# Trial by File Formats: Exploring Public Defenders' Challenges Working with Novel Surveillance Data

RACHEL B. WARREN, University of California, Irvine, School of Information & Computer Sciences, USA
NILOUFAR SALEHI, University of California, Berkeley, School of Information, USA

In the United States, public defenders (lawyers assigned to people accused of crimes who cannot afford a private attorney) serve as an essential bulwark against wrongful arrest and incarceration for low-income and marginalized people. Public defenders have long been overworked and under-resourced. However, these issues have been compounded by increases in the volume and complexity of data in modern criminal cases. We explore the technology needs of public defenders through a series of semi-structured interviews with public defenders and those who work with them. We find that public defenders' ability to reason about novel surveillance data is woefully inadequate not only due to a lack of resources and knowledge, but also due to the structure of the criminal justice system, which gives prosecutors and police (in partnership with private companies) more control than defense attorneys over the type of information used in criminal cases. We find that public defenders may be able to create fairer situations for their clients with better tools for data interpretation and access. Therefore, we call on technologists to attend to the needs of public defenders and the people they represent when designing systems that collect data about people. Our findings illuminate constraints that technologists and privacy advocates should consider as they pursue solutions. In particular, our work complicates notions of individual privacy as the only value in protecting users' rights, and demonstrates the importance of data interpretation alongside data visibility. As data sources become more complex, control over the data cannot be separated from access to the experts and technology to make sense of that data. The growing surveillance data ecosystem may systematically oppress not only those who are most closely observed, but groups of people whose communities and advocates have been deprived of the storytelling power over their information.



CCS Concepts: • **Security and privacy → Social aspects of security and privacy**; • **Human-centered computing → Empirical studies in collaborative and social computing**; • **Social and professional topics → Governmental surveillance**.

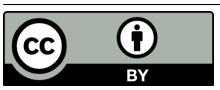
Additional Key Words and Phrases: criminal justice, social-technical systems, digital trace data, privacy

**ACM Reference Format:**
Rachel B. Warren and Niloufar Salehi. 2022. Trial by File Formats: Exploring Public Defenders' Challenges Working with Novel Surveillance Data. *Proc. ACM Hum.-Comput. Interact.* 6, CSCW1, Article 67 (April 2022), 26 pages. https://doi.org/10.1145/3512914

## 1 INTRODUCTION

With the advent of cheap data storage and the rapid rise of digital communications, the amount of information recorded about Americans by private companies and the government increases every year. Phones, CCTV cameras, license plate readers, and computers record our movements,

Authors' addresses: Rachel B. Warren, rwarren2@uci.edu, University of California, Irvine, School of Information & Computer Sciences, , Berkeley, California, USA, ; Niloufar Salehi, nsalehi@berkeley.edu, University of California, Berkeley, School of Information, , Berkeley, California, USA, .




2573-0142/2022/4-ART67
https://doi.org/10.1145/3512914

associations, and communication. At the same time, the criminal justice system has failed to shrink.[1] Inevitably, the ocean of novel surveillance data seeps into the criminal justice system: it directs law enforcement decisions, it is used to prosecute, and occasionally it is leveraged to acquit.[2] Although an increase in the amount of data available to law enforcement and in the courtroom could make a notoriously biased system more fair, many worry that the rise in surveillance data enables the arrest and control of our society's most vulnerable people [13, 24, 26, 28]. It is clear from previous research that proactive surveillance from law enforcement drives arrests, and that how data is used in criminal proceedings can have a profound impact on case outcomes [18, 39, 61]. As we embrace growing concern in the HCI community about the implications of design on issues of social justice [13, 20, 27, 50], it is our responsibility to consider how the technologies we create and study have an out-sized impact on people confronted with criminal charges and how they are able to defend themselves.

Public defenders (PDs), lawyers who defend indigent people people charged with crimes, play a unique and often overlooked role in the American criminal justice system. The vast majority of criminal defendants, and all defendants who meet locally defined poverty qualifications, are represented by public defenders [38]. Although public defenders are state employees with nominal access to much of the same surveillance data as law enforcement, they have the power to present an alternative narrative from or about the data collected by police, private companies, and federal agencies. In this way, the public defender can be seen as a critical bulwark between a poor person charged with a crime and the most consequential harms of state surveillance. Public defenders do not just prevent conviction and incarceration—they advocate against longer sentences, higher fines, pretrial detention, and a lasting criminal record. However, PDs' ability to protect their clients hinges upon their ability to adequately access, parse, and reason about the data used before and during trial. Consequently, targeted solutions to help public defenders may be an important way to protect the civil liberties of their indigent clients. Furthermore, examining the challenges public defenders face working with technology is a useful way of studying harms associated both with digital surveillance and with existing inequalities in the criminal justice system.

Through a series of open-ended interviews with public defenders—and the paralegals and investigators who work with them—we explore the types of surveillance data that public defenders encounter, the challenges they face accessing and working with that data, and how these challenges impact the representation PDs can provide. In addition to open-ended questions, the interviews also include a structured interview component designed to solicit technical pain points experienced by participants and to encourage them to walk us through their process of using technology. We use the grounded theory method to analyze our data, and we focus on generating insights about different technologies and situations which impede representation [17].

We find that public defenders uniformly felt that lack of time, lack of technical resources, and lack of technical knowledge impacted their ability to process surveillance data used throughout criminal proceedings, and consequently undermined their legal defense. The primary disadvantage public defenders felt they experienced relative to prosecutors was structural; PDs have little control over the format and volume of data used in the cases against their clients. Furthermore, public defenders

[1]Despite widespread calls for reform, the American criminal justice system remains the largest in the world. Law enforcement officers make ten million felony arrests [19] and thirteen million misdemeanor arrests [52] each year. Those arrested are disproportionately people of color [74].

[2]The criminal justice system consists of three branches: law enforcement, the courts (including prosecutors, defense attorneys, and judges), and the corrections system. Each branch operates at different geographic levels called jurisdictions. Though everyone accused of a crime will go through criminal proceedings (often a hearing between attorneys in the presence of a judge), very few cases actually go before a jury trial. See https://bjs.ojp.gov/media/image/45506 for a useful visual aid.

believe that prosecutors have superior capacity for the de-facto summarizing and sense-making of that data due to their ability to partner with private companies and federal institutions like the Federal Bureau of Investigation (FBI) and Department of Justice (DOJ). In this time-constrained and high-stakes work, seemingly minute details about data storage and delivery are critical. Public defenders' relative lack of power in shaping the way information enters the courtroom seems to have significant consequences for their clients.

