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

Kentrell Owens, University of Washington
Camille Cobb, Carnegie Mellon University
Lorrie Cranor, Carnegie Mellon University

Twitter: @KentrellOwens
Incarcerated people’s communication is surveilled

- U.S. leads the world in incarceration
- Facilities use advanced surveillance tech
- Potentials harms of surveillance
- Families MUST undergo surveillance to communicate with incarcerated relatives

Source: International Center for Prison Studies, UK
Notable Surveillance Mechanisms

Tech Company Gave Two New Orleans–Area Sheriff’s Offices Access to Track Cell Phones Without Warrants

Neither agency had written policies on how to capture or store the location data without violating privacy rights.

Prisons Across the U.S. Are Quietly Building Databases of Incarcerated People’s Voice Prints

The voice-print technology allows authorities to mine call databases and cross-reference the voices of individuals prisoners have spoken with.

Prison Mail Surveillance Company Keeps Tabs On Those On the Outside, Too

Prisons are increasingly copying mail to prevent contraband, but this means prisoners never get to hold letters and photos from loved ones. One company goes even further.
What privacy concerns and preferences do FMIP have when they use prison communication services? How do they react to surveillance?

Interviewed 16 family members of people incarcerated in Pennsylvania (December 2019)

Asked about their perceptions of data collection, retention, & use and surveillance/privacy
Findings
Communication Practices

- People feel an obligation to stay in touch with incarcerated relatives.
- This communication can be inconvenient and costly.

“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.” -- P12
High awareness of surveillance …

… but assumptions, policies, practices may not align

- Brought up surveillance unprompted
- Believed some surveillance mechanisms were not possible
- Prison staff might not follow policies around surveillance (E.g., reading mail without approval)

“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

“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.” -- former CO
People raised harms of surveillance

- Expressed concern that their words could be manipulated against them or their incarcerated relative
- Thought it was unfair
- Half of participants believed data was collected for prosecution
  - 7 mentioned safety reasons
- Mentioned the harms of “false positives”
  - E.g., drugs detected during in-person visit
- Discomfort being in a facility

“... there is a lot of communication [discussing] the judicial system between the person and then their family ... 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.” -- P12
People described their privacy-preserving strategies

- Using the “most private communication method”
  - Thought physical mail was the most private, followed by in-person visitation
- Self-censorship of case details/names
- No strategy

Re: location tracking: “[I would feel like I] was under heavy monitoring, and 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” -- P12
Recommendations from participants

“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.” -- P12
Findings summary

- Participants believed that there were legal, practical, and technical barriers that limited surveillance
- Concerns about fairness
- Concerns about misrepresentation of their words
- Mentioned privacy-preserving strategies
  - Using the “most private” communication method, self-censorship
- Raised numerous other, non-surveillance/privacy related issues
  - E.g., cost, convenience, accessibility, prior trauma in prisons
Discussion
Prison communication companies design products to work for facilities, not for the people that use their services.
Surveillance of communication contributes to incarceration.
Recommendations for end-users

Use the most private communication method
Recommendations for policy makers

- **Minimize data collection**
  - Mass data collection makes systems vulnerable to massive hacks

- **Increase access to data controls**
  - Specifically for the purpose of data deletion (e.g., after someone leaves a facility)

- **Require disclosure of surveillance practices**
  - Information buried in FOIA’d contracts, privacy policies and news articles
Focus on people’s most likely goal: staying in touch with loved ones.

People can make more informed choices about which communication method best suits their needs -- including privacy -- if they at least know about all of the options.

Identify the authors of the document to establish credibility. The makers of this document may also choose to share their contact information.

Each facility has different practices, so information sheets should be about a specific facility.

Make it as easy as possible to access links by providing a digital version.

Actual surveillance practices are too complex for one page, but give people a sense of privacy risks, typical surveillance practices, and enough information to find out more.

Because facilities’ practices change frequently, the date of publication should be included.

Contacting Someone at Allegheny County Jail (ACJ)

To get a digital version of this flyer, visit https://tinyurl.com/ACJ-flyer or use the QR code to the right.

---

Phone Calls (vendor: GTL/ConnectNetwork)
ACJ Info: https://www.alleghehnycounty.us/jail/inmate-phone-system.aspx

Mail
Send mail to: Name, DOC Number, Allegheny County Jail, 550 Second Avenue, Pittsburgh, PA 15219
ACJ Mail Policies: https://www.alleghehnycounty.us/jail/inmate-mail.aspx

Electronic Messaging (aka “Email” vendor: GTL/GettingOut)
ACJ Info: https://www.alleghehnycounty.us/jail/inmate-tablets.aspx

In-person Visitation (temporarily suspended for COVID-19)
ACJ Info: https://www.alleghehnycounty.us/jail/visitors/visitor-information.aspx

Video Visitation (GTW/GettingOut)
ACJ Info: https://www.alleghehnycounty.us/jail/inmate-tablets.aspx

How private are your communications?
- All of the information from your communication can be accessed by prison staff, prosecutors, or police without a court order or warrant
- Software can automatically analyze and save communication data, or prison officials might read/listen to communication manually
- Some surveillance practices might surprise you. For example, your location is tracked if you talk to someone at ACJ on your cell phone (maybe even after the call ends)
- Prisons and jails aren’t always up-front about how they process data, but you can find out more at the links above

This document was created by Carnegie Mellon Researchers on Jan 7, 2021.
Implications for privacy engineers

- Considering marginalized groups’ threat models
  - End-users might (unbeknownst to you) consider government entities as their adversaries
    - E.g., smartphone probation/parole monitoring apps
- Technology you make could be (mis)used to further marginalization
  - Securus made an app that gave real time location access to any phone number to people who “uploaded proper legal documents”
  - People uploaded fake documents to bypass the warrant process
- Diversify your teams
  - “Race of interviewer” effect has been shown to have an impact when people are interviewed about police violence [24, 65, 82]
- Thank you for your time!
“You Gotta Watch What You Say”: Surveillance of Communication with Incarcerated People

Kentrell Owens, University of Washington
Camille Cobb, Carnegie Mellon University
Lorrie Cranor, Carnegie Mellon University

Email: kentrell@uw.edu
Twitter: @KentrellOwens
Link to the paper