"You Gotta Watch What You Say": Surveillance of Communication with Incarcerated People

Kentrell Owens*
kentrelo@alumni.cmu.edu
Carnegie Mellon University
Pittsburgh, PA, U.S.A.

Camille Cobb
ccobb@andrew.cmu.edu
Carnegie Mellon University
Pittsburgh, PA, U.S.A.

Lorrie Faith Cranor
lorrie@cmu.edu
Carnegie Mellon University
Pittsburgh, PA, U.S.A.

ABSTRACT

Surveillance of communication between incarcerated and non-incarcerated people has steadily increased, enabled partly by technological advancements. Third-party vendors control communication tools for most U.S. prisons and jails and offer surveillance capabilities beyond what individual facilities could realistically implement. Frequent communication with family improves mental health and post-carceral outcomes for incarcerated people, but does discomfort about surveillance affect how their relatives communicate with them? To explore this and the understanding, attitudes, and reactions to surveillance, we conducted 16 semi-structured interviews with participants who have incarcerated relatives. Among other findings, we learn that participants communicate despite privacy concerns that they felt helpless to address. We also observe inaccuracies in participants' beliefs about surveillance practices. We discuss implications of inaccurate understandings of surveillance, misaligned incentives between end-users and vendors, how our findings enhance ongoing conversations about carceral justice, and recommendations for more privacy-sensitive communication tools.

CCS CONCEPTS

• **Security and privacy → Usability in security and privacy**; **Social aspects of security and privacy**.

KEYWORDS

surveillance, privacy, prison, communication, ICT

ACM Reference Format:
Kentrell Owens, Camille Cobb, and Lorrie Faith Cranor. 2021. "You Gotta Watch What You Say": Surveillance of Communication with Incarcerated People. In *CHI Conference on Human Factors in Computing Systems(CHI '21), May 8–13, 2021, Yokohama,Japan.* ACM, New York, NY, USA, 18 pages. https://doi.org/10.1145/3411764.3445055

*Currently at the University of Washington. This research was conducted while the first author was a student at Carnegie Mellon University.

CHI '21, May 8–13, 2021, Yokohama, Japan

ACM ISBN 978-1-4503-8096-6/21/05.
https://doi.org/10.1145/3411764.3445055

1 INTRODUCTION

The United States (U.S.) has the highest incarceration rate and the largest population of incarcerated people[1] in the world [107]. Nearly half (45 percent) of adults in the U.S. (113 million people nationwide) have an immediate family member who has spent at least one night in jail or prison [28]. About 1 in 7 adults has a close family member — defined as a parent, child, sibling, partner or a spouse — who was imprisoned for at least one year [28].

Incarcerated people in the United States are under near-constant surveillance, particularly when communicating with people who are *not* incarcerated. Attorney-client communication is privileged and has some legal protections from surveillance [2], but other communication does not. Communication to and from incarcerated people is scanned, indexed, and screened by prison officials or third-party contractors (prison communication companies) who provide communication services [19, 42, 90]. Although individual facilities may not be equipped to leverage cutting-edge advancements in computing, the increasing prevalence of prison communication companies has created an economy of scale for surveillance [7]. Recently, prison communication companies have integrated artificial intelligence into their systems to automate analysis of communication data, creating a detailed level of surveillance that was previously impractical [14, 30].

Advocates of prison communication monitoring argue that these forms of surveillance are necessary to combat future criminal activity and keep incarcerated people safe [30, 87, 89]; however, this surveillance has been shown to limit incarcerated people's willingness to report misconduct by prison staff [78]. For example, in January 2020 an incarcerated man was placed in solitary confinement for two weeks after he wrote a letter to the state governor through the prison's email system complaining about conditions in the prison [27]. Furthermore, since 74% of people held by jails have not been convicted of a crime and may be incarcerated only because they cannot afford bail [83], some legal scholars argue that they should not be subjected to the same level of surveillance as convicted individuals [87].

Because of inequities in the U.S. criminal legal system, prison communication surveillance disproportionately impacts people of color and their family members who communicate with them [83]. For example, Pennsylvania (PA) has a higher incarceration rate than the national average, and Black Americans comprise 46% of the incarcerated population but only 11% of the state population [40].

[1]The U.S. incarcerates 698 people per 100,000 and has approximately 2.3 million incarcerated people. The next highest country is China, with approximately 1.6 million.

Family members of incarcerated people (FMIP) face surveillance mechanisms similar to their incarcerated relatives when communicating with them. FMIP have to make a decision: consent to surveillance and stay in touch with loved-ones, or do not communicate with them at all. This choice is not only unfair and potentially harmful to non-incarcerated individuals (e.g., due to *chilling effects* [51, 69]), but it may also have negative societal impacts. Research has shown that recidivism is reduced when people in prison communicate frequently with their relatives [67]; thus, policies that *encourage* rather than discourage communication with incarcerated people have the potential to help reduce recidivism.

In this paper, we present the results of semi-structured interviews with adults in the Pittsburgh area (N = 16) with relatives currently incarcerated in county and state prisons/jails in PA. Our study was designed to answer the following research questions:

- In what ways do FMIP's mental models (or expectations) of surveillance align (or not) with actual surveillance practices of prisons or prison communication companies?
- What privacy concerns and preferences do FMIP have when they use prison communication services?
- How do FMIP cope with having limited privacy? What concessions do they make? What mitigation strategies do they use to protect their personal information?

We report participants' awareness of different surveillance mechanisms, their attitudes about surveillance, and their privacy-preserving strategies. We also present recommendations that we solicited from participants and add our own recommendations to policy makers and prison communication companies to improve the privacy of FMIP's communication with their incarcerated relatives.

Participants anticipated that surveillance would occur when they communicated with their incarcerated relatives, but their understanding of more technologically-advanced surveillance mechanisms was limited. They believed that there were legal, practical, and technical barriers that limited the amount of surveillance they could experience (although as we show these barriers are either non-existent or have little impact). Moreover, they believed that even if a carceral facility (e.g., a prison or jail) is transparent about its surveillance policies, there is no way for them to ensure that staff at that facility do not step outside the bounds of those polices.

Our findings highlight the unique privacy concerns of FMIP—a population that is vulnerable in multiple ways—and serve as a motivator for HCI and security/privacy researchers to investigate privacy challenges in the domain of prisons and jails. We believe these findings will help institutions better balance with the tension between privacy and institutional security that exists around incarceration and society more broadly.

2 BACKGROUND

The concept of a "panopticon" prison — designed so that the guard is not visible from the cells but can see into all cells — emerged in the late 18th century [84]. The aim was to encourage incarcerated people to always behave "appropriately" because they never know whether they were being watched [53]. Although the physical architecture of a panopticon has not seen widespread adoption, it has been used as a metaphor for modern surveillance systems [49, 79, 108]. Our focus is on surveillance of communication, but surveillance of incarcerated people extends to many other aspects of incarcerated peoples' experiences. This section presents background information about surveillance practices for common prison communication methods and discusses relevant prior work.

2.1 Prison communication landscape

Non-incarcerated people can keep in touch with incarcerated individuals via phone calls, electronic messaging, video visitation, in-person visitation, or physical letters. Not all facilities offer all five choices, and the financial cost of each option may limit a person's ability to choose their preferred communication method. Although there are also well-documented instances of private communication devices such as mobile phones being used by incarcerated people [38, 77], these are outside of the scope of our study.

The prison communication market in the US is loosely regulated and has seen significant consolidation in the past 30 years [106]. Together, two private companies — Global Tel Link Technologies (GTL) and Securus Technologies (Securus) — control about 83% of the prison phone market [10]. These companies are largely responsible for the introduction of new forms of communication and have also leveraged advancements in computation to implement more sophisticated surveillance capabilities, such as automated analysis of communication data. For example, electronic forms of communication (i.e., electronic messaging and video visitation) were introduced to many facilities in the 2010s with the promise of more convenient communication for FMIP [73]. The scope and scale of these contracts increase prisons' dependence on the service provider and enable consolidation of data from different communication methods. GTL touts a tool it offers that "enables investigators to consolidate data from multiple sources, including inmate telephone calls, jail management system data, financial transactions and payment deposits, and video visitation sessions" [95].

GTL and Securus both note in their privacy policies that may share data they collect with prison staff or law enforcement [19, 96]. These companies and facilities have policies in place for prison staff to follow, but the actions of individuals may differ from the stated policies. For example, in 2000, a correctional officer ("CO") in Delaware read the contents of an incarcerated person's mail over the prison's intercom system and prevented him from calling his attorney in retaliation for his filing a formal complaint about conditions affecting his physical well-being [78].

2.2 Prison communication surveillance practices

We next summarize typical experiences with phone calls, physical mail, in-person visitation, video visitation, and electronic messaging. We consolidate information about specific surveillance capabilities for each communication method, as described in publicly available policies, contracts, and news reports. Although our descriptions are general, they are predominantly informed by policies of specific facilities in PA. We also found that detailed information about surveillance practices was often unavailable; thus, there may be additional or different surveillance practices at other facilities or that we were unable to discover.

Phone calls. Phone calls are the most common way incarcerated people communicate with non-incarcerated people [106]. In general,

phone calls must be placed as outgoing calls from facilities. Upon receiving a call from an incarcerated person, a pre-recorded message specifies which facility the call originated from and who is calling, and reminds the recipient that the phone call will be monitored. Periodically, conversations are interrupted with a similar message, reminding both parties that the call is monitored or specifying how long they may keep talking. Some facilities allow incarcerated people to place phone calls to most numbers, while others require them to maintain pre-approved lists of people they may call. Call recipients may be required to provide identifying information (in addition to financial data collected to pay for calls). For example, Texas state facilities require call recipients to submit a photocopy of their driver's license or state ID; the name on this ID must match the name on the listing for the landline in a telephone directory, or to receive calls on a mobile phone, they must submit a copy of their phone bill as proof that the phone number belongs to them [100]. Reports show that Securus has also used voices as biometric data to identify call recipients [42].

Phone calls can be monitored in real time, recorded, and/or transcribed [95, 96]. GTL and Securus index phone content and make it searchable for police and prison officials [94–96]. They also flag certain slang terms to prompt additional manual scrutiny [95, 101]. Phone recordings can be given to law enforcement and district attorneys and used as evidence to strengthen a case against someone who is incarcerated pre-trial or to bring additional charges against someone who has already been sentenced [6, 23, 80].

In addition to identifying call recipients and monitoring the contents of communication, surveillance of phone calls includes monitoring people's behavior and communication patterns. In some facilities, call forwarding, three-way calling, or speakerphone are prohibited because they could allow unapproved people to communicate with the incarcerated person. Communication companies monitor for violations (e.g., use of three-way calling), and they may disconnect the call or restrict future phone use if a violation is detected [93, 101]. Both GTL and Securus obtain the location of non-incarcerated people via their wireless carrier if they answer calls on a mobile phone [19, 58, 96]. GTL records location for one hour after a phone call is accepted and retains this data for one year. Securus has previously provided location data to the police without a warrant [45]. Both GTL and Securus track who calls what phone numbers and visualize communication networks [95, 101].

Physical mail. Mail at facilities is typically limited to personal letters, publications, and legal mail (i.e., between an incarcerated person and their attorney). Outgoing and incoming letters can be opened, read, scanned, and/or photocopied [21, 59]. Legal mail is legally protected from surveillance, but at many facilities staff still open it to check for contraband [25]. Although policies vary, the type and forms of mail that can be received are heavily restricted, and mail that does not comply is returned or discarded [55]. For example, restrictions might include: envelopes without the sender's full name, letters with stickers or crayon drawings (e.g., those that might be included by the children of incarcerated people), handwritten letters that use an unauthorized pen color, and books or magazines not sent directly from the publisher [21, 59, 81]. In some cases, mail must be sent as a postcard [21, 59, 81].

Federal and county facilities typically process mail internally [21, 62]. For example, at Allegheny County Jail in PA, a correctional officer photocopies incoming mail and delivers copies to recipients [21]. The original is retained for 30 days and then destroyed. Letters sent to people incarcerated at state prisons in PA must first be mailed to a private company in Florida: Smart Communication Holding, Inc. According to its contract with the PA Department of Corrections (DOC), Smart Communications Holding, Inc. offers "services and systems that allow the DOC to monitor and archive" the mail of incarcerated people electronically [18].

In recent work examining how carceral facilities use technology to surveil mail, Austin used the Wayback Machine [4] to analyze how mail policies at federal, state, and county facilities in the U.S. have changed over time. They and found that just a few companies have consolidated control of communication surveillance technology and that as facilities change their communication policies to reduce access to mail, they also increase the digitization of mail and, consequently, digital surveillance [7].

In-person visitation. Most facilities offer in-person visitation, with a pre-approved list of visitors. These visits may be "contact" visits (i.e., FMIP are physically near the incarcerated person) or "no contact" visits (i.e., talking through a glass barrier on a facility-provided phone). In-person visitation can be challenging for FMIP since travelling to a facility can be costly and time-consuming; around 63% of incarcerated people in state prisons are over 100 miles away from their families [71].

Visitors, including children, must provide identification (e.g., birth certificates can be used as identification for children). Upon arrival at a facility, visitors' vehicles may be searched, and they may have to go through additional procedures, e.g., walking through a metal detector, having their hands scanned for drug residue, etc. Typically, visitors must adhere to policies such as dress codes, restrictions on what they may bring into a facility (e.g., outside food or mobile phones), or not talking to other visitors or incarcerated people besides the person they are visiting [61]. During visits, COs are physically present to observe visitors, and prison staff also remotely monitor visits through live camera footage [20, 61].

Video visitation. Many facilities offer "video visitation" in addition to or in lieu of in-person visitation. Newer contracts with communication companies sometimes require that facilities remove the option of in-person visitation to encourage FMIP to use their video platform (which, unlike in-person visitation, is typically not free) [72]. Video visits must be scheduled in advance, and visitors must be pre-approved. To register for a video visitation account, prospective visitors typically must use a webcam to take a photo of their identification [99].

At some facilities, personal computers or mobile phones can be used by FMIP for video visitation. Many facilities require that visitors go to a state prison or an approved alternative site to use video visitation. Nevertheless, video may be more feasible than in-person visitation when incarcerated people are geographically distant from visitors. Incarcerated people use a terminal in a shared space equipped with a camera, screen, and phone [72]. The PA DOC has implemented temporary policy changes in light of COVID-19; they now allow video visitation via mobile phone or computer from anywhere, through a popular video conferencing application [60].

Audio from video calls is handled similarly to audio from phone calls, but the visual content undergoes additional analysis [19, 96].

Video calls can be monitored live, recorded, and saved [97]. Securus indexes phone and video content and makes it searchable for police and prison officials. Securus' interface allows COs to view a "slideshow" of active video visitation sessions [98]. This live view lets facilities enforce conduct and attire policies similar to those used during in-person visitation.

Electronic messaging. Incarcerated people can receive electronic messages or "email" on personal tablets. Messages are downloaded by docking the tablets at a shared kiosk or on a wireless intranet (i.e., not connected to the Internet directly). Non-incarcerated people typically use a browser or mobile application to send and receive electronic messages. State prisons in PA offer electronic messaging through the PA DOC's contract with GTL [91, 92].

Unlike typical email, electronic messages sent to incarcerated people are typically paid for individually and allow only a limited number of characters per message. Messages are screened and sometimes automatically rejected. Electronic messaging systems at different facilities vary in terms of whether they allow photos to be sent in addition to the text messages. Photographs may undergo more scrutiny and must be approved manually before the incarcerated person can receive them [46, 73, 74, 92].

2.3 Impacts of surveillance

Prior work and real-world events have increased awareness of the negative impacts of surveillance, both in prisons specifically and in the world more generally. Marx [52] and Browne [12] give thorough overviews of existing surveillance practices and impacts.

2.3.1 Harms of prison communication surveillance. Retaliation by prison officials against incarcerated people who file grievances is a systemic problem [78]. A survey of people incarcerated in Ohio revealed that 70% of those who brought grievances against guards suffered retaliation, and 92% of all incarcerated people *believed* that they would face retaliation if they did [56].

Even if they were not retaliating because of information sent through monitored communication channels, prison officials have used details from incarcerated people's communications to *enable* retaliation. For example, in 2000 after a blind and diabetic incarcerated man filed a formal complaint about excess cigarette smoke, guards read his mail over the prison's intercom system and also "barred him from phoning his attorney, cursed at him, spoke derogatively of his blindness, subjected him to harassing strip searches, and threatened to 'smash his face' and hang him" [78].

Aside from the harms surveillance can impose on incarcerated individuals, people who are not the primary targets of surveillance are also impacted. Around 75% of people incarcerated in local jails around the country *have not been convicted of a crime* and are subject to surveillance only because they cannot afford bail [105, 106].

2.3.2 Impacts of surveillance beyond prison. Research on the effects of surveillance has documented "chilling effects"; i.e., the way surveillance deters the exercise of free speech due to awareness of constant monitoring [69]. Penney notes that even people who do not fear being persecuted may modify their online activities for fear of being labeled as non-conformist or socially deviant [69]. Increasing public awareness of government surveillance following the 2013 Edward Snowden NSA and PRISM revelations impacted privacy-sensitive Google and Bing searches, Wikipedia article traffic, and Tor browser usage [51, 69, 70].

In recent years, public discourse on privacy has expanded from discussions of state surveillance to include corporate surveillance. Some have stated that the recent surge of political energy around protecting privacy is because surveillance that was traditionally carried out on marginalized communities now targets affluent communities [31]. Low-income Americans must accept impromptu home visits from inspectors to receive federal housing assistance, and some states require low-income Americans to undergo drug tests to receive Medicaid or food and housing assistance [54, 57]. Incarcerated people and their relatives have also been subjected to high levels of surveillance for decades. This work focuses primarily on data privacy/surveillance, but it is important to recognize that marginalized communities often face other targeted and discriminatory forms of surveillance [31].

2.4 Additional Related Work

Our work focuses on communication technologies used while people are incarcerated, but prior work has addressed other aspects of incarcerated peoples' technology-related experiences. Verbaan et al. described challenges with designing technologies for incarcerated people to encourage the HCI (human-computer interaction) community to do more work in this area [104]. Ogbonnaya-Ogburu et al. examine the digital literacy challenges faced by returning citizens (i.e., "formerly incarcerated people") reentering society and their implications for job readiness [66]. Although there has been significant work in the social sciences and humanities exploring the impact of having a relative incarcerated on families [5, 13, 17, 36, 103], existing literature does not focus on their unique privacy needs.

Recent work in the computer security and privacy community has examined the unique security and privacy needs of several specific (and sometimes marginalized or vulnerable) populations, including refugees [86], undocumented immigrants [35], survivors of human trafficking [16] and intimate partner violence [15, 32, 37], older adults [33], teenagers [22], people with visual impairments [1], people with a low socioeconomic status [50, 75, 85], and transgender people [47]. Our work contributes to this space by exploring the unique privacy needs of another specific group: family members of incarcerated people.

3 METHODOLOGY

Our study consisted of 16 in-person interviews with FMIP who regularly communicate with a relative who was incarcerated at a prison or jail in PA at the time of the study. The semi-structured interview protocol first focused on participants' experiences with communication, then shifted to their perceptions regarding specific surveillance practices at their incarcerated relatives' facilities, and finally directly asked about their privacy concerns.

We interviewed FMIP rather than incarcerated people directly for several reasons. Working directly with incarcerated people introduces ethical challenges, including the notion of consent in an environment where participants may be *compelled* to participate because of the amount of financial compensation we offer (especially if they are unable to earn similar amounts of money themselves

while incarcerated). Additionally, interviewing incarcerated people would have likely introduced bias or risks to participants since our conversations would have been monitored. Lastly, recruiting and gaining access to currently incarcerated people would have been challenging. Another research strategy could have focused on interviewing formerly incarcerated people. However, interviewing people who *currently* communicate with an incarcerated person gave us an up-to-date view of participants' experiences with these communication systems, whereas formerly incarcerated people might have an outdated understanding of these systems.

3.1 Recruitment

To recruit participants, we used standard recruitment methods, including (1) flyers posted on campus and at libraries throughout the city, (2) advertisements on local online forums (i.e., Craigslist, Reddit, and Facebook), (3) sharing the study through relevant email distribution lists, and (4) encouraging people who saw the study advertisement to share it within their own social networks (i.e., snowball sampling). We connected with local organizations that support incarcerated peoples and their relatives (e.g., Pennsylvania Prison Society [88] and Families Outside [68]), and they shared our study on relevant email distribution lists.

Recruitment materials specified only that the study was "about prisons and communication with their incarcerated relatives" and did not mention surveillance. The screening survey contained a header that described ours as a "study on privacy and prisons" and identified our association with a security and privacy-related institute. This was the extent of surveillance-related framing before the interview. Online recruitment materials and the screening survey instrument are included in Appendix A.3. Cross-referencing participants' reported recruitment method with the (limited) details they provided about their incarcerated relative, we are confident that no participants were related to the same incarcerated person.

Potential participants completed a screening survey, which allowed us to ensure that all participants had a relative (including a grandparent, parent/guardian, child, grandchild, sibling, cousin, partner, or spouse) at a PA prison or jail with whom they regularly communicate (via phone, video, mail, email or in-person visitation). Participant demographics are included in Table 1.

Participants were mostly young, predominantly Black/African American, and had formal education levels ranging from high school to college degrees. These characteristics do not necessarily reflect the age or race of their incarcerated relatives — for ethical reasons, we did not collect such details about participants' incarcerated relatives. Although the state in which the study was conducted is 79% White and 11% Black, the incarcerated population is 46% Black and 39% White [40]. Most participants' incarcerated relatives were at state prisons. Many participants used more than one method of communicating with their relative — the majority being phone, mail, and in-person visitation. No participants used video-conferencing, possibly due to restrictions on its use in PA; instead of using the tool at home, FMIP were required, at the time of our study, to physically go to a prison (possibly closer to their home than the one where their relative was incarcerated) to access video conferencing. Currently, in reaction to the COVID-19 pandemic, FMIP are allowed to video conference from their homes [60].

Age	25-34 (7), 35-44 (3), 45-54 (5), 55-64 (1)
Education	High School or GED (5), Some College (4), Associate's Degree (5), Bachelor's Degree (2)
Gender	Male (7), Female (9)
Race	Black/African American (10), White (6)
Relative's Prison or Jail	County Jail (6), State Correctional Institution (10)
Communication Methods Used	Phone (15), Physical Mail (13), In-person Visitation (12), Electronic Messaging (4)

Table 1: Summary of Participant Characteristics.

3.2 Interview logistics and protocol

We made a concerted effort to be flexible when scheduling interviews to minimize the impacts of systemic inequities that might otherwise prevent or discourage individuals from participating. To accommodate a variety of job schedules, we started interviews as early as 6am and as late as 7pm, any day of the week. We also accommodated participants who needed to reschedule. We obtained permission to conduct interviews in meeting rooms at local libraries (from the libraries and our institution's IRB), and at an on-campus location; this helped ensure that participants would not need to weigh the financial, time, or logistical effort of arranging transportation across the city against their desire to participate. Historically, libraries have acted as safe gathering places for low-income individuals, especially young people [48], and people from low-income families are over-represented in prisons [83]. These factors made libraries particularly well-suited hosts for an inclusive study design.

All interviews were conducted by the first author, who is Black and felt comfortable using African American Vernacular English. Prior work has demonstrated "race-of-interviewer" effects, showing that African American's sensitivities to the race of the interviewer has a large impact on their reported political attitudes [24]. This effect has been shown to have a particular impact in the context of police violence [82], which is related to the topic of our study. Recent findings in HCI also show that Black participants gave longer and more detailed responses to interviews that were led by a Black researcher [65]. Because the majority of participants in our study were Black, our use of a Black interviewer with similar lived experiences may have made participants more comfortable and forthcoming in their responses.

Interviews lasted approximately one hour, and participants were compensated $30 USD. With consent, interviews were audio recorded and transcribed using a third-party transcription service. Interviews were conducted in December 2019.

We began the interviews by reviewing our consent form and verifying participants' screening survey responses. Then, we asked questions about their communication with their incarcerated relative (e.g., via phone, video, letter, etc.) and their perceptions of how prison communication companies manage data collection, retention, and use. Some questions were specific to the prison/jail where their relative was incarcerated since different prisons contract with different vendors that may use different practices, which we investigated prior to the interviews. We closed the interview by

asking directly about privacy and left time for additional participant comments.

3.3 Data analysis

Our analysis used a collaborative, qualitative open coding process [102]. Two researchers collaboratively analyzed the first six interviews and generated themes based on quotes/ideas from the interviews. We then organized quotes/ideas into these themes, and iterated until disagreements and ambiguities were resolved. Both researchers listened to the remaining 10 interviews to identify new themes, which were subsequently discussed together. Once agreement was reached, we created a codebook based on the identified themes. The first author applied this codebook to all interview transcripts. The interview protocol and codebook are included in A.1 & A.2.

3.4 Ethical considerations

All procedures were approved by our institution's IRB, and participants read and signed an informed consent document prior to beginning the interview. Because of the nature of the topics discussed in these interviews, there was a risk that participants might reveal private or sensitive information about their incarcerated relatives, who were not participants in the study. At the beginning of the interview, we reminded participants to focus on their own experiences and not reveal any such details. If participants still mentioned potentially sensitive information, we removed those portions of the audio recordings before sending them for transcription.

4 FINDINGS

We now describe the results from our interview study. To understand the context of the privacy-related aspects of participants' communication experiences, we start by providing a general overview of participants' communication practices with their incarcerated relatives. Subsequently, we describe participants' awareness of surveillance practices, their attitudes about these surveillance practices, and what privacy-preserving strategies, if any, they use when communicating with their incarcerated relatives. We evaluate the accuracy of participants' perceptions of surveillance practices in this section where it is possible and straightforward. We end this section with recommendations from select participants on how to improve these communication methods.

4.1 Communication practices

Participants broadly expressed a desire to stay in touch with their incarcerated relatives. P4 said he wanted to *"make sure the person is safe ... they're still alive. It feels good to have someone in your corner in that horrible situation, you know. If you don't talk to no one on the outside, you feel kinda boxed in, like people left you."* P8 also thought in-person visitation was important for the well-being of the children of the incarcerated person: *"They get to see their dad ... and he gets to see his kids."*

Common conversational topics when communicating with incarcerated relatives included updates about family and friends, current events (e.g., sports or news), requests for money for commissary or phone accounts, and conditions inside the facility (e.g., poor food quality and mistreatment by staff).

Twelve participants said that they avoided topics that might agitate or sadden their incarcerated relative, such as their struggles or enjoyable things that they are able to do because they are not incarcerated. For example, P14 said, *"people miss home when they're in prison, so I don't even talk about it."* P7 avoids mentioning some of her personal struggles because her incarcerated relative becomes frustrated that he is unable to help: *"I did [mention that] in the beginning. Then he's like 'well that wouldn't happen if I was there.' "*

Participants discussed challenges of communicating regularly, related to money, emotional stress, or other personal circumstances—including the participants' work schedule or the proximity of the facility to their home. For example, P11 sent electronic messages daily but only visited in person once per month because electronic messaging is relatively inexpensive (25 cents per message) and less time-consuming than in-person visitation. However, P11 and P16 also expressed irritation about the errors within the electronic messaging platform, with P16 saying that *"it could take anywhere from like 10 minutes to days"* for her incarcerated relative to receive a message she sent. When speaking about the cost of electronic messaging, P12 described the financial burden that using electronic messaging placed on their entire family, not just on the person who was incarcerated: *"Even though it's email, they call it a stamp. You still have to pay to send the email. It's messed up because the person in the beginning didn't have any money ... did the crime, and the family that has to pay for the crime didn't have any money anyway."* Eight participants mentioned the price of phone calls as a challenge for communicating with their incarcerated relative. Mail was commonly described as taking too long to be delivered. In an especially egregious example, P14 said she ordered a textbook for her incarcerated relative to take a class, and it arrived 8 months later after his class was already completed.

P1, like P5, said that doing in-person visitation made them uncomfortable: "*The whole process of going to the jail just sucks, you know? [I] just feel uncomfortable, getting in front of the police and the correctional officers, you know?*"

4.2 Awareness of surveillance

Demonstrating that surveillance is a salient component of their communication with incarcerated relatives, 12 participants discussed privacy or surveillance before we explicitly brought it up. For example, P1 said: *"You gotta be careful what you say ... I'm sure they're monitoring or somethin' like that."* All participants believed that they are identified when communicating with incarcerated relatives, either because they know they are required to be on a pre-approved list (as often is the case for phone, video, in-person, and electronic messaging) or from the return address on physical letters they send (P3,P5,P15). Another practice that eight participants accurately anticipated was the capability for prison staff to conduct a keyword or "buzzword" search of collected data, such as recorded phone calls or scanned mail.

We now describe participants' understanding of surveillance practices for each communication method and their general understanding of how legal, practical, or technical limitations impact surveillance practices. Actual surveillance practices are a complex confluence of technical capabilities and tools provided by the government or third-party communications companies, law and policy,

and individuals' behaviors (i.e., possibly against policy), and they change over time and may differ between facilities.

4.2.1 *Surveillance of specific communication methods.*

Phone calls. Of the 15 participants who used phone calls, 14 understood that someone could listen to their call, and all 15 anticipated that the call would be recorded. Regarding phone call audio data retention, P11 knew that records are retained even after incarcerated people leave facilities because her brother used phone records in a lawsuit against a former partner with whom he had communicated while incarcerated. P13 realized "phone system" company employees (e.g., at Securus) listened to calls but inaccurately believed that officials at a jail could not also listen: *"The phone system is not through the jail. The phone system has nothing to do with the jail. ... I do not think that [a guard or correctional officer could access a recording of a call]."*

Participants were less aware of other surveillance mechanisms, such as voice-printing (i.e., inferring the identity of the call recipient(s) based on their voice) and location tracking for calls received on cell phones. Respectively, only three and five participants believed each of these would happen. Even when participants were aware of these types of surveillance practices, they lacked an accurate understanding of how they are implemented. For example, P6 (whose relative is at a facility that uses GTL's phone service) thought that location tracking would end once the phone call ends; however, as mentioned in Section 2, GTL tracks call recipients' location for 60 minutes after the start of a call, regardless of the call's duration. Some were aware of additional surveillance mechanisms, such as those used to prevent three-way calls, but did not understand them, either. P11 described how GTL's three-way call detection capability was used at a county jail: *"My [relative] was in jail, and I tried to call my mom on three-way. And it had warned me, and it picked up on that three way. And it hung up on the call."*

Physical mail. All 14 participants who sent physical mail realized that the letters they sent would likely be opened before receipt. Furthermore, 13 believed the written contents were read by a human other than their relative. This belief is supported by the posted mail policies of all facilities we studied.

As previously discussed, three participants thought that the return address on mail envelopes could be used to identify senders. We believe this is accurate since the stated policies of the facilities within this study required senders to put their full first and last names in the return address field in order for mail to be accepted. One of the participants (P9) said that she previously had a letter rejected because she used her first initial instead of her full first name in the return address. P12 noted that this could be circumvented by writing a false return address on a letter: *"I can send the letter, I could be anywhere. I could put a different address on the letter, but still send it. Which people do."*

In-person visitation. Everyone who did in-person visitation (12 participants) realized they are monitored in some way during their visit (e.g., that there are guards physically present and/or surveillance cameras). However, their understanding of what guards were paying attention to varied. For example, only three participants believed that guards were attempting to listen to their conversation. P6 and P11 believed even if guards wanted to, it was not possible: "*You're just in close proximity... it's hard to pinpoint what anybody's saying*" (P6). P16 was keenly aware of surveillance via cameras from people she could not see. One time she began breastfeeding her child "*very discreetly and they caught it. It was like instant, as soon as I started. So they're definitely monitoring.*"

P9 described learning about several aspects of in-person surveillance during her first visit, specifically that she was being surveilled to prevent her from talking to another person, which is against prison rules. Another visitor offered to cover the cost of a sandwich because she did not have exact change and cautioned that the guards were watching them:

> "I didn't even think anything of it, and then I started to walk over with her [to buy the sandwich]. And she said, 'They're watching us.' And I'm like, 'What do you mean they're watching us, like, what is this, 1984, Big Brother?' [laughing] And I'm thinking to myself: 'What are they watching? They [metal detector] wand you. They [scan] your hands and everything. You're not allowed to take anything in. They have your ID. You take your shoes off and everything, like ... Why are they watching? But she said ... I'm not allowed to talk to other people there, only the person I'm visiting. So I didn't know that was a rule ... So, yeah, they monitor. And they walk around. They're up on ... a couple of steps where they look down on everything. And then every once in a while they walk around."

Less-used communication methods. Only four participants used electronic messaging tools: P11, P12, P13, and P16. P11 noted that these messages were being monitored and screened and was concerned by how long it took for her relative to receive them: *"Some of them will be on delay. And I'm like 'Did I say something crazy in there where they're on delay?' "*

No one in our study used video visitation, which is available only at state (not county) facilities in PA. P12, whose relative is in a state facility, mentioned that she does not use video visitation because the places she would have to go to use it are too far away.

4.2.2 *Perceived legal, practical, and technical limitations.*

Legal. Participants thought that there were legal protections that limited what information could be collected about their communication, who could access the data, or when it would be deleted. For example, eight participants, including P10, believed that police needed a warrant or a court order to access communication records: *"I believe they will have to get a warrant because that's invading someone's privacy even though it does tell you that these calls are monitored."* However, as mentioned in Section 2, law enforcement or district attorneys can obtain audio recordings upon request.

When asked if he thought voice-printing was happening during his calls, P14 did not believe this was allowed and was unaware that it was enabled by Securus, the phone vendor at his relative's facility: "*They're not allowed to do that, are they?*"

P5 explicitly mentioned that there must be a limited duration of keeping phone records after the relative gets out because FMIP have their data collected as well:

> "I think they still gotta hold of 'em even after you leave, ya know? But there has to be some type of limitation where as though they have to destroy 'em

> after a certain point in time. Especially if you haven't been incarcerated, ya know? And then the person who you're talking to, they have a right to know what you recorded, too. Especially being as though they're not incarcerated, you know? You have recordings of them. That's like, some guys they be on there having phone sex. What do you do with that? How long you wanna keep that? Do you listen to that?"

When asked if she thought she had the right to delete her data, P9 said: *"I never thought about that but it seems like I should have rights in that situation because it's me, my voice, my information ... IDK [I don't know], I feel like that's one person against a big organization."*

Practical. Regardless of their views on the legal requirements related to surveillance of communications with incarcerated people, participants brought up practical reasons for disbelieving that certain types of surveillance were in use, mainly related to those that they believed required manual effort. For example, some participants believed that officials *could* track call recipients' location, copy mail, and/or implement voice-printing, but they do not, not realizing that these data collection mechanisms were automated and required little administrative effort.

Some participants, such as P2, believed that some surveillance mechanisms were not worth implementing against them because the data would not be useful: *"It's a matter of, like, you can't monitor everything, and how much are you really gonna glean?"* One way participants thought officials might evaluate usefulness and, thus, prioritize which communications to monitor was dependent on the "riskiness" of the incarcerated person or if their case was still open. For example, P1 believed phone calls were not listened to *"unless if it's some violent person, you know?"* These participants all felt that, given their particular situation, they were not especially likely to encounter the most invasive surveillance practices.

Technical. In some cases (n=4), perceived practical limitations were rooted in participants' understandings of technical challenges or costs. When asked whether he believed his location was tracked when receiving phone calls, P2 said: *"Where there's a will there's a way,"* but followed up that *"If we're talking about just, like, a county jail, I don't know ... I think that's above their pay grade, slightly."*

Perceived prohibitive data storage costs were a reason eight participants doubted that all communication data would be collected and/or saved for prolonged times. Considering whether phone calls might be recorded and analyzed, P5 posited: *"I don't even think they record them all. I think it's really a scare tactic 'cause that's a lot of audio, you know? That's a lot of transcripts. That's a lot of data right there, you know? Like, where you storin' all that?"* P5 thought that recorded phone calls would be transcribed and the audio deleted in a timely manner to reduce storage space requirements.

P9 expressed skepticism about the technical processing ability at individual facilities; she thought external entities handled any data processing. Additionally, she pointed out that storing this data externally made the data more vulnerable to hacking: *"I don't think that facility can handle all that kind of communication, meaning video recordings, plus telephone recordings, plus. So I think it has to go out somewhere. And anytime it goes out, I guess you have that propensity for a problem to occur. And/or hacking or something."* Not only did she accurately differentiate between the technical ability of individual facilities and the communication companies, P9 also anticipated that mass storage of phone call records might lead to data security challenges. This is evident from the 2015 hack and release of 70 million phone records (metadata and audio recordings) from Securus, including 14,000 calls between incarcerated people and their attorneys [87].

The participant who was formerly a county jail correctional officer (CO) believed that computer-based analysis could not provide useful data and, thus, did not enable complete automation of surveillance. He viewed slang as difficult to interpret, even manually, and thought it would be too complex for a computer:

> "There's a lot of slang ... You think you're paying attention, but there's just things that ... you almost don't even hear them ... I know that's kind of making an argument for transcripts and against audio, but I'm saying the transcripts would almost certainly be wrong. The voice automation trying to decode like prison slang I don't think it would do well with that, so I would think they would have to have the audio so they could drill back on it."

GTL and Securus both claim that their products can identify and flag "street" or slang terminology.

4.2.3 Distrust of official policies. Despite official policies they realized might exist, seven participants did not trust that prison staff would consistently adhere to them, which could result in privacy invasions beyond those described in official documents. When previously incarcerated, one participant recalled guards reading mail even though they were supposed to only check mail for contraband, not read its contents. Another participant conveyed similar distrust of official policies: *"They say they're not supposed to read [physical mail], but how are you ever gonna prove it?"* This was further substantiated by his experience as a CO: *"You'll be told to do things by the book but also get them done, and those two things will be almost unreconcilable [sic] ... you're not specifically told to cut those corners, but you're told, like, get it done."*

Regarding whether police need a warrant to access her communication data, P13 said: "*The laws probably say you need a warrant, but I'm pretty sure that if they got ...like a connection on the inside that they can probably get it.*"

4.2.4 Learning about surveillance. First-hand experiences contribute to participants' understanding of surveillance practices. For example, P11 learned from experience that visitors' cars can be subject to random searches at state prisons and that police dogs are sometimes used to search visitors. Most frequently, personal experiences came up in the context of realizing that their identity would be known and recorded because of procedures they had to follow, such as showing identification documents to communicate with their relative. P9 was even required to provide a child visitor's birth certificate as identification before being allowed into the facility for an in-person visit. Similarly, some participants learned about surveillance from *other people* in similar positions; for example, P9 was warned by another in-person visitor about being watched and therefore unable to converse.

Five participants learned about surveillance through firsthand experience in a facility in roles besides being a visitor. Since these roles

may make them more identifiable, we do not report participant numbers. One participant worked as a CO for two years. Although not asked for ethical reasons, four participants voluntarily mentioned that they were previously incarcerated. They described surveillance practices they observed — including some that diverged from stated policies — and times when they saw people face consequences for sharing the wrong information.

Although no participants stated that they explicitly sought out official documentation such as privacy policies, five called attention to the recorded notices that interrupt phone conversations every few minutes to remind callers that they are talking to an incarcerated person and the call may be monitored: *"They interrupt a few times to let you know you're being recorded"* (P9).

Finally, media portrayals of prison life were another source of information, which five participants used to explain their understanding of surveillance. For example, P15 watched a TV show in which a surveillance camera was used to catch a person transferring drugs to an incarcerated person by kissing them during a visit. P12 responded to a question about whether technology might be used to analyze his voice and identify him on a phone call by saying that he learned about this practice from the prison documentary series *Lockup*: *"I've watched Lockup. They have places that do that for 'high gang' related individuals. I don't think they have that for [my relative's facility]."* He then explained that he watches this series explicitly to learn about what his relative might be experiencing: *"I watch it 'cause I wanna know, in a sense, what her world's like."*

4.3 Attitudes about surveillance

In this section we highlight participants' comments about their concerns, attitudes, and perceived goals regarding surveillance.

4.3.1 Reactions to surveillance. Even when they did not expect to experience any consequences related to their communication with incarcerated relatives, 13 participants described a general sense of unease or apprehension about being monitored. P12 described challenges with trying to communicate while knowing one is under surveillance:

> "... there is a lot of communication [discussing] the judicial system between the person and then their family. So there's no real communication on that which doesn't tap on all three levels of letter, visits, and phone calls. But it's just difficult to communicate with somebody when you know that their communications are being tracked and being monitored and ... of course ... can be used against them."

Participants specifically expressed discomfort in reaction to our questions about how they would feel if their location was being tracked whenever they answered a call from a facility on their cell phones (P1,P4, P5, P10) and how they would feel about a kiosk taking their picture (P1, P4, P5, P6). For example, P5 said *"I don't like being tracked ... I hate that shit!"* P1 said that would make him uncomfortable, but he would still answer his phone even if he knew it would reveal his location.

Some participants believed that surveillance is unfair to them. P6 mentioned that this type of tracking can *"make you feel like you're criminal because you have a loved one in prison."* P11 expressed a similar sentiment regarding location tracking: *"Um, I mean, I wouldn't care for that. I mean, I guess it wouldn't be a big enough problem for me to stop answering calls. But I feel like that would be a violation, you know? I'm not in jail, you know?"* He also said: *"I don't want my face in some police database; I didn't even do anything."*

4.3.2 Potential harms of surveillance. Participants rarely talked about consequences or harm they had actually experienced as a result of something they said or did when communicating with their incarcerated relative. One exception was P15's description of emotionally disturbing aspects of surveillance while visiting her son in person. She was falsely flagged as trying to smuggle drugs in, which she was told could lead to disciplinary action for her son:

> "It was a traumatic experience because my son, I had see him behind bars. Well anyway, they scanned my hand ... and then the thing started going off. And he looked at me and he says, 'Ma'am, I'm not saying personally but it's coming up positive for cocaine' ... He told me ... 'if it comes up positive [again] you will not be allowed back up here and your son is going in the hole.' And I'm like 'this is my first time up here sir' and he just looked at me."

While they had not faced or feared legal consequences themselves, some participants noted that *other people* could face such consequences due to what they say or do while communicating with an incarcerated person. For example, P3 would not be worried if her location was tracked because she does not "*get in trouble. But other people would.*" P7 sometimes overheard other visitors having conversations she thought were too risky because of surveillance:

> "I mean, not with me personally, but I've been in rooms and heard people telling 'So you did do it! And where did you put this?' and I'm thinking 'This is a recording line, are you stupid?' So, not me personally, but yeah, some people aren't the brightest, like, really? ... I don't know what they did, but I'm thinking 'You don't wanna put that on a line. It says they're all recorded.' I'm sure they can't listen to everybody's all the time, because there's how many people visiting? I wouldn't chance it, though, if I was in trouble."

4.3.3 Perceived intentions of surveillance. Six participants agreed that facilities monitor communication with inmates in order to prevent drugs or other items from entering the facility. Eight participants believed that facilities collect evidence to strengthen a legal prosecution — e.g., *"to strengthen a case against someone"* (P7) or *"to get more information on what they might be in for to get more charges pressed against them"* (P10). Seven participants said facilities monitor communication for the safety of incarcerated people, COs, or other individuals in or outside of the facility — e.g., P5 believed that *"there's inmates that call out and send hits out."* Additionally, P14 believed that *"they listen to prevent jail breaks,"* and P10 believed that, in addition to gathering evidence of crimes, *"being nosy"* could motivate them to listen.

4.3.4 Other privacy risks. In addition to acknowledging surveillance concerns, participants discussed aspects of their threat model that went beyond the scope that our interview protocol was designed to address. P6 said that he tries not to have other people around when speaking on the phone for privacy reasons. He does

not want to let them know that the relative is in prison or which prison the relative is in. P11 expressed concern about her phone conversations being overheard by other incarcerated people:

> "See on my end, I'm alone. I'm wherever on the phone. But on his end, I think the phones are all – I hear other people on the phone. So I'm sure people hear us on the phone, which is kind of weird. I think that's another reason why you censor yourself on the phone because, you know, the phones are, like, side by side."

The former CO participant said he was monitored by senior staff to ensure that he did not show favoritism to any incarcerated people. He believed outgoing calls from the facility he worked at were flagged if it was the phone number on record of any staff: *"I know like, I would guess my home phone number [would] ... trigger something ... because they had guards who were busted for fraternization."* This caused him to self report to his manager after receiving an unexpected call from an incarcerated person.

4.4 Privacy-preserving strategies

Participants employed several strategies to help preserve their privacy despite using communication methods that are under significant surveillance, including avoiding certain topics, using euphemisms or nicknames that their family member would understand but officials would not, and choosing communication methods that suited their particular privacy concerns.

4.4.1 Using the most 'private' communication method. Some participants chose the communication methods that they felt would be most appropriate for the type of privacy they wanted at a given time, or where they would be most able to manage their own privacy. For example P9 said, *"On the phone, you know, you just run your mouth ... but when you put it down in writing, you think about it."* P1 believed that the content of his letters would be under less scrutiny than the content of other conversations: *"They just look for contraband. If I send a letter I can just say what I want, I don't feel like I have to worry, really."* Similarly, P2 focused on the privacy of conversation content but concluded that when visiting in person, he takes comfort in "*not having to watch*" what he says because the loud environment of many people talking would render any audio recordings too poor-quality to be useful. P11, considering the threat model of other incarcerated people overhearing their conversation, preferred electronic messaging: *"I would say messaging just because the phones are so close and open. He is the only one getting the message on his tablet."*

When asked which communication method they thought was the most private, nine participants chose physical mail, three chose in-person visitation, two chose electronic messaging, one chose phone calls, and one chose video visitation (although the person had never used it). Mail advocates noted that with mail, anyone could write the letter, no audio or video data is collected, and any return address could be used. Unlike phone calls, in-person visitation, and visitation, the letter writers are usually not required to be on a pre-approved list. We concur that mail may be best for achieving anonymity; however, if someone is caught forging a name or address on a letter to achieve anonymity, a facility might permanently ban them from communicating with their incarcerated relative, or it might introduce legal liability. FMIP who wish to avoid this risk could use in-person visitation, particularly *contact* visits that do not require using facilities' phones. In-person visitation typically occurs in a large space shared with other FMIP and their incarcerated relatives. While other visitors sitting nearby may overhear them (as some participants noted), we do not believe facilities currently have the capability to record bulk audio data and isolate conversations, so they may be able to have a conversation that is not monitored.

4.4.2 Self-censorship. For privacy reasons, 11 participants avoided discussing specific topics when communicating with their incarcerated relatives. These topics included legal representation, family problems, and their relative's case — e.g., P4 said: *"I try not to talk about the case so much ... they can use that as evidence against her."* P5 also mentioned that you would not want to say anything threatening or related to a security breach that might raise suspicion. He also said that generally *"You can't really be open and honest because that can be to a fault."* P4's reason for avoiding certain topics was to give his incarcerated relative privacy from other incarcerated people, not necessarily from the officials: *"There's a lot of people around the phones ... you don't want to talk about nothing too personal or sentimental ... to make her tear up or potentially cry."*

P10 said that she *"[does her] best to not say the wrong thing [and speaks] in code."* P2 mentioned that they used euphemisms and nicknames for people when communicating for privacy reasons.

4.4.3 Lack of privacy-preserving strategies. On the other hand, some participants did not envision any strategies they could use to preserve their privacy while simultaneously maintaining their relationship with their incarcerated relative. P3 said that she already provides her name, and they have her location from her letters, so she is not sure what actions she could take to protect her privacy. P6 could not *"think of any strategies to keep privacy from [the prison]"*. When asked if he had any concerns about his communication methods, P4 said *"No, I mean I don't have a problem with them cause that's the only forms of communication you got."* P2 also mentioned that he did not like the location tracking and the kiosk photos, but he would not change his behavior or stop answering phone calls. P1 felt that in-person visits were not the most private form of communication, but "he's my brother." He wants to see how his brother is doing and see his face. Despite saying that he would write letters to communicate especially private information, P4 still mostly uses the phone because *"You know they're still alive ... it feels good [for them] to know that [they] have someone in [their] corner ... if you don't have no one you feel boxed in, like people left you."*

4.4.4 Behavioral strategies. Participants described *behavioral* strategies they used to protect their privacy when communicating with their incarcerated relatives. For example, P6 tried to avoid letting people see the envelopes he used to send mail out because it has a prison address and his relative's DOC number on it. P5 (who used a mobile application for electronic messaging) typically denied all location permissions requests from mobile applications in general and turned them off immediately after using the application if he had to give location permission in order to use the app. He believed this strategy would also help avoid unwanted location tracking when receiving a call from an incarcerated relative.

While many participants were satisfied with the strategies they had developed for maintaining their privacy based on their current

understanding of surveillance practices, a few participants told us that they would plan to change their behavior if they knew about a particular form of surveillance. For example, P12 said that he would stop using the phone for communication if he knew his location was being tracked:

> "[I would feel like I] was under heavy monitoring, and [I was] probably next in line to be arrested ... I would probably be less likely to receive the phone call, go to another form of communication, so I could then not have to give my location ... current location, I think it's the current location part that freaks anyone out."

P1 said he would stop using the kiosks if he found out they were taking his photo and sharing it with law enforcement.

4.5 Recommendations from participants

Near the end of interviews, we asked participants if they had any suggestions for researchers or policy makers on how to improve prison communication methods. While none of these recommendations focus on improving privacy, they are illustrative of the broader needs of FMIP beyond privacy. We present quotes from three participants that contextualize their recommendations.

P12 expressed a desire for increased transparency and ease of communicating while also recognizing that many people are dismissive of the needs of incarcerated people and their families:

> "On the computer programming side ... none of that stuff is going to change ... The only thing that's going to change is ... that you can make it easier for the people on the outside to reach out ... not only to the person but to the judicial system and find out what's going on. But that's not going to be something that people will push for and approve, because these are people that we are meant to punish and forget in a sense. But these people still have lives and people that they love and want to communicate with."

P15 wanted policy makers to make communication less costly and called for more empathy towards incarcerated people:

> "The prices are too high. I mean, they're supposed to be inconvenient ... but to me, it is a good thing to let them talk to a loved one so they can get support ... You keep all this stuff away from them, they're going to be like a caged animal. They're not gonna be reformed ... 'Love the sinner, hate the sin.' Give 'em what they need so they can flourish, you know? ... I know they've done terrible things, but everybody deserves a chance to change and [they should] give them the support they need to make those changes, in the prison and outside the prison."

P16 wished communication options were more flexible. She shared a story about how her significant other didn't find out about their child's birth until a day later:

> "I would say that families need to have more communication, they need to have more options. Like I was pregnant with her when he went into jail. I called up at the jail, he was in ... to let them know that I was having [my child] and they wouldn't tell him and up there you can get one call every four days. And so he didn't find out about me having [our child] until the day after ... That was pretty messed up. And when I called there, the Chancellor was like, we don't do birth announcements. We only do death or sick calls now ... They say they're about family, they need to really be about the family. And I feel like part of the rehabilitation for an inmate would be connection with their families. Like I know they, they want to keep certain people not connected, but ... being connected will help ... them feel like they have a purpose."

5 DISCUSSION

5.1 Misalignment of stakeholder incentives

In many sectors, companies are naturally incentivized to create tools that support end-users and to respond to feedback from them. This can lead to tools that end-users *want* to use (e.g., Apple marketing its products based on their privacy features to appeal to privacy-conscious consumers [41]). There are different incentives in the prison communication landscape. Some companies have exclusive contracts covering multiple forms of communication, giving people no alternative but to accept surveillance or cut off contact with incarcerated loved-ones. Participants in our study conveyed that, while they do not *like* the communication tools available (for surveillance reasons but also because of high costs, inconvenience, and low quality or reliability), no other options are available. That is, despite the drawbacks, their desire to support their relatives leads them to use these communication tools anyway. While people can (and do) complain about these tools, ultimately, the companies providing communication for carceral facilities answer to the prisons and jails rather than to end-users. Consequently, they do not have strong incentives to cater to end-users' needs because they are, both literally and figuratively, a captive audience.

This dynamic helps explain why the few privacy controls that exist for FMIP have limited impact. For example, some participants believed that they could request that the communication companies delete their communication data, especially after their relative is no longer incarcerated. Based on stated policies, we do not believe this is accurate. Only GTL's policy addresses data deletion: it can be requested only by California residents under the California Consumer Privacy and Protection Act (CCPA). However, its privacy policy outlines broad exceptions under which deletion requests can be denied. For example, GTL can deny a data deletion request if the information is necessary to "make other internal and lawful uses of that information that are compatible with the context in which you provided [it]" [19]. Additionally, to opt out of location tracking *after* a phone call has ended FMIP must contact GTL and request this; they cannot opt out *during* the call. To even use these limited existing controls, FMIP—some of whom may never use online tools if they are communicating exclusively via phone, mail, or in-person visitation—must find and read privacy policies online. Given that only 9% of Americans say that they read privacy policies before agreeing to them, it is unlikely that FMIP will become aware of these already limited controls [8].

5.2 Surveillance and incarceration

Some participants believed that surveillance of communication with incarcerated people was done for safety reasons, such as preventing drugs from being smuggled in or assassinations from being ordered over the phone. However, some of these same participants expressed unease about being surveilled by staff at carceral facilities, the communication companies, or external law enforcement agencies (police, FBI, district attorneys, etc.). This contrast highlights two competing narratives about the role of surveillance in society broadly. One narrative insists that state actors (COs, law enforcement, prosecutors) need surveillance to ensure public safety and stop bad actors. The other views widespread surveillance as an opportunity for state actors to abuse the information they collect.

The latter narrative questions who is considered a bad actor (or deserving of surveillance) and for whom surveillance supposedly provides safety. Simone Browne argues that blackness is and has historically been coded as criminal; this explains why many forms of surveillance are disproportionately used on Black people in the U.S. [12]. This may also help explain why surveillance of incarcerated people and FMIP is deemed obvious and necessary. Similar to the logic of stop-and-frisk, once state actors consider someone suspicious or criminal, they must deal with additional surveillance without meaningful mitigations (besides not communicating with your relative or, in the case of stop-and-frisk, not walking outside). FMIP are coded as criminal because they communicate with someone who is incarcerated, despite the fact that 3 in 4 people in jails have not been convicted of a crime and may only remain incarcerated because they are low-income and cannot afford bail.

As some participants noted, discussing the events leading up to their relative's arrest can help them gain closure or insight into these events. But since they cannot communicate without surveillance, discussing such information is risky. Being unable to discuss these events adds more uncertainty and difficulty to the already disruptive event of having a family member incarcerated. Several participants were aware that what they discuss while communicating with their relatives can be used to strengthen an ongoing case or open a new case against their relative. However, people who avoid pretrial detention have significantly better case outcomes [26], suggesting that this surveillance affects case outcomes (i.e., that some people do have conversations that are used against them in court [6]). Black people disproportionately face pretrial detention (and, thus, surveillance). Given this context, it makes sense that multiple participants had privacy concerns in which they viewed state actors as adversaries, contrary to the narrative of surveillance ensuring safety.

5.3 Recommendations

Although this work focuses on the surveillance of communication with incarcerated relatives, the larger context is the problem of mass incarceration in the U.S., which is fueled by mass criminalization [3, 29, 34, 44]. While we can offer design and policy recommendations to make communication easier and more privacy-preserving for FMIP 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 (through, e.g., decriminalization, abolition) [43]. That being said, we present privacy-focused recommendations for policy makers and end-users based on participants' recommendations and existing privacy advocacy efforts. We omit explicit recommendations for carceral facilities and *prison communication companies*. These entities already have the technical capabilities to significantly limit or eliminate the forms of surveillance they provide to facilities, and over time they are increasing the surveillance capabilities they offer, not curtailing them. Given the history of regulating the prison phone industry [39], little evidence suggests that they will change surveillance without being forced to do so by regulators. Consequently, we focus our recommendations relevant to carceral facilities and prison communication companies on regulatory action.

5.3.1 *Recommendations for policy makers.*

Minimize data collection. Similar to the principle of data minimalization outlined in the European Union's General Data Protection Regulation (GDPR) [64], prison communication companies should limit what data they collect. The 2015 Securus hack [87] shows that these systems may be vulnerable and, when they are compromised, sensitive information about an already vulnerable population may be released and cause substantial harm.

Increase access to data controls. Corporations and state actors have long argued that they need bulk data collection for legitimate purposes; yet, regulation has increased individuals' power over how their data is managed. Prison communication companies should not be exempt from these data protections; these protections should give individuals control and power, and they need to be extended nationally to all people (not just U.S. citizens or California residents).

Require transparency about surveillance practices. Multiple participants wished that facilities and communication companies were open and transparent about their surveillance practices. Secret or obfuscated surveillance practices inherently create risks of abuse, discrimination, and selective enforcement because of the lack of public oversight and accountability [76]. Incarcerated people and their families are particularly vulnerable given the broad power that prison staff have to temporarily or permanently limit their ability to communicate. If FMIP are not aware that a certain form of surveillance is happening, they might do or say something thoughtlessly that could have severe negative consequences for them *and* their incarcerated relative.

5.3.2 *Recommendations for end-users.*

Use the most private communication method. Individuals who want to communicate privately should use the communication method that best preserves their privacy given their threat model. For example, to communicate with someone who is incarcerated while protecting your identity, mail may be a fitting option. If your objective is to prevent facilities and companies from monitoring your conversations (while accepting that other people may overhear them), in-person visitation might be your preference. Electronic messaging can also be advantageous since no audio or video data is collected when one uses it (although the identity of the person whose account is being used to send messages is known). While we evaluate the privacy of the previously mentioned communication methods, we recognize that other factors may dominate people's decisions about what communication method to use, including cost, convenience, schedule, and reliability.

5.3.3 Communicating surveillance practices, risks, and legal rights to end-users. In addition to our recommendation above – that policy makers pursue transparency requirements – it is vital that this information be communicated effectively. It should be disclosed (1) in a way that is understandable, (2) at a time when FMIP have the capacity to process it before regularly using a communication method, and (3) in a way that does not frequently interfere with communication. Because we hope that conveying this information will eventually be a requirement for communication companies, we propose approaches that integrate with communication systems; however, we also include a suggestion for how advocacy groups could disseminate information without waiting for policy changes.

Contacting an incarcerated relative via phone, video visitation, and electronic messaging already requires creating an account in advance (e.g., online, in an app, or by phone). Information about surveillance practices and risks (e.g., that what is said on a phone call may be used against their incarcerated relative in court) should be presented during the registration process, similar to requiring users to accept a privacy policy before using a service. When FMIP create communication accounts in an app, we suggest that surveillance practices be disclosed directly in the app (rather than only in the app store), because prior work found that people recall more information from privacy notices if they are shown in this way [9].

On the other hand, FMIP typically learn facilities' mailing addresses by word-of-mouth, receiving a letter from an incarcerated person, or looking it up online. Facilities should explain collection, use, and retention of mail on their website, alongside information they already provide about mail policies (e.g., no red ink allowed). Since some FMIP may not look up information online, a postcard or brief handout containing relevant information should be mailed to people after they send their first personal letter to a facility (as suggested by P3). If a FMIP's first letter is rejected for violating mail policies, such a response would create further benefit by helping them understand the reason for the rejection.

One opportunity to encourage prison communication companies to increase transparency is to require that Requests for Proposals (RFPs) during the bidding process for facility contracts demand that potential vendors provide a readable summary of their surveillance practices. However, such policy change often takes significant time. In the meantime, advocacy groups could produce and distribute handouts summarizing local facilities' surveillance practices and the potential risks for all available communication methods. This could provide considerable immediate benefit to FMIP, although these handouts would inevitably be incomplete (since detailed information about facilities' practices are often not available) and may quickly become outdated as facilities change their practices. Towards this effort, we attach an example handout, designed for Allegheny County Jail in Pittsburgh in Appendix A.5.

5.4 Limitations and future directions

Despite searching for details about surveillance practices of prison communication companies and the specific facilities at which participants' relatives were incarcerated (including submitting an open records request for a contract), we were unable to determine a thorough ground truth. Some contracts we accessed had redacted sections describing the implementation details of surveillance mechanisms to allegedly protect trade secrets, despite a court having ordered in the past that one of the contracts be provided to a plaintiff in its unredacted form [11]. This meant that although we might be able to identify the availability of a particular surveillance mechanism (such as voice-printing), we cannot state that this capability is begin used by a specific facility on *all* calls. Facilities' policies also change; one facility in this study changed its video visitation policy because of COVID-19.

This work focuses on how the families of incarcerated people face unique privacy risks. However, our study does not include the perspectives of currently incarcerated people. As mentioned in Section 3, it is difficult to interview incarcerated people to ask about the impact of surveillance because *the communication is being surveilled*. Further, it is also more challenging to recruit incarcerated people, notwithstanding the ethical issues around compensation and consent. We interviewed participants who had relatives incarcerated at prisons and jails, but there are several other areas within the U.S. carceral system (e.g., youth or immigrant detention centers) where incarcerated individuals and their families might be more vulnerable and have stronger privacy needs.

As in many qualitative interview studies, the number of participants is small and limits the generalizabilty of our results. Future work could explore other methodologies that are easier to scale (e.g., surveys). While it would not address bias due to surveillance, a survey-based methods could enable incarcerated people to be recruited and participate in the study via mail.

While this project was an exploratory study by design, future work could involve participatory design studies with FMIP or incarcerated individuals to understand what specific UI improvements could increase their awareness about surveillance practices without being intrusive. These studies could include designing browser extensions or mobile applications that present contextual information to end-users about surveillance practices and associated risks.

6 CONCLUSION

We conducted a qualitative, exploratory study to understand the experiences of family members of incarcerated people with surveillance when communicating with their incarcerated relatives. We interviewed 16 adults whose relatives were currently incarcerated in Pennsylvania and investigated the surveillance practices of the facilities and prison communication companies that service them. Participants anticipated that surveillance would occur when they communicated with incarcerated relatives, but their understanding of the sophistication of some surveillance mechanisms was limited. They also believed that there were legal, practical, and technical barriers that limit the amount of surveillance they experienced. However, there are few legal protections for incarcerated people's communication [63], and the practical and technical barriers they anticipated are minimized by low-cost data storage and automated analysis. This work highlights the privacy challenges of communicating with incarcerated people, and the unique vulnerability of their families. We hope it serves as a call to action for the HCI, computer security/privacy, tech-policy, and other communities to critically examine the use of surveillance technology and consider ways of ameliorating harm within carceral systems.

ACKNOWLEDGMENTS

We would like to thank our study participants for making this work possible. We would like to thank Jay Aronson, The Pennsylvania Prison Society, Families Outside, the Prison Policy Initiative, and Abigail Marsh for supporting this study and its goals. We would also like to thank Sandy Kaplan, Os Keyes, the University of Washington Security & Privacy Lab, and our anonymous paper reviewers for their helpful feedback in the writing process. This project was supported in part by the CyLab Usable Privacy and Security (CUPS) Laboratory at Carnegie Mellon University and a gift from CyLab.

REFERENCES

[1] Tousif Ahmed, Roberto Hoyle, Patrick Shaffer, Kay Connelly, David Crandall, and Apu Kapadia. 2017. Understanding Physical Safety, Security, and Privacy Concerns of People with Visual Impairments. *IEEE Internet Computing* 21, 3 (2017), 56–63. https://doi.org/10.1109/MIC.2017.77

[2] Douglas Akney. 2019. Attorney-Client Privilege Under Attack in Jails Across the Nation. https://www.prisonlegalnews.org/news/2019/may/2/attorney-client-privilege-under-attack-jails-across-nation/

[3] Drug Policy Alliance. 2011. Mass Incarceration and Criminalization. http://www.drugpolicy.org/issues/mass-criminalization.

[4] The Internet Archive. 2001. Wayback Machine. https://web.archive.org/

[5] Joyce A. Arditti, Jennifer Lambert-Shute, and Karen Joest. 2003. Saturday Morning at the Jail: Implications of Incarceration for Families and Children*. *Family Relations* 52, 3 (2003), 195–204. https://doi.org/10.1111/j.1741-3729.2003.00195.x

[6] Ken Armstrong. 2015. A Phone Call From Jail? Better Watch What You Say. https://www.themarshallproject.org/2015/09/04/a-phone-call-from-jail-better-watch-what-you-say

[7] Jeanie Austin. 2019. Mechanisms of communicative control (and resistance): Carceral incorporations of ICT and communication policies for physical mail. https://doi.org/10.5210/fm.v24i3.9657

[8] Brooke Auxier, Lee Raine, Monica Anderson, Andrew Perrin, Madhu Kumar, and Erica Turner. 2019. Americans' attitudes and experiences with privacy policies and laws. https://www.pewresearch.org/internet/2019/11/15/americans-attitudes-and-experiences-with-privacy-policies-and-laws/

[9] Rebecca Balebako, Florian Schaub, Idris Adjerid, Alessandro Acquisti, and Lorrie Cranor. 2015. The Impact of Timing on the Salience of Smartphone App Privacy Notices. In *Proc. of the 5th Annual ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices* (Denver, Colorado, USA) *(SPSM '15)*. ACM, New York, NY, USA, 63–74. https://doi.org/10.1145/2808117.2808119

[10] Wanda Bertram. 2019. Victory for phone justice: Securus and ICSolutions abandon attempted merger. https://www.prisonpolicy.org/blog/2019/04/02/securus-ics-merger/.

[11] Honorable P. Kevin Brobson. 2019. Wishnefsky v. Pennsylvania Department of Corrections. http://www.pacourts.us/assets/opinions/Commonwealth/out/598CD19_11-8-19.pdf?cb=1.

[12] Simone Browne. 2015. *Dark matters: On the surveillance of blackness.* Duke University Press, Durham and London.

[13] William Bülow. 2014. The Harms Beyond Imprisonment: Do We Have Special Moral Obligations Towards the Families and Children of Prisoners? *Ethical Theory and Moral Practice* 17, 4 (Aug 2014), 775–789. https://doi.org/10.1007/s10677-013-9483-7

[14] Albert Fox Cahn, Esq. 2020. Listening Beyond the Bars: New York's Artificial Intelligence Surveillance of Prisoners and their Loved Ones. https://static1.squarespace.com/static/5c1bfc7eee175995a4ceb638/t/5f5ff0bd5b99c619be085e91/1600123069848/2020-9-15+Listening+Beyond+The+Bars.pdf

[15] Rahul Chatterjee, Periwinkle Doerfler, Hadas Orgad, Sam Havron, Jackeline Palmer, Diana Freed, Karen Levy, Nicola Dell, Damon McCoy, and Thomas Ristenpart. 2018. The spyware used in intimate partner violence. In *2018 IEEE Symposium on Security and Privacy (SP)*. IEEE, San Francisco, CA, USA, 441–458.

[16] Christine Chen, Nicola Dell, and Franziska Roesner. 2019. Computer Security and Privacy in the Interactions Between Victim Service Providers and Human Trafficking Survivors. In *28th USENIX Security Symposium (USENIX Security 19)*. USENIX Association, Santa Clara, CA, 89–104. https://www.usenix.org/conference/usenixsecurity19/presentation/chen

[17] Megan Comfort. 2007. Punishment beyond the legal offender. *Annu. Rev. Law Soc. Sci.* 3 (2007), 271–296.

[18] Smart Communications. 2018. Smart Communications Contract Redacted. https://cdn.muckrock.com/foia_files/2018/10/17/Smart_Communications_Contract_Redacted.pdf.

[19] Global Tel*Link Corporation. 2020. Privacy Policy. https://web.archive.org/web/20200521171846/https://web.connectnetwork.com/privacy-policy/.

[20] Allegheny County. 2020. Before Visiting Allegheny County Jail. https://www.alleghenycounty.us/jail/visitors/visitor-information.aspx

[21] Allegheny County. 2020. What You Can Send to an Inmate. https://www.alleghenycounty.us/jail/inmate-mail.aspx.

[22] Lorrie Faith Cranor, Adam L. Durity, Abigail Marsh, and Blase Ur. 2014. Parents' and Teens' Perspectives on Privacy In a Technology-Filled World. In *10th Symposium On Usable Privacy and Security (SOUPS 2014)*. USENIX Association, Menlo Park, CA, 19–35. https://www.usenix.org/conference/soups2014/proceedings/presentation/cranor

[23] Joel Currier. 2020. Prison phone calls lead to charges in 2017 double homicide in Carondelet neighborhood. https://www.stltoday.com/news/local/crime-and-courts/prison-phone-calls-lead-to-charges-in-2017-double-homicide-in-carondelet-neighborhood/article_8e5ab8a0-9d5b-5d22-b2b7-48e803551965.html

[24] Darren W. Davis. 1997. The Direction of Race of Interviewer Effects among African-Americans: Donning the Black Mask. *American Journal of Political Science* 41, 1 (Jan 1997), 309. https://doi.org/10.2307/2111718

[25] Zuri Davis. 2018. Pennsylvania's New $4 Million Prison Mail System Brings Privacy Concerns. https://reason.com/2018/10/10/pennsylvanias-4-million-prison-mail-scan/.

[26] Will Dobbie, Jacob Goldin, and Crystal S. Yang. 2018. The Effects of Pre-Trial Detention on Conviction, Future Crime, and Employment: Evidence from Randomly Assigned Judges. *American Economic Review* 108 (Feb 2018), 201–240. https://doi.org/10.1257/aer.20161503

[27] Paul Egan. 2020. U.P. prison inmate wrote complaint about conditions. Then he was moved to solitary. https://web.archive.org/web/20200413000934/https://www.freep.com/story/news/local/michigan/2020/02/11/chippewa-correctional-facility-michigan-prisoner-edward-walton/4721477002/

[28] Peter K. Enns, Youngmin Yi, Megan Comfort, Alyssa W. Goldman, Hedwig Lee, Christopher Muller, Sara Wakefield, Emily A. Wang, and Christopher Wildeman. 2019. What Percentage of Americans Have Ever Had a Family Member Incarcerated?: Evidence from the Family History of Incarceration Survey (FamHIS). *Socius* 5 (2019), 1–45. https://doi.org/10.1177/2378023119829332

[29] Sandra Feder. 2020. https://news.stanford.edu/2020/06/08/race-mass-criminalization-u-s/

[30] Chris Francescani. 2019. US prisons and jails using AI to mass-monitor millions of inmate calls. https://web.archive.org/web/20200525045330/https://abcnews.go.com/Technology/us-prisons-jails-ai-mass-monitor-millions-inmate/story?id=66370244

[31] Mary Anne Franks. 2017. Democratic Surveillance. *Harvard Journal of Law and Technology* 30 (2017), 425.

[32] Diana Freed, Jackeline Palmer, Diana Minchala, Karen Levy, Thomas Ristenpart, and Nicola Dell. 2018. "A Stalker's Paradise": How Intimate Partner Abusers Exploit Technology. In *Proc. of the 2018 CHI Conference on Human Factors in Computing Systems* (Montreal QC, Canada) *(CHI '18)*. Association for Computing Machinery, New York, NY, USA, 1–13. https://doi.org/10.1145/3173574.3174241

[33] Alisa Frik, Leysan Nurgalieva, Julia Bernd, Joyce Lee, Florian Schaub, and Serge Egelman. 2019. Privacy and Security Threat Models and Mitigation Strategies of Older Adults. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*. USENIX Association, Santa Clara, CA, 21–40. https://www.usenix.org/conference/soups2019/presentation/frik

[34] Elizabeth Gaynes. 2017. The Destructive Lie Behind "Mass Incarceration". https://time.com/4786379/the-destructive-lie-behind-mass-incarceration/

[35] Tamy Guberek, Allison McDonald, Sylvia Simioni, Abraham H. Mhaidli, Kentaro Toyama, and Florian Schaub. 2018. Keeping a Low Profile? Technology, Risk and Privacy among Undocumented Immigrants. In *Proc. of the 2018 CHI Conference on Human Factors in Computing Systems* (Montreal QC, Canada) *(CHI '18)*. Association for Computing Machinery, New York, NY, USA, 1–15. https://doi.org/10.1145/3173574.3173688

[36] Angela J Hattery and Earl Smith. 2014. Families of incarcerated African American men: The impact on mothers and children. *Journal of Pan African Studies* 7, 6 (2014), 128–153.

[37] Sam Havron, Diana Freed, Rahul Chatterjee, Damon McCoy, Nicola Dell, and Thomas Ristenpart. 2019. Clinical Computer Security for Victims of Intimate Partner Violence. In *28th USENIX Security Symposium (USENIX Security 19)*. USENIX Association, Santa Clara, CA, 105–122. https://www.usenix.org/conference/usenixsecurity19/presentation/havron

[38] Mike Hynes and Nick Jordan. 2019. How to Cure Prisons' Contraband Mobile Phone Epidemic. https://www.securitymagazine.com/articles/90543-how-to-cure-prisons-contraband-mobile-phone-epidemic.

[39] Prison Policy Initiative. 2019. Regulating the prison phone industry. https://www.prisonpolicy.org/phones/

[40] Prison Policy Initiative. 2020. Pennsylvania profile. https://www.prisonpolicy.org/profiles/PA.html.

[41] Rishi Iyengar. 2020. Apple's new iPhone ad puts privacy front and center again. https://madison.com/lifestyles/technology/apples-new-iphone-

ad-puts-privacy-front-and-center-again/article_afb6f614-f806-5036-8eea-993c3bfdd28e.html
[42] George Joseph and Debbie Nathan. 2019. Prisons Across the U.S. Are Quietly Building Databases of Incarcerated People's Voice Prints. https://theintercept.com/2019/01/30/prison-voice-prints-databases-securus/
[43] Mariame Kaba. 2020. Opinion | Yes, We Mean Literally Abolish the Police. https://www.nytimes.com/2020/06/12/opinion/sunday/floyd-abolish-defund-police.html
[44] Charles G. Koch and Mark V. Holden. 2015. The Overcriminalization of America. https://www.politico.com/magazine/story/2015/01/overcriminalization-of-america-113991.html
[45] Emily Lane. 2019. Tech Company Gave Two New Orleans-Area Sheriff's Offices Access to Track Cell Phones Without Warrants. https://theappeal.org/louisiana-sheriffs-securus/
[46] Victoria Law. 2018. How Companies Make Millions Charging Prisoners to Send An Email. https://www.wired.com/story/jpay-securus-prison-email-charging-millions/
[47] Ada Lerner, Helen Yuxun He, Anna Kawakami, Silvia Catherine Zeamer, and Roberto Hoyle. 2020. Privacy and Activism in the Transgender Community. In *Proc. of the 2020 CHI Conference on Human Factors in Computing Systems*. ACM, Honolulu, HI, U.S.A., 1–13. https://doi.org/10.1145/3313831.3376339
[48] M. Elena Lopez, Margaret Caspe, and Lorette McWilliams. 2016. Public Libraries: A Vital Space for Family Engagement. https://globalfrp.org/content/download/72/431/file/Public%20Libraries-A%20Vital%20Space%20for%20Family%20Engagement_HFRP%20PLA_%20August-2-2016.pdf
[49] David Lyon. 2003. *Surveillance as social sorting: Privacy, risk, and digital discrimination.* Routledge, London and New York.
[50] Mary Madden. 2017. Privacy, security, and digital inequality. https://datasociety.net/wp-content/uploads/2017/09/DataAndSociety_PrivacySecurityandDigitalInequality.pdf.
[51] Alex Marthews and Catherine Tucker. 2017. Government Surveillance and Internet Search Behavior. , 53 pages. http://www.ssrn.com/abstract=2412564
[52] Gary T. Marx. 2015. Surveillance Studies. , 733–741 pages. https://doi.org/10.1016/B978-0-08-097086-8.64025-4
[53] Thomas McMullan. 2015. What does the panopticon mean in the age of digital surveillance? https://www.theguardian.com/technology/2015/jul/23/panopticon-digital-surveillance-jeremy-bentham
[54] Jamila Michener and Julilly Kohler-Hausmann. 2017. Opinion | Why We Shouldn't Drug Test Poor People. https://www.nytimes.com/2017/06/28/opinion/drug-test-poor-medicaid-walker-trump.html
[55] Colin Miller. 2015. EvidenceProf Blog: Signed, Sealed, Delivered: The Different Prison Mail Policies of Different States. https://lawprofessors.typepad.com/evidenceprof/2015/02/as-a-result-ofyesterdays-post-i-started-doing-some-research-into-the-prison-mail-reading-policies-in-various-states-if-you.html
[56] Vincent M Nathan. 2001. Evaluation of the inmate grievance system. https://www.law.umich.edu/facultyhome/margoschlanger/Documents/Resources/Prison_and_Jail_Grievance_Policies/Ohio_Nathan_Evaluation_Grievance_System.pdf
[57] NCSL. 2020. Drug Testing for Welfare Recipients and Public Assistance. https://www.ncsl.org/research/human-services/drug-testing-and-public-assistance.aspx
[58] Kristen Nugent. 2015. GTL's Location IQ™ gives correctional facilities insight by pinpointing called party location. https://web.archive.org/web/20170715003108/https://www.gtl.net/gtls-location-iq-gives-correctional-facilities-insight-by-pinpointing-called-party-location/.
[59] PA Department of Corrections. 2020. Mail. https://www.cor.pa.gov:443/Pages/Mail.aspx.
[60] PA Department of Corrections. 2020. Video Visitation Program. https://web.archive.org/web/20200603124505/https://www.cor.pa.gov/family-and-friends/Pages/Video-Visitation.aspx.
[61] PA Department of Corrections. 2020. Visiting Rules. https://www.cor.pa.gov:443/family-and-friends/Pages/Visiting-Rules.aspx
[62] Federal Bureau of Prisons. 2020. BOP: Community Ties. https://www.bop.gov/inmates/communications.jsp
[63] Alameda County DA's Office. 2005. Intercepting Prisoner Communications. , 15–20 pages. https://le.alcoda.org/publications/point_of_view/files/IPC.pdf
[64] Information Commisioner's Office. 2020. Principle (c): Data minimisation. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/data-minimisation/
[65] Ihudiya Finda Ogbonnaya-Ogburu, Angela D.R. Smith, Alexandra To, and Kentaro Toyama. 2020. Critical Race Theory for HCI. In *Proc. of the 2020 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '20)*. Association for Computing Machinery, New York, NY, USA, 1–16. https://doi.org/10.1145/3313831.3376392
[66] Ihudiya Finda Ogbonnaya-Ogburu, Kentaro Toyama, and Tawanna R. Dillahunt. 2019. Towards an Effective Digital Literacy Intervention to Assist Returning Citizens with Job Search. In *Proc. of the 2019 CHI Conference on Human Factors in Computing Systems - CHI '19*. ACM, Glasgow, Scotland, UK, 1–12. https://doi.org/10.1145/3290605.3300315
[67] Pew Center on the States. 2011. State of recidivism: The revolving door of America's prisons. https://www.pewtrusts.org/~/media/legacy/uploadedfiles/wwwpewtrustsorg/reports/sentencing_and_corrections/staterecidivismrevolvingdooramericaprisons20pdf.pdf.
[68] Families Outside. 2020. About Wesley Family Services. https://wfspa.org/about/. Accessed: 2020-06-11.
[69] Jonathon W. Penney. 2016. Chilling Effects: Online Surveillance and Wikipedia Use. *Berkeley Technology Law Journal* 31, 1 (2016), 117–182. http://lawcat.berkeley.edu/record/1127413
[70] Sören Preibusch. 2015. Privacy behaviors after Snowden. *Commun. ACM* 58, 5 (2015), 48–55.
[71] Bernadette Rabuy and Daniel Kopf. 2015. Separation by Bars and Miles: Visitation in state prisons. https://www.prisonpolicy.org/reports/prisonvisits.html
[72] Bernadette Rabuy and Peter Wagner. 2015. Screening Out Family Time: The for-profit video visitation industry in prisons and jails. https://www.prisonpolicy.org/visitation/report.html.
[73] Stephen Raher. 2016. You've Got Mail: The promise of cyber communication in prisons and the need for regulation. https://www.prisonpolicy.org/messaging/report.html.
[74] Stephen Raher. 2017. The Wireless Prison: How Colorado's tablet computer program misses opportunities and monetizes the poor. https://www.prisonpolicy.org/blog/2017/07/06/tablets/
[75] Elissa M. Redmiles, Sean Kross, and Michelle L. Mazurek. 2017. Where is the Digital Divide? A Survey of Security, Privacy, and Socioeconomics. In *Proc. of the 2017 CHI Conference on Human Factors in Computing Systems* (Denver, Colorado, USA) *(CHI '17)*. Association for Computing Machinery, New York, NY, USA, 931–936. https://doi.org/10.1145/3025453.3025673
[76] Neil M. Richards. 2013. The Dangers of Surveillance. *Harvard Law Review* 126 (2013), 32.
[77] Matt Riley. 2017. Which states have the most smuggled prison cellphones? https://www.nbcnews.com/news/corrections/southern-prisons-have-smuggled-cellphone-problem-n790251.
[78] James E Robertson. 2009. " One of the Dirty Secrets of American Corrections": Retaliation, Surplus Power, and Whistleblowing Inmates. *University of Michigan Journal of Law Reform* 42, 3 (2009), 611–649.
[79] Alberto Romele, Camilla Emmenegger, Francesco Gallino, and Daniele Gorgone41. 2015. Technologies of Voluntary Servitude (TovS): a post–Foucauldian Perspective on Social Media. In *Proc. of the 2nd European Conference on Social Media 2015: ECSM 2015*. ECSM, Portugal, 377–382.
[80] Nick Rummell. 2019. Recorded Prison Calls May Be Used Against You, NY Court Rules. https://www.courthousenews.com/recorded-prison-calls-may-be-used-against-you-ny-court-rules/
[81] Leah Sakala. 2013. Return to Sender. https://www.prisonpolicy.org/postcards/report.html.
[82] Brenda K. Savage. 2016. Race-of-interviewer effects and survey questions about police violence. *Sociological Spectrum* 36, 3 (2016), 142–157. https://doi.org/10.1080/02732173.2015.1110508
[83] Wendy Sawyer and Peter Wagner. 2020. Mass Incarceration: The Whole Pie 2020. https://www.prisonpolicy.org/reports/pie2020.html
[84] P (Ed). Schofield. 2017. *The Correspondence of Jeremy Bentham, Volume 1.* UCL Press, London.
[85] Mirela Silva and Daniela Oliveira. 2020. Brazilian Favela Women: How Your Standard Solutions for Technology Abuse Might Actually Harm Them. , 6 pages.
[86] Lucy Simko, Ada Lerner, Samia Ibtasam, Franziska Roesner, and Tadayoshi Kohno. 2018. Computer Security and Privacy for Refugees in the United States. In *2018 IEEE Symposium on Security and Privacy (SP)*. IEEE, San Francisco, CA, USA, 409–423.
[87] Jordan Smith and Micah Lee. 2015. Not So Securus: Massive Hack of 70 Million Prisoner Phone Calls Indicates Violations of Attorney-Client Privilege. https://theintercept.com/2015/11/11/securus-hack-prison-phone-company-exposes-thousands-of-calls-lawyers-and-clients/
[88] Pennsylvania Prison Society. 2020. WHO WE ARE | paprisonsociety. https://www.prisonsociety.org/about_us. Accessed: 2020-06-11.
[89] Securus Technologie. 2020. "Moniteau County Sheriff's Office Saves Time and Manpower With Securus Technologies' Guarded Exchange". https://web.archive.org/web/20200526205257/https://www.officer.com/command-hq/corrections/press-release/21129664/securus-technologies-moniteau-county-sheriffs-office-saves-time-and-manpower-with-securus-technologies-guarded-exchange
[90] Aventiv Technologies. 2019. Privacy and Data Processing Policy. https://web.archive.org/web/20200519044230/https://www.aventiv.com/privacy/
[91] GTL Technologies. 2014. Contract Between Commonwealth of Pennsylvania Department of Corrections and Global Tel*Link, Contract No. AGR-13-346_2014. https://www.patreasury.gov/transparency/e-library/ContractFiles/285767_Corrected%20Treasury%20Contract%20Link%204400013765%20Kiosk%20RFP.pdf

[92] GTL Technologies. 2016. GTL/ConnectNetwork.com Services Available at the PA DOC. https://www.gtl.net/pa-doc-inmate-services-by-gtl/
[93] GTL Technologies. 2020. ConnectNetwork Help | FAQ about our services and features. https://web.connectnetwork.com/help/.
[94] GTL Technologies. 2020. Inmate Telephone Systems | GTL. https://www.gtl.net/correctional-facility-services/communication-solutions/inmate-telephone-systems/.
[95] GTL Technologies. 2020. MyApps.GTL.Us Overview. https://myapps.gtl.us/SSO.Help/myapps.gtl.us_overview.htm.
[96] Securus Technologies. 2019. Privacy - Securus Technologies 2019. https://web.archive.org/web/20190504193725/https://securustech.net/privacy/index.html.
[97] Securus Technologies. 2020. Securus Video ConnectSM. https://securustechnologies.tech/corrections/communication/video-visitation/.
[98] Securus Technologies. 2020. Securus Video Visitation: A Better Way To Visit. https://securustechnologies.tech/wp-content/uploads/2018/08/Securus-Video-Visit.pdf.
[99] Securus Technologies. 2020. Securus Video Visitation Tutorial. https://www.tcsheriff.org/inmate-jail-info/video-tutorial.
[100] Securus Technologies. 2020. TDCJ. https://securustech.net/tdcj/index.html.
[101] Securus Technologies. 2020. Telephone Service. https://securustechnologies.tech/corrections/communication/telephone-service/.
[102] David R. Thomas. 2006. A General Inductive Approach for Analyzing Qualitative Evaluation Data. *American Journal of Evaluation* 27, 2 (Jun 2006), 237–246. https://doi.org/10.1177/1098214005283748
[103] Jeremy Travis and Michelle Waul. 2003. *Prisoners once removed: The impact of incarceration and reentry on children, families, and communities.* The Urban Insitute, Washington, DC, USA.
[104] Sanne Verbaan, Clair Aldington, Roisin McNaney, and Jayne Wallace. 2018. Potentials of HCI for Prisons and Incarcerated Individuals. In *Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems*. ACM, Montreal, QC, Canada, 1–4. https://doi.org/10.1145/3170427.3185367
[105] Peter Wagner. 2015. Jails matter. But who is listening? https://www.prisonpolicy.org/blog/2015/08/14/jailsmatter/
[106] Peter Wagner and Alexi Jones. 2019. State of Phone Justice. https://www.prisonpolicy.org/phones/state_of_phone_justice.html
[107] Peter Wagner and Wendy Sawyer. 2018. States of Incarceration: The Global Context 2018. https://www.prisonpolicy.org/global/2018.html
[108] Shoshana Zuboff. 1988. *In the age of the smart machine.* Basic Book, New York City.

A APPENDIX

A.1 Interview protocol

Our study used semi-structured interviews, meaning that the below script served as a guide for the interviews. When relevant, we deviated from the script and followed up on statements made by participants and also skipped questions that were irrelevant.

General Questions

- Tell me about the most recent time you talked to your relative. What general topics did you talk about?
- For each communication method that you use, could you explain why you use it (and how)? Do you prefer using one method over another? What are some good things and bad things about the communication methods you use?
- What general topics do you typically discuss when communicating with your incarcerated relative? What type of sensitive information, if any, do you discuss? [Choose from the following: concerns about conditions inside the prison, concerns about treatment from prison staff, concerns about their legal support, events leading up to their incarceration, other topics]
- Think about a time when you wanted to discuss something but choose not to. Did concerns about your method of communication influence that decision?
- Do you have any problems/concerns with your communication methods? What do you think the prison/jail, policy makers, or computer science researchers could do to help address these concerns?

Perceptions of surveillance We ask similar questions for each communication method a participant used. For brevity, we include the portion relevant to phone calls.

- *Identification:* Do you think the prison/jail knows who you are when you the phone? How might they identify you? Do you think they associate your name with this method? Do you think they use characteristics of your voice to identify you?
- *Surveillance:* Do you think your phone calls are monitored live? Who do you think is monitoring them? Why do you think they might be monitored?
- *Collection:* Do you think they keep records of what you discuss over the phone? If so, what kinds of records do you think they might keep (e.g., transcript, audio recording)?
- *Use:* How do you think they use any records they might keep? Why? Do you think your relative could be negatively impacted by anything you say? Who do you think has access to these records?
- *Retention:* How long do you think records are kept? Do you think the records are destroyed after your relative leaves prison? Do you feel like you have any control over these records?
- *If the facility's phone vendor is GTL Technologies:* Do you think your device's location is being tracked whenever you call your relative? How long do you think your location is being tracked after you pick up the call? Do you think any information is being collected about when you use a kiosk? What information do you think is being collected when you use the mobile application?

Miscellaneous final questions

- If you found out that the following practices were being used at your relative's prison/jail, how would that make you feel? [Geo-location after answering the phone, pictures taken a kiosk without being alerted]
- Do you use any of these communication methods with any children under the age of 13?
- What does privacy mean to you, in the context of communication with your incarcerated relative(s)? What actions, if any, do you take to protect your privacy?
- What communication method do you feel most protects your privacy?
- Are there things that could change the way you communicate with your incarcerated relative that would improve the privacy of that communication?
- What drew you to participate in this study?
- We only have a few minutes left; is there anything else you want to discuss before the interview is over?

A.2 Codes used for qualitative analysis

Communication practices

- Mentioned an obligation to stay in touch
- Has personal circumstances affection communication
- Described the type of topics discussed with incarcerated relative

- Described topics not discussed because they could agitate or sadden incarcerated relative

Awareness of Surveillance & Privacy Risks

- Brought up privacy/surveillance without being prompted

Learning about surveillance properties

- Described how they learned about surveillance practices

Limits of surveillance

- Believe something is not possible because of technical limits
- Mention that data storage capacity limits amount of data stored about them
- Mentioned slang or poor audio quality would make surveillance challenging
- Believed a warrant or court order is necessary for police/non-prison agencies to access data
- Indicated that only "really bad" people warrant the most invasive surveillance

Understandings about specific communication methods

- Believed data is retained after leaving jail
- Did not believe voice printing was in use
- Did not believe location was tracked
- Thought someone might be listening to call (live or recorded)
- Thought call is recorded
- Believed the letter is unopened before being received by incarcerated relative
- Believed the letter contents are read by a human (besides relative)
- Believed the letter is somehow saved (e.g., scanned or photocopied and the copy saved)
- Believed that letters sent by their incarcerated family member are opened and/or read before reaching them
- Thought guards pay attention to their physical behavior during in-person visitation
- Mentions surveillance from guards you can't see
- Thought guards try to listen in on their in-person conversations
- Thought other visitors might listen in on their conversations

Reactions to Surveillance

- Acknowledged a possible repercussion due to surveillance
- Expressed unease about surveillance practices
- Expressed unease about surveillance practices despite doing nothing wrong
- Described why facilities might conduct surveillance
- Believed surveillance is unfair to them
- Avoided a topic for privacy reasons
- Used euphemisms/nicknames when communicating
- Chose a communication method for privacy reasons
- Mentioned that strategies for protection against other threats
- Felt they have no power to preserve privacy
- Prioritized something else over privacy

Miscellaneous codes

- Thought keyword search is used for mail and/or audio data
- Mentioned recorded notices on phone
- Was formerly incarcerated
- Thought mail is swabbed for chemicals
- Described reason they do not use video visitation
- Believed facilities' staff do not follow their policies

A.3 Online recruitment text

The following text was included in emails and forum posts that we used to recruit participants:

Carnegie Mellon Study on Prisons and Communication We're recruiting adults to participate in an interview study about prisons and communication with their incarcerated relatives (grandparent, parent, child, grandchild, sibling, cousin, partner or spouse). We're looking for people who currently have an adult relative in a Pennsylvania prison. This study involves a 60 minute interview at Carnegie Mellon's campus or in a private meeting room at a public library near you. If you participate in the interview, you will be compensated $30 cash. Please complete a short screening survey at [https://bit.ly/PrisonStudy] so we can determine if you are eligible. If you are eligible, one of our researchers will reach out to you about next steps.

A.4 Screening survey instrument

[Logo for our institute, which mentions security and privacy ("Carnegie Mellon University CyLab Security and Privacy Institute")] Study on Privacy and Prisons

Please complete this short screening survey which will help us determine if you are eligible for our Prison Communication Study.

[Online recruitment text repeated]

(1) What is your name? *[Free response]*
(2) Do you have a close adult relative (grandparent, parent, child, sibling, cousin, partner or spouse) currently in prison/jail in Pennsylvania? *[Select one: Yes, No, Other (with free response)]*
(3) Is this person a primary relative (spouse, partner, parent, son/daughter, sibling), secondary relative (cousin, grandparent, grandchild) or another type of relative? *[Select one: Primary relative, Secondary relative, Other]*
(4) Which prison/jail (name, city)? *[Free response]*
(5) Approximately how long have they been in prison/jail (in days, weeks, months, or years)? *[Free response]*
(6) How do you communicate with them? *[Select multiple: Phone, Physical Mail, Video conferencing, In-person visitation, Email, Other (with free response)]*
(7) How frequently do you communicate with them? *[Select one: A few times a day, A few times a week, A few times a month, A few times a year, Once a year, Other (with free response)]*
(8) What is your age? *[Select from dropdown]*
(9) What is your gender? *[Select one: Type here (with free response), I prefer not to answer]*
(10) What is your race/ethnicity? *[Select one: Type here (with free response), I prefer not to answer]*
(11) What is the highest degree you have earned? *[Select one: No high school diploma, High school diploma/GED, Some college but no degree, Associate degree, Bachelor degree, Professional degree (e.g. master's/PhD/medical/law), I prefer not to answer]*
(12) How would you describe your level of comfort/experience with computers? *[Select one: High, Medium, Low]*
(13) If you are eligible for the interview, how would you like us to contact you? *[Select one: Email (enter email address), Phone (enter phone number), Other]*
(14) When is a good time to call? *[Select one: Mornings, Around Noon, Afternoons, Evenings, Other (free response)]*

A.5 Example handout for advocacy groups

Advocacy groups (like some of the organizations we connected with for recruitment) are especially well-positioned to distribute educational materials related to surveillance risks and practices at local carceral facilities. Rather than merely suggest that they create such materials, we prepared an example handout based on our understanding of practices at one of the facilities in Pennsylvania. A digital copy of this handout can be found at https://tinyurl.com/ACJ-flyer.

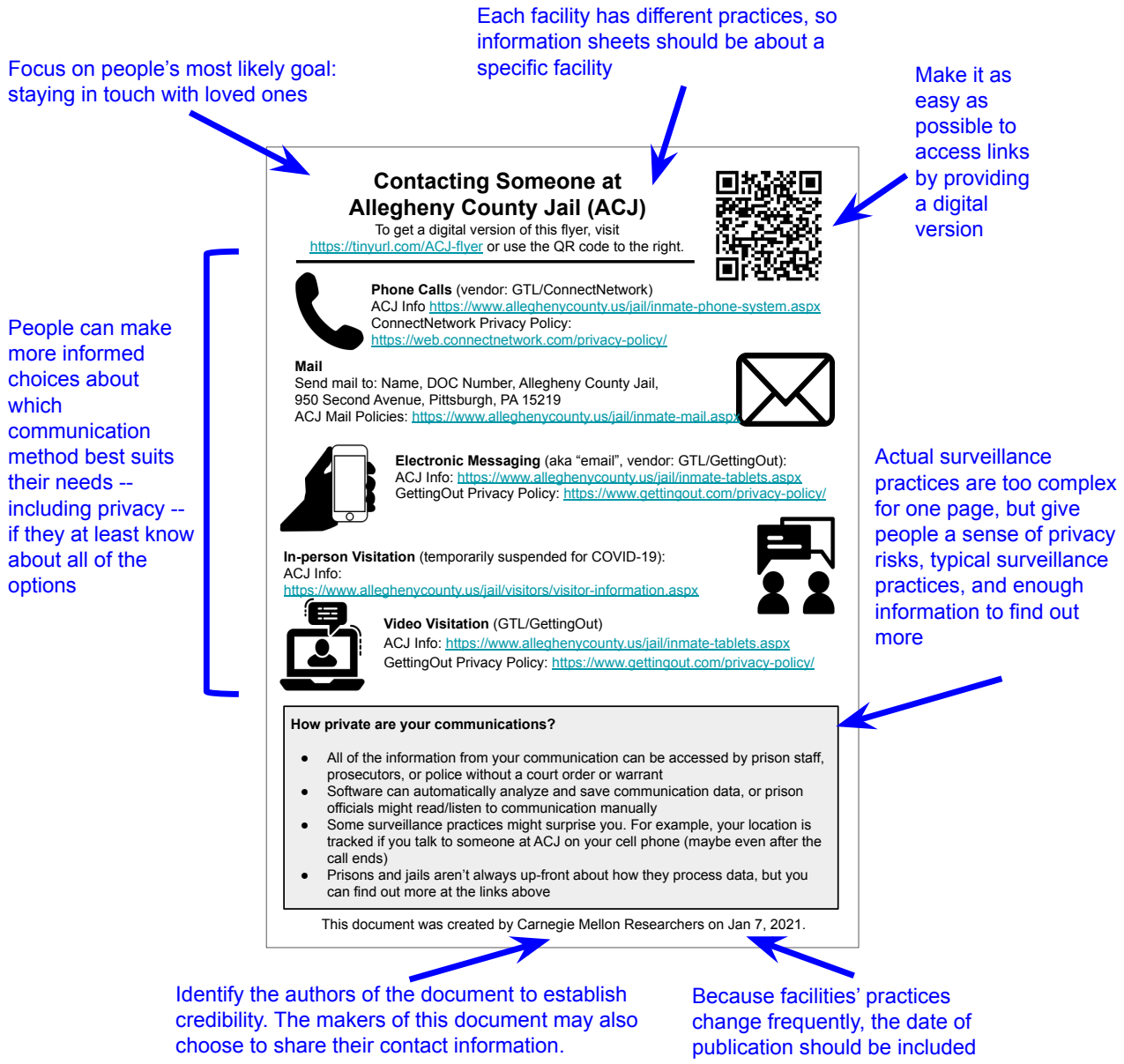

Figure 1: A diagram of the handout we created with pointers to key information to include when designing such a document.