Our findings demonstrate that explicitly considering the needs of public defenders, and by extension the impact of surveillance data on the criminal justice system, should be an acute concern for technology producers and designers, especially those who are responsible for the production and storage of digital trace data.[3] We also reinforce the importance of community participation in the design of (and resistance to) public technological systems which can be used for surveillance [4, 78]. In the near future, we see opportunities for the HCI community to consider designing systems to assist public defenders, taking as inspiration participatory design projects such as Strohmayer's participatory work creating tools to support sex workers and the collaboration of Freed et al. with victims of intimate partner violence to identify security flaws in mobile technology [29, 70].

However, we caution that while poorly designed technology adversely impacts the criminal justice system, the power disparities and bias which our work highlights are unlikely to be solved by technical means alone. More broadly, this case study shows the limitations of the "notice and choice" privacy regime, which considers individual privacy as a primary axis for evaluating the potential harms of an information technology.[4] Our work adds to calls within the HCI, STS, and legal literature for considering problems of interpretation and impact above simple questions of visibility when discussing the harms of surveillance. Though we advocate for regulations limiting law enforcement's ability to seek out data from third parties and purchase new surveillance systems [39, 78], we also find that justice requires that more tools of interpretation be made available and that parity in data access for public defenders be prioritized. We argue that the most oppressive regime is not necessarily the one with the most information, but one that has a monopoly on constructing the narratives from that information which will define its citizens' freedoms and choices.

## 2 BACKGROUND: WHO ARE PUBLIC DEFENDERS?

### 2.1 Public Defenders

Public defenders—or "indigent defense counsel"—represent clients who are charged with crimes and are otherwise unable to acquire legal representation, thus fulfilling poor clients' Sixth Amendment right to legal counsel. Most people charged with felonies rely on publicly funded defense: 80% of defendants in most local and county jurisdictions and 66% of federal criminal defendants qualify, according to one analysis [38]. Despite its constitutional importance and widespread use, the indigent

[3] Digital trace data is the record of our behaviors and activities generated by using network technologies, e.g., browsing history and location data.

[4] The current privacy paradigm in the U.S., often called "notice and choice," generally holds data-gathering entities accountable only for disclosing their data collection practices, and leaves individuals with the responsibility to decide to whom they disclose their personal information [63].

defense system is relatively new,[5] heterogeneously administered,[6] and poorly monitored. There is no national reporting requirement for public defense offices as there is with police departments [51], making comprehensive statistics about the system extremely difficult to find.[7] Further, public defenders, who are full-time employees of the government and serve only indigent clients, are just one of three forms of indigent representation. Indigent clients can also be represented by attorneys contracted by the government for a period of time (contract-service systems) or private attorneys assigned by the government (an assigned-counsel system). On average, the most populous counties nationwide are able to provide about 80% of indigent criminal defendants with representation from full-time public defenders. By contrast, at the federal level, only a quarter of defendants are represented by a federal public defender [38].

The indigent defense system and public defense offices are notoriously underfunded. A comprehensive survey of public defense offices found that 70% of public defense offices exceeded the generous recommended case limit of 400 misdemeanors or 150 felonies per attorney per year [25]. At least one analysis suggests that under-funding public defense offices may actually *increase* costs in the criminal justice system by expanding expensive (and civil liberty-violating) pretrial incarceration [30]. Every year, horror stories from particular jurisdictions emerge—for example, defendants in Florida have been found to wait for as many as nine months in jail before being assigned an attorney [12, 32, 43, 58]. Although it is difficult to compare outcomes for indigent defendants with outcomes for those who can afford a private attorney, it is clear that the quality of representation impacts outcomes for poor defendants. It also seems that the public defender system is more effective than the assigned-counsel or contract-services systems. A 2012 analysis found that the 20% of murder defendants in Philadelphia who were randomly assigned public defenders, rather than assigned counsel working outside a public defense office, were significantly less likely to be convicted of a crime (19% reduction) and less likely to receive a life sentence (60% reduction) [3].[8] Anderson and Heaton attribute this difference to public defenders' ability to prepare more for a case, collaborate with each other, and leverage in-office investigative resources [3]. Although not possible to study causally, it seems likely that these findings may be extrapolated to differences in representation between public defense offices, and that public defenders with more time and resources are able to achieve better outcomes for their clients. Our analysis focuses on the needs of full-time public defenders. However, we expect other attorneys performing indigent defense have similar, if not greater, challenges.

### 2.2 How Public Defenders Receive Surveillance Data

In this section we will provide an overview of the rules of evidence in the U.S. court system. There are two primary sources of surveillance data which public defenders encounter. First, data is captured directly by state actors, often for the purpose of law enforcement, through systems such as license plate readers, body cameras, surveillance cameras (in public spaces like parks and public housing departments), drone footage, gunshot detection systems (e.g., ShotSpotter), and

[5]The Sixth Amendment requires that any individual convicted of a crime "have the Assistance of Counsel for his defence". However, until the landmark case Gideon v. Wainwright, 372 U.S. 335 (1963), states had the right to decide which crimes required counsel. After Gideon, all defendants facing criminal charges were entitled to government-appointed attorneys, catalyzing the development of public defense offices around the country meant to "mirror" the role of the public prosecutor (DA).

[6]In 23 states (mostly small states in the Midwest and West), public defense is handled at the state level, while in the remaining 27 states, public defense offices are administered at the county and local level—although some of these states have state public defenders who handle capital (death penalty) cases [25, 42].

[7]The best data currently is a census of public defender offices compiled by the Bureau of Justice Statistics in 2010 [25, 42].

[8]The significance and direction of these findings, although not the magnitude, was replicated for multiple felony defendants in San Francisco [65].

an ever-expanding set of forensics and bio-identification technologies which are purchased and administered by police departments, municipalities, and federal law enforcement agencies. Second, law enforcement has relatively easy access to a growing wealth of digital trace data generated by private companies, including call records, social media data, GPS data, and privately collected surveillance video. In both instances, data is usually collated by prosecutors, often in partnership with law enforcement and private companies, before prosecutors pass it to defense counsel as a collection of data called "discovery". Discovery is an electronic or paper packet which is supposed to contain all the information that prosecutors plan to present in the case as well as any known exculpatory information.

Prosecutors can request any relevant data from law enforcement, and few rules or procedures restrict the flow of information between law enforcement and prosecutors.[9] Prosecutors and defenders can access data using a subpoena (described below). There are two legal instruments for acquiring data from private companies:

- **Subpoenas:** A subpoena for records—a *subpoena duces tecum*—can be issued by any lawyer on behalf of the court. To issue a subpoena, one must only provide a description of the records requested and how they are relevant. Subpoenas do not require review by a judge. Failure to respond to a subpoena can convey legal penalties, although they are not always enforced. Under the third-party doctrine, most information that an individual willingly gives to a third party can be requested with a subpoena.[10]
- **Search Warrants**: Search warrants are meant to cover a higher standard of evidence than subpoenas. They are issued by a court on behalf of law enforcement, who must present evidence that there is "probable cause" that a crime has been committed and that the search material will reveal the evidence of that crime. In practice, sworn testimony from law enforcement is usually sufficient to establish probable cause.[11] Lawyers do not issue search warrants.

## 3 RELATED WORK

### 3.1 Surveillance Data and the Criminal Justice System

A rich body of historical literature discuses the difficulty of translating science and data into law [48, 73], and the potential of that data to perpetuate racial inequality [2]. Since the information technology revolution, scholars have documented how digital data—and a host of algorithms used to categorize people from that data—can exacerbate the problems of older technologies and wrongfully criminalize the poor [10, 26, 47, 50, 60].

Surveillance data collected by public agencies as well as private companies is not just used to bolster cases investigated by other means; cases are also often opened as a result of active surveillance [44]. For example, in a survey of gang task forces, Patton et al. found that 40% of criminal investigations begin as a result of monitoring social media [60]. Interviews with law enforcement focused on human trafficking reveal that many investigations of human trafficking begin as a result of proactive social media monitoring [18]. More complex surveillance technologies also drive arrests: predictive policing algorithms use historical data to direct police patrols to the same historically policed areas [6, 49, 64], and ShotSpotter sensors trigger police to come to the scene and are enough to justify a search [35]. Three observations from this scholarship are

[9] See: https://www.law.cornell.edu/wex/brady_rule.

[10] The most notable exception is information protected by the Stored Communications Act (SCA), 18 U.S.C. 121 §§2701 – 2712, which protects phone calls and electronic communication from warrantless search [40]. The Supreme Court has interpreted the SCA protections to extend to digital device searches. Electronic searches are governed by "Rule 41" of the Federal Rules of Criminal Procedure, Fed. R. Crim. P. 7(b).

[11] See: https://www.law.cornell.edu/wex/search_warrant.

particularly important in understanding the impact of the surveillance data ecosystem on public defenders: (1) the emergence of private technology providers who collect and process surveillance data directly for law enforcement; (2) the disproportionate ill effects of surveillance on marginalized people; and (3) the paradoxical reality that some people suffer when they are invisible to public and private institutions.

*3.1.1 Public-Private Partnerships in Law Enforcement.* The rise of surveillance data in the criminal justice system correlates with the emergence of a private technology ecosystem providing data collection services to law enforcement. The emergence of this ecosystem makes data production in the criminal justice system increasingly complex and opaque to public oversight. Body-worn cameras—an important source of data for our interview participants—provide a useful case study. The leading provider of body camera footage, Axon (formerly Taser) offers police departments free annual subscriptions to its cloud-based evidence management software. Axon has already filed patents on facial recognition systems, and the company claims to be developing video tagging and automatic redacting services using this trove of data, which is not easily accessible to the public [36]. Thus, while the public debates whether to allow police to acquire facial recognition systems, Axon seems poised to integrate facial recognition tools into the services they already offer to to police [36]. Axon has also stated that they intend to develop software that would write police reports automatically and would suggest to police where they should go (i.e., predictive policing) [36, 79]. Thus, Axon's technology choices may actually "change police judgements and actions", but cannot be easily audited or regulated since police departments will receive the new technological advances without undertaking any new acquisition process [39].

Legal scholars have noted that the opacity of this public-private data collection might make it more difficult for public defenders to acquire information and to reason about evidence used in court. In particular, Joh and Wexler find that companies sometimes forbid law enforcement to disclose the existence or workings of a new surveillance technology to journalists, judges, or defense attorneys—nominally to prevent competitors or criminals from discovering how the technology works [39, 76]. For example, it was revealed that the Harris Corporation—the monopolistic manufacturer of cell site simulators[12]—convinced law enforcement and the Federal Communications Commission to withhold the technology from public inspection, including by journalists and defense attorneys [39]. Unable to directly use information from cell-site simulators to prosecute, police began to practice what is called "parallel construction", in which prosecutors present an alternative narrative as to how a suspect was found [5]. In this case, law enforcement would use cell site simulators to locate a suspect, then apply for a pen register (or "wire tap")[13] citing a confidential informant, and try to present the case as occurring without use of the technology—further obscuring defense attorneys' (and any other parties') ability to challenge the legality of the tools used [39]. Given public defenders' unique role in challenging data collected by the police, and the complexity of these emerging social-technical systems, we think it is particularly important to consider how this new private-public techno-surveillance environment plays out for public defenders in practice.

*3.1.2 Biased Data Collection.* This public-private surveillance hydra gazes most intensely at the urban poor and people of color [10, 15, 47]. Since the 1970s, much of our privacy regime has focused around the paradigm of "notice and choice", which lets individuals determine their own disclosures and navigate their own privacy boundaries [15, 34, 63]. However, vulnerable people have less

[12]Cell site simulators, known colloquially as "stingrays," are devices which mimic a cell phone tower. They can be used to determine which cell phones are nearby, and can even intercept communications from those cell phones. See https://www.eff.org/pages/cell-site-simulatorsimsi-catchers.

[13]Pen registers are the standard devices used by law enforcement to record all calls associated with a particular number. The use of pen registers (or "wire tapping") has required a search warrant since Katz v. United States (1967).

access to information and far fewer choices than people of means. Redmiles et al. find through surveys that poor people are the least knowledgeable about personal security and the most likely to experience breaches to their digital security and privacy [62]. Others observe that marginalized people are forced to occupy places that are more intensely monitored and policed [11, 16]. For example, unhoused Americans not only have to perform the daily activities of living in public, but often must undergo surveillance to receive basic services. Shelters are required by federal law to disclose the names and social security numbers of those they serve to the nationwide Homeless Management Information Systems (HMIS), which can be searched by police without a warrant [55]. Common spaces in public housing developments are usually monitored by CCTV cameras [34, 41].[14] The introduction of more sophisticated technologies, such as predictive policing algorithms, may normalize existing bias in surveillance practices, such as preventative police patrols [6].

The problem of surveillance for vulnerable populations is not just one of hyper-visibility, but of misrepresentation. The context of data collection often encodes the poor as criminal and denies people the opportunity to make meaning of their own data. Benjamin describes a "coded exposure" where the harms of visibility are experienced differently due to the bias of the seer [10]. As an example, Benjamin traces how bias in algorithmic facial recognition does not begin with imbalanced training data, but with early decisions in the photography industry to develop photographs within a color spectrum that favors lighter skin tones; thus, being "seen" by these algorithms carries higher consequences (e.g. misrepresentation and arrest) for dark skinned people [10]. More concretely, Patton et al. describe a multi-step everyday racism of social media surveillance [60]. In "everyday racism," communications between black people on social media are produced and disseminated by their own particular self-fulfilling contexts. However, the decoding of this information by police and the encoding of that information into public databases happens without an awareness of the discursive relationships out of which the content was generated. As a result, police are inclined to read content generated by marginalized communities as deviant and criminal [60]. We hypothesize that with careful input from their clients, public defenders might be able to help provide a different, contextually-aware decoding of the relevant communication.

*3.1.3 Too Much Privacy?* A growing scholarship recognizes that in some instances, a lack of visibility—more specifically, a lack of the right kind of visibility—can exacerbate the risk of criminalization and continued poverty for marginalized people. Moreover, surveillance is not as simple as being visible or hidden. Gilman and Greenco describe the "surveillance gap" in which groups such as undocumented immigrants, unhoused people, and those with felony convictions fall outside of systems which might offer them protection and support [34]. Wexler defines "privacy asymmetries" where defense counsel lacks the same access to data as prosecutors—in particular, defense counsel are legally prevented from getting access to social media data about someone other than their clients—and argues that increasing defense counsel's access to information might make the criminal justice system more fair [77].

The body-worn camera (BWC) is one material technology that embodies this tension between accountability and privacy. BWCs were adopted by police amid calls for transparency and accountability in the wake of the killing of Michael Brown in 2014. Some advocates argue that with the right policies, they can make criminal proceedings more fair [69]. Others argue that body-worn camera data, which as discussed above are now privately collected and administered, simply expand police power [46]. Regardless, body camera footage or any other surveillance video alone does

[14]Sometimes people using public housing or the shelter system are required to disclose more than just their name and location. Though discouraged by federal housing policy, some municipal public housing administrations (PHAs) require drug testing and financial inspection [66]. In order to receive funding for specific programs, homeless shelters must disclose the self-reported drug use and HIV status of their clients to HMIS [55].

not necessarily speak for itself. In his 1988 analysis of police undercover work, Marx documents a series of egregious incidents in which selective recordings enabled wrongful conviction [48]. Marx suggests that generating recordings may make undercover offices more accountable, but stresses that these recordings may require careful linguistic interpretation and strict policy restrictions to minimize collateral damage [48]. Body cameras carry the same risks. Whether body cameras serve as a desired form of resistance through observation (what Brown calls "sousveillance" [11]) or are merely another recording eye of police hinges on the minutiae of data-sharing policies, controls on police discretion over stopping and starting the video, and the extent to which the public and defense lawyers may access and process it [36, 39, 46, 53]. It is not just a matter of legal rights, but a matter of design.

### 3.2 HCI and Public Defenders

Despite its technological complexity, relatively little design literature centers on the courthouse. Some design scholarship has focused on the technological needs of law enforcement, finding that technology adoption in law enforcement is slow and mired by a maze of disparate public databases and outdated modes of information sharing [18]. Ethnographic analysis of a crime lab indicates that despite a strong culture of commitment to science and neutrality, forensics experts are constantly anticipating how their findings may be used in court as they struggle to translate scientific findings into legal reports [8]. Others have examined the technology needs of—and effects of surveillance on—those in communities adjacent to the criminal justice system, such as the family members of incarcerated people [59] and undocumented immigrants [37]. However, few have considered the needs of public defenders from an HCI perspective since Elliott et al. studied the impact of introducing digital record systems to public defense offices in the 1990s [22]. A few studies examine the effect of specific types of data, such as body-worn cameras, on public defender practice [33] and the challenges of PDs' work environment [7]. We build on this work and study how the increased availability of surveillance data and its associated technical challenges impacts the work of public defenders and their ability to represent their clients. We are interested specifically in how new technology impacts the balance of power between defenders and prosecutors. We investigate if the difficulties public defenders face working with surveillance data are due to a lack of technical or monetary resources, or if the introduction of new data exacerbates structural inequalities in the criminal justice system.

## 4 METHODS

In this paper, we seek to understand how an increase in digital surveillance data impacts the quality of representation that public defenders can provide their clients, and what specific barriers complicate making sense of that data. To answer this question, we conducted a qualitative study.

### 4.1 Recruiting

We interviewed 21 people in the indigent defense community. For the interview process we partnered with an Oakland-based non-profit called Secure Justice.[15] The first eight interviewees were selected through a snowball sample from our network and through contacts at Secure Justice, in which we focused on range [45]. For example, we interviewed senior public defenders, an individual who had built technology for the Electronic Frontier Foundation (EFF), and an individual who worked with the nationally renowned Bronx Defenders non-profit. After our initial set of interviews, we realized that public defenders who worked on felony cases had the most experience with surveillance data, so we sought a wider sample of PDs. We posted in the public defender

[15] https://secure-justice.org/

subreddit r/public_defenders asking for volunteers to talk about their work experience. We received enough responses to conduct focused sampling [45]. We focused our interviews on public defenders who had experience working on cases with higher volumes of discovery, including cybercrimes and capital crimes, as well as PDs who had previous experience working in prosecutors' or district attorneys' offices.

Consistent with Reddit's general demographics, the Reddit responses were mostly men (eight of the ten people sourced through Reddit) under forty with high technical literacy. Through the initial Reddit seed, we were introduced to a third round of participants who we selected if they had comparative experience in other parts of the criminal justice system or filled demographics that were not previously well represented. After interviewing participants working across the country, we conducted separate interviews with six people working in the same jurisdiction in California in order to develop a full picture of one PD office (this is listed in the participants table as Office X). A description of participants can be found below in Table 1, and a participant demographics can be found in Table 3.

### 4.2 Interview Protocol

Although we wanted rich, specific discussions of technology, we also aimed for breadth of technological experience and understanding [9]. We wanted to understand not only the mechanics of one technology, but the entire socio-technical system surrounding public defense. We conducted semi-structured interviews in which we did not ask predefined questions, but instead tried to guide the conversation in four acts.

First, we asked interviewees where they worked and why they chose to be public defenders. This helped elicit their values and provided context for the rest of the conversation. In the second act, we focused on surveillance technology in discovery. We avoided asking participants directly about times when they had difficulty with discovery or when they thought prosecutors had the upper hand so as not to bias the data with leading questions [75]. Instead, we asked participants to list what technologies they saw in their practice, and then followed up with probing questions where appropriate on particular elements of technology that were mentioned. Through this method, we aimed to draw out a full picture of the power dynamics embedded in the use of that technology and give the participants local control over the conversation [71]. In the third act, we asked interviewees about other technical difficulties which impacted their work. In this section, all interviewees mentioned challenges with case management software and their day-to-day technology pain points. We tried to save this conversation for the end of the interview so as to prevent the conversation from being bogged down in a discussion of pain points particular to database software or old laptops, which were outside our research question. However, we found that when public defenders talked about office technology, it was often very revealing as to how they perceived their funding and support, especially relative to their local district attorneys.

In the fourth act, we explained the project and our working thesis that problems with technology arise not only from under-funding, but from systemic issues in the criminal justice system where prosecutors, police departments, and the federal government control the introduction of data into the system. We felt that this disclosure was important since we wanted our interviewees to understand our positionality as researchers and to provide interviewees with a broader way to participate in the project. Often, this disclosure elicited more stories about interviewees' challenges, which will be helpful in future policy and design research. However, we are cautious about interpreting statements in this last act as reflecting public defenders' subjective experience because we prompted them to focus on power relations with prosecutors. In some instances, participants disagreed that they had worse technical skills or fewer technical resources than prosecutors, contradicting our assumptions entering the project.

### 4.3 Data Analysis

We used a modified version of grounded theory to analyze the data, most closely resembling that described in Charmaz's *Constructing Grounded Theory: A Practical Guide through Qualitative Analysis* [14]. For participants who consented to recording, we recorded the interviews and then uploaded them to the automated transcription program. For five of the participants, we relied on detailed notes. After correcting any transcription errors, we then read the notes a second time and performed "housekeeping coding", organizing the data according to general topic and sorting the conversations so they could be more easily compared [45]. In particular, we highlighted three broad issues to follow up on: self-reported background and information about organizational structure; specific stories about technology; and broader statements about experiences, perceptions, access to resources, and relationships with prosecutors. We further divided technology stories by the type of technology discussed. We then moved the relevant parts of the interviews into a new consolidated document, organized by housekeeping code. For some technologies, we also developed a consistent set of groupings for practices that were common to that technology. For example, most defenders described being unable to watch all body camera video in discovery, but defenders varied in their individual processes of selecting videos and the extent to which they felt that their representation suffered due to this filtering.

Next, we assigned initial codes to each story about technology and each quote. We coded with open-ended phrases. When coding the statements about larger structural problems, we tried to keep the codes "in vivo" to retain public defender-specific language—for example, several public defenders used the specific phrase "junk" or "bunk" science to describe particular kinds of forensic evidence, particularly breathalyzers [14]. For technical stories, we organized by the technology discussed and type of challenge: lack of resources, problems of organizational structure, and lack of legal access (a complete list of these codes can be found in Appendix Table 2). After an initial coding phase, we consolidated the codes into a few broader themes that stood out to us and performed a third round of "focused coding" [14]. Like Owens et al. and Guberek et al., we have tried to determine information about the particular technologies through independent research whenever possible [37, 59].

### 4.4 Limitations

Our interview study reveals public defenders' perceptions about their ability to help their clients. However, additional research that studies their client's perspectives is required to obtain a full picture of the effect of surveillance data on indigent representation. In particular, we must be careful making decisions based on this analysis because they may provide subjective benefit to public defenders at the expense of their clients or other actors in the criminal justice system. Public defenders do not always have an accurate picture of what could be done with the data they receive or the resources of prosecutors. Thus, before proceeding with further technical or political solutions, the perspectives of others impacted by the work of public defenders—including their clients, law enforcement officers, and prosecutors—should also be considered. This research should be paired with a mixed methods approach that examines the efficacy of particular tools [17]. Finally, since in the U.S., people of color are widely and disproportionately harmed by the criminal justice system, future research should expand on this work by explicitly centering race in the analysis [56, 67].

### 4.5 Our Position and Approach

We entered this project concerned about economic and racial bias in the criminal justice system, as well as wanton use of surveillance data. We began the work in collaboration with Secure Justice, a non-profit whose explicit mission is to reduce the harms associated with surveillance data. Early in

Table 1. Description of each participant. "Office X" refers to a public defender office in one California city where we interviewed several employees in different roles.

| Participant | Role |
|---|---|
| P1 | Felony PD in urban, county office (over ten years experience) |
| P2* | Chief county PD, work in the same, urban, county PD office as P3 and P4 |
| P3* | Deputy PD (over ten years experience) |
| P4* | PD and Law Professor (over ten years experience) |
| P5 | Federal PD focused on cyber crimes, (over ten years experience) |
| P6 | Researcher at EFF who put together guides for PDs on novel surveillance tech. |
| P7 | Young paralegal in a PD office strong technical skills |
| P8 | Private attorney working as assigned council for indigent clients |
| P9 | Former misdemeanor PD (two years), now private, civil law. |
| P10 | New PD working on misdemeanor crimes near an urban area |
| P11 | Capital PD, formerly felony PD in three states (over ten years experience) |
| P12 | Felony PD who worked in a conservative, under-resourced county office |
| P13 | Felony PD in Office X (3-5 years experience). |
| P14 | New PD in a small New England county, previously intern at the DOJ |
| P15 | Previously an immigration lawyer, now misdemeanor PD |
| P16 | Investigator in PD Office X (five years experience) |
| P17 | Prosecutor focused on police abuses and cyber crimes, formerly PD in Office X |
| P18 | Felony PD Office X, previously misdemeanour PD in a suburban county |
| P19 | Intern, now new PD in a rural, conservative county PD office |
| P20 | Investigator, PD Office X (over ten years experience) |
| P21 | Legal Services representative for a major tech company |

**P2, P3 and P4 were interviewed jointly*

our process, our collaborators at Secure Justice shared stories with us indicating willful deception from prosecutors with respect to data, and painting public defenders as consistently under-resourced with respect to prosecutors. As we detail below, these early assumptions were challenged by our interviewees. While we find that public defenders are systematically disadvantaged in their ability to acquire and use surveillance data, we find it is rarely due to malicious or unlawful actions from adversarial parties in the criminal justice system, and is often due to structural factors rather than a simple lack of funding. Our motivation in this work is to draw attention to the challenges that PDs face as a way to examine the broader harms of surveillance and to surface important questions about how to control and produce knowledge about those impacted by the criminal justice system [21].

## 5 RESULTS

All of the public defenders we spoke to found that their ability to review and analyze surveillance data such as body camera footage, surveillance videos, and social media reports was instrumental to adequately representing their clients. Our participants explained how prosecutors used surveillance data to paint a narrative that criminalized their clients, and explained that it is critical to public defender practice to re-frame those narratives by reanalyzing the data to reveal inaccuracies or to provide alternative explanations. Although this ability to tell a convincing story with data proved to be a critical aspect of winning a case, public defenders' lack of time and resources made it difficult for this opportunity to be realized. Finally, our participants described structural disadvantages that they faced in relation to prosecutors. Public defenders must respond to data and formatting choices

made by prosecutors, and doing so is often made more challenging by prosecutors' superior ability to partner with law enforcement, private companies, and federal institutions. In this section, we describe each of these aspects in more detail. In the discussion section that follows, we will provide recommendations and paths forward for technologists as well as policymakers.

### 5.1 "Data is Not Neutral": Telling Convincing Stories with Data

The public defenders we spoke to told us that spending time reviewing evidence improved their likelihood of winning cases. Usually, discovery information stems from "raw data"—e.g., body camera footage, social media feeds, or blood samples—and must be synthesized and summarized through a police report or lab report before being passed to defense counsel or presented in court. PDs uniformly felt that these reports and summaries—e.g., surveillance video compilations from private vendors, breathalyzer results, or police reports—could be untrue or unfair to their clients. Consequently, PDs believed it was important for them to re-examine the raw data to craft their own story about how judges and juries should interpret that data. For example, although a description of interviews and the arrest is provided in the police report, body-worn cameras very often provided valuable information which expanded, complicated, or disproved the information in a police report. Public defenders detailed how reviewing body camera footage could reveal inaccuracies in how police and subjects' actions were described in police reports, identify new witnesses, and serve as context for future interviews with victims and witnesses [Participants 13, 15, 16, and 18]. "It's a significant amount of video [...] And you are required to watch it. It can break a case," explained Participant 13.

Social media data is one form of raw data over which prosecutors have a disproportionate ability to paint a narrative. Several participants explained how, armed with access to a person's full social media history, law enforcement officials and prosecutors could often extract a few exchanges to paint a narrative of criminal intent. For example, a Midwest defender described how prosecutors had pulled a few off-color jokes from the juvenile client about "killing" a friend to paint the client as a "super-violent person" [P19]. However, upon examining the client's full social media records and public records from other students, the PD found that the language the client used was routine amongst the young man's acquaintances who made similar "shock value" jokes [P19]. Several interviewees described arguing with prosecutors over the meanings of emojis or slang posted on social media [P13, P14, P19]. For example, Participant 14 witnessed debate about whether a gun emoji and the "one-hundred percent" emoji were sufficient evidence that a client was armed (without a concealed carry permit) all of the the time or if both were merely used for emphasis. The contents of social media accounts are often subpoenaed by prosecutors to bolster a case, but participants also confirmed that law enforcement organizations, particularly gang task forces, actively monitor social media—in particular, accounts belonging to black men in communities with existing gang violence—and use it to begin criminal proceedings [P13, 14, 16], which further raises the stakes of PDs' ability to challenge a prevailing narrative for clients of color. This is consistent with quantitative findings in [61].

The importance of providing an opposing interpretation of the same data was not unique to video and social media histories. One participant, now a captial public defender, explained that now that he has more resources than he did as a "line public defender" and closes only half a dozen cases a year, he hires his own expert to review every piece of analysis provided by prosecutors during discovery, including technical analysis:

> Every single thing from the cops [to] laboratory analysts ... there's always some element of human decision-making ...We need to hire experts [and we] make that person reinvent the whole wheel. Then it's not just to tell us, did that analyst get the

> right result? . . . But the way they phrase the result, is that really an accurate depiction? . . . Or were they trying to kind of fudge the numbers on the margins? [P11]

This public defender felt it would be malpractice for him not to go back to the raw data in every instance where he was handed a report. He understood that every step of interpretation which goes into the report could wrongfully implicate a client. He also acknowledged that this level of review was impossible when he had fewer resources in his old role.

Information that is either technical or too long to present in its entirety requires synthesis and interpretation. Public defenders believed that the nuance of this presentation could materially change outcomes for their clients. In the words of a long-time investigator, "data is not neutral". Public defenders were acutely aware that it was their job to draw out new narratives from that data [P20]. Unfortunately, they uniformly described how their workload, in addition to technical and structural disadvantages, prevented the thorough review they would prefer to provide.

### 5.2 Technical Challenges and Lack of Resources Impact Representation

Most participants described being unable to examine the data to the extent they would like to due to a lack of time and money. For attorneys in jurisdictions with body cameras, body camera footage made up the bulk of surveillance data they received. All cases, even a mundane DUI, assault, or petty theft case (of which misdemeanor attorneys may process hundreds a year), include at least several hours of video [P10, 18]. Felony cases could include up to 150 or 200 hours [P2, P3, P4, P18]. Most felony defenders said it was not possible to watch all the surveillance videos associated with their cases, although they were divided about whether this impacted representation. The pain points around private (non-body camera) surveillance video were not only related to quantity, but included technical problems playing, transferring, downloading, and editing video [P1, P2, P3, P4, P6, P7, P11, P13, P15, P16, P18, P19]. Most PDs described spending hours or days trying to watch videos from private surveillance companies, which often could only be viewed using proprietary software. Though all agreed that these technical hurdles rarely prevented them from watching videos, these issues slowed down cases and delayed defendants' release from jail.

As with body camera footage, adequately parsing through social media reports could be prohibitively time-consuming. Participants stated that Facebook and Instagram feeds received through prosecutors' warrants were often delivered as unstructured PDFs that included every transaction since the user originally signed up for a service, and might be tens of thousands of pages long [P5, P12, P18, P19]. Participant 5 clarified that discovery laws did not require prosecutors to release this discovery in its native, more structured format, and that in these cases PDs just had to "deal with it" [P5]. A few more tech-savvy defenders and paralegals described writing scripts to parse through social media PDFs, body camera footage, and digital forensics reports [P5, P7, P17, P18, P19].

In the case of body camera videos and social media reports, the only theoretical barrier to learning is time. In other cases, public defenders lack the specific technical resources to replicate an analysis. For example, PDs often do not have access to digital forensics tools such as Cellebrite machines, which are used to extract data from physical devices [P1, P12, P19]. In other cases, lack of knowledge within the office combined with lack of funds to hire experts could make it impossible to challenge or replicate the forensic science or analysis of more complex forms of data such as data from car black boxes or ShotSpotter history. One public defender described being "laughed at" when he gave experts a quote for what he could pay them [P18]. Another described feeling unable to adequately defend clients in DUI cases when she didn't have the resources to fully understand the science interpolating blood alcohol numbers in the hours before or after a breathalyzer or blood test read. She explained: "The question isn't if the breath machine is working properly, or if the breath machine is designed properly; the question is whatever the number that breath machine spit out

means!" [P15]. This participant had a strong sense that the methods for determining drunkenness at a particular time long before or after a breathalyzer reading were "bunk science", but was frustrated that she didn't have enough knowledge or context to incorporate that argument in her cases [P15].

*5.2.1 Temporal Pressure.* Several participants described a common and difficult trade-off between time and thoroughness in their work [P11, P12, P16, P17]. As one investigator explained, even a favorable outcome from the defense attorney's perspective is still "unfair" to the accused if he spends time in jail or prison [P17]. Some participants said that sometimes they would forgo the review of evidence in order to expedite a trial, or at least felt that delaying an outcome could cause more harm than good. As one interviewee said about his time as a felony line defender, "It's a horrible sad situation, but you go to them and you [see someone in jail and] are like, 'yeah, I know you want to go home, but I haven't gotten to watch your video yet."' [P11]. Asked about his decision to forgo watching videos, a particularly overburdened felony defender in the Midwest said, "Sometimes we just need to figure out how to [move] forward. It's in a client's interest to resolve it" [P12]. Several other defenders spoke about their difficulty getting access to experts in time for critical early moments in the criminal justice process outside of the courtroom. A new misdemeanor attorney said that though he could sometimes obtain funds for an expert at trial, "All these tech issues come up pretrial, like motions to suppress evidence, and it would be useful to have someone who could explain it to me [so I can then explain it to a judge]" [P10]. Public defenders explained that in many situations, simply not having access to data in time was just as detrimental to clients as not having access to it at all. PDs struggled to balance the benefits to their clients of potentially uncovering exculpatory information with the very real costs of delaying resolution of a case.

*5.2.2 Systematic Lack of Resources.* An important part of our research question was the extent to which these technological pain points were felt by defense attorneys as compared to prosecutors. Many of our interviewees considered their local DAs to have better in-house tech—for example, up-to-date laptops, or access to county-issued phones [P11, P12, p15, P19]. One participant described being a public defender as being in a constant state of "tech envy" when he would see prosecutors' technology in court [P12]. Another said he was prevented from using the WiFi set up by prosecutors in the courthouse, making both courtroom presentations and remote communications with clients and witnesses needlessly difficult.

However, in contrast to our initial expectations, some participants (particularly those in rich, left-leaning jurisdictions) did not believe that district attorneys (DAs) had vastly better access to surveillance data or better ways of making sense of it. Notably, the public defenders we spoke to in Office X (the public defender office for a California city) as well as one former public defender who now works in a local DA's office, were very confident that the prosecutor's office was equally if not more technologically behind [P13, P17, P18]. One interviewee said he was sure that body camera footage had to be compiled through an automated process because "the DA screws stuff up. They don't seem to be screwing up the process as much." [P18].[16] Some described a frustrating back and forth with the DA about discovery, particularly video evidence—less due to malicious intent, and more due to the DA not fully understanding a particular piece of technology [P5, P18].

### 5.3 Structural Advantages of Prosecutors

Public defenders' disadvantages in surveillance data sense-making do not only stem from a lack of time and money. Talking with public defenders illuminated the extent to which defense counsel

[16]This PD's office uses the provider Axon (formerly Taser). The company has a feature which uses police dispatch information to tag body camera footage [36].

and local DAs are part of a large surveillance and forensics ecosystem. The more complex the technology, the more actors—police, federal prosecutors, the FBI, local forensics labs, gang task forces, and private technology providers—shape the format in which public defenders receive discovery. A primary structural disadvantage is simply that most data public defenders interact with is delivered as discovery from prosecutors, which allows prosecutors greater control over the format and structure of the data. Defenders felt particularly disadvantaged in their relative lack of power in relation to private companies, in proximity to law enforcement, in sharing information amongst themselves, and in working within the law to challenge commonly used, but perhaps unreliable, forms of scientific evidence.

*5.3.1 PDs Must Respond to Data Choices Made by Prosecutors.* Most of the data that public defenders encounter is delivered to them from prosecutors, depriving PDs of valuable control and knowledge about the minutiae of data formats. Many felony defenders also mentioned spending time organizing body camera video clips which were often delivered as a large collection of files named without clear conventions or an easy way to determine the time and officer involved [P15, P18, P19]. Most participants felt that this was due mostly to a lack of process or control over the design of the body camera systems, but at least one felt confident that he received intentionally duplicated body camera clips from prosecutors as well as duplicated PDFs in discovery [P19]. The same participant also noted that the prosecutor's office could internally tag text conversations which they extracted from Cellebrite, but would provide the defense counsel with the original untagged and unsorted version as a PDF [P19]. Senior public defenders in California described how, due to an upgrade to the jail calls database in their area (about which which they were not informed), they received hundreds of hours of jail calls in a file format that they did not have the tools to play, only a few weeks before an important court date [P2, P3, P4].

Regardless of intent, public defenders often receive data from complex, multi-stakeholder technical systems into which they provide very little input. Most data public defenders see is essentially third-hand, having been collected by private institutions, subpoenaed by law enforcement, and then provided through discovery to public defenders. Worse, some data comes through law enforcement via contracts. An investigator described how public housing units contract with a private video surveillance provider called WatchTower [P16]. Police may call WatchTower twenty-four hours a day on a dedicated line and describe an incident they believe to have occurred. The company will then provide police with a video montage of the incident to police who, after an arrest, may share the video with prosecutors, who in turn transmit the highly edited video through discovery to public defenders [P16]. Thus, the montage enters the public defense office after passing through three sets of adversarial hands: the private company, the police, and the prosecutor's office.

*5.3.2 Prosecutors and Private Partnerships.* Public defenders' frustrations with public-private partnerships took three forms, all with essentially legal origins. The first perceived problem was companies' unwillingness to comply with public defenders' subpoenas and a lack of legal mechanisms to get the same data as prosecutors. These issues came up most often with respect to social media data, in which privacy laws prevent defense counsel from obtaining social media about anyone other than their client [77] [P5, P11]. The animosity of public defenders was not directed at the legal structures, but at these companies. When asked if legal or technical hurdles prevented him from getting full access to social media data, a public defender blurted out: "It's not privacy laws or technical hurdles ... It's Facebook being dicks ... they will provide all of this information to law enforcement without a warrant, but they will not respond to our subpoenas very often" [P13]. Other participants explained that companies seemed to respond to law enforcement requests with more data than was legally required [P12, P19]. For example, Participant 19 described cases in which law enforcement only had a warrant to examine the text messages between a few people, but

providers provided someone's full messaging history and left it to law enforcement to do their own redacting. Laws could be passed requiring Facebook to respond to subpoenas from the defense, and penalizing slow or incomplete response, but the spirit of this comment speaks to a strong perception that public defenders are excluded from agreements between data brokers and the state. Indeed, regardless of the legal landscape, several participants suggested that private companies were simply more eager to give information to the DA. Investigators we spoke with explained that many companies would provide reports to law enforcement without formal subpoenas, while public defenders had to aggressively leverage their legal avenues [P16, P20].

Second, public defenders resented being denied access to surveillance tools for intellectual property reasons. One public defender said, "with forensic tools [...] from Cellebrite machines to interviewing techniques [...] nobody will train us on it ...they're trying to keep it a black box and keep it law enforcement only" [P12]. Although the federal public defender we spoke with did have access to a Cellebrite machine, Participant 12's frustration is likely in part because these tools are, as explained by the longest tenured attorney in our sample, often explicitly "designed for law enforcement" even if that audience is not legally enforced [P8]. Another public defender stated that although he felt the DNA lab in his district was unbiased, what he wanted access to was the analysis software, which "is trade secrets that the company will not allow us to look at" [P13]. In short, this lack of access to the "black box" of surveillance tools gave public defenders a strong feeling that they could not properly reason or fight against forensic evidence that might be faulty.

Third, public defenders were concerned that the federal government had a "voice at the table" [P11] when designing surveillance infrastructure such as cell phone towers, and that prosecutors were then aided or trained by the federal government[17] [P5, P11, P13]. Pressure from law enforcement can indirectly lead companies to build technical infrastructure to support law enforcement surveillance. Participant 21, an employee at a major tech company, explained that the company had needed to build new technical infrastructure in order to process geo-fencing warrants when the volume of these warrants—which require searching on a bounding box rather than by user or device identifier—increase dramatically. He also claimed that law enforcement's use of the legal tool "really went up" after the publication of a critical exposé of geo-fencing warrants in the *New York Times* [72], and remains prevalent even after a federal court ruled them unconstitutional in August 2020 [68] [P21]. It is worth noting that instances where pressure from national law enforcement organizations expands and tailors surveillance infrastructure are well documented through independent reporting and legal literature.[18]

## 6 DISCUSSION

Our findings have three categories of implications. First, the incredible difficulty public defenders faced obtaining and using data from private companies and public surveillance systems relative to law enforcement highlights the importance of considering surveillance harms, and the experience of public defenders more specifically, in the design and development of new technologies. Public defenders' numerous technical challenges working with data suggest opportunities for the careful development of technical solutions to aid in digitizing and analyzing data with low-code or no-code interfaces. Second, we argue that the overflow of data in the criminal justice system is inherently harmful. We identify opportunities for policy and advocacy work to reduce the inflow of data into the criminal justice system and enable public defenders to fairly interpret what data is used. Finally, in addition to these implications for design and policy, we explore how this new understanding of

[17] For example, see this DOJ bulletin on cell site analysis [57].

[18] A particularly salient case is Enhanced 911 (E911) response, which requires that network providers have a mechanism for determining the location of a phone within 100 meters. This same mechanism is what enables law enforcement to use a "tap and trace" phone tracker [31, 54].

public defenders' relationship to surveillance data contributes to a larger discussion of privacy and justice in the CSCW literature [20, 21, 27, 28].

### 6.1 Implications for Technologists

Public defenders' difficulties with data are unlikely to be solved by technologists alone. However, we find that technologists' ignorance of the struggles of public defenders exacerbated the imbalance between prosecutors' and public defenders' ability to work with data, and that unique opportunities exist for technologists to design for public defenders.

*6.1.1 Considering Public Defenders During Design.* The most critical implication of our findings for technologists is the importance of considering the needs of public defenders when designing and maintaining systems which passively collect data about people. First, technology providers should focus on developing the technical and procedural means to respond to data requests in as narrow and interpretable a way as possible. Search warrant requests often only require access to a subset of a user's data (e.g., communication within a certain time frame or between a few people). However, our respondents said that companies would return the full history of someone's social media data dump and leave it to law enforcement to redact what they did not need. Second, providers should develop a subpoena process specifically for public defenders. Often, PDs were unable to get data to which they were legally entitled because the person or entity to whom they issued a subpoena was either slow to comply or complied in a way that rendered the information useless. Simple steps like having a dedicated phone number for defense attorneys to call (so they do not have to navigate a phone tree) or a data pipeline that outputs user data in an easy-to-use file format such as a CSV (rather than an unstructured PDF) would save public defenders hours and increase the likelihood that a user's information appears fairly in criminal proceedings. Though public defenders should be able to hold someone who does not respond to a subpoena request in contempt of court, they often lack the resources exercised by law enforcement to enforce their data-gathering rights.

*6.1.2 Designing for Public Defenders.* Design is another avenue for researchers and technologists seeking to advance justice [20, 27, 70]. Prefigurative design is one framework that guides interventions by researchers through social relationships, distribution of resources, and building counter-structures [4]. We found that in the short term, public defenders and their clients would benefit from technical tools for searching and processing data, including access to technical tools that prosecutors have access to either directly or through training from the federal government. The public defense space does offer some opportunity for system designers. For example, a majority of interview participants expressed interest in transcription software for surveillance video and body camera footage, tools to label and sort body camera footage, and tools to extract information from common sources of social media.

However, in developing these solutions, technologists should be mindful of the stakes involved in defense work and the complexity of the work environment. Several misdemeanor PDs described how even among indigent clients, inequalities were vast, and outcomes were best for relatively more privileged clients who were able to better participate in their own defense. For example, it is often easier for defendants to request their own phone records from their provider in cases where they provide an alibi than for them to rely on the PD to subpoena those records. However, this option may be difficult for the most vulnerable clients such as people with mental disabilities, non-English-speaking people, or unhoused people—and it is impossible in instances where defendants use older, cheaper devices such as prepaid phones [P8, P9, P15]. Technical solutions that only work for some clients risk exacerbating these inequalities. In addition, even though they see many similar kinds of data, different PDs operate in vastly different IT contexts and tend not to specialize on particular types of cases [51]. Finally, public defenders operate in an adversarial environment

and may be wary of solutions that might inadvertently provide data to prosecutors [51]. System designers are most likely to be successful developing solutions in close partnership with a few public defense offices.

Time and money remain insurmountable barriers to public defenders working with novel data. Public defenders and their clients would benefit from resources to hire their own experts and in-house scientists, as is done in capital cases. Reflecting on his time as an unspecialized felony defender working on 75 cases a year, a capital public defender described what it feels like to inadequately represