.
- [77] U.S. Department of Health and Human Services. Privacy Impact Assessments, 2024. <https://www.hhs.gov/pia/index.html>.
- [78] C. Vachiradath. The efficacy of technology in preventing the escape of inmates in prison. *Journal of Applied Security Research*, 8(4), 2013.
- [79] J. Valentino-Devries. Service meant to monitor inmates' calls could track you, too. *New York Times*, 2018. <https://www.nytimes.com/2018/05/10/technology/cellphone-tracking-law-enforcement.html>.
- [80] S. Verbaan, C. Aldington, R. McNaney, and J. Wallace. Potentials of HCI for prisons and incarcerated individuals. In *Extended Abstracts of the CHI Conf. on Human Factors in Computing Sys.*, 2018.
- [81] ViaPath. About ViaPath - ViaPath. <https://www.viapath.com/about/>.
- [82] W. S. Wagner and Peter. Mass incarceration: The whole pie 2024. *Prison Policy Initiative*, 2024. <https://www.prisonpolicy.org/reports/pie2024.html>.
- [83] Washington State Department of Corrections. Social media and electronic device monitoring for supervision, 2022. <https://www.doc.wa.gov/information/policies/showFile.aspx?name=380260>.
- [84] M. Wei, J. Mink, Y. Eiger, T. Kohno, E. M. Redmiles, and F. Roesner. SoK (or SoLK?): on the quantitative study of sociodemographic factors and computer security behaviors. In *USENIX Security*, 2024.
- [85] E. Weill-Greenberg, C. Ballesteros, and M. O'Connor. Michigan counties ban jail visits to profit from videochat fees, lawsuits say. *The Appeal*, 2024. <https://theappeal.org/michigan-counties-allegedly-ban-jail-visits-to-profit-from-videochat-fees/>.
- [86] M. Wessler. SMH: The rapid and unregulated growth of e-messaging in prisons. *Prison Policy Initiative*, 2023. <https://www.prisonpolicy.org/reports/emessaging.html>.
- [87] C. West. We surveyed people in prison about how they use technology. their answers paint a glitchy future. *Slate*, Sep 2023. <https://slate.com/technology/2023/09/prison-tech-survey-viapath-securus.html>.
- [88] C. West. Why WA pulled secure laptops from 1,200 incarcerated students. *Seattle Times*, 2024. <https://www.seattletimes.com/seattle-news/law-justice/why-wa-officials-pulled-secure-laptops-from-1200-incarcerated-people/>.
- [89] L. Wiehl. The Law; Inmates Sue to End Ban on Computers in Cells. *The New York Times*, 1989. <https://www.nytimes.com/1989/08/18/us/the-law-inmates-sue-to-end-ban-on-computers-in-cells.html>.
- [90] P. Wright. Washington prisoners lose computers, again. *Prison Legal News*, 1996. <https://www.prisonlegalnews.org/news/1996/dec/15/washington-prisoners-lose-computers-again/>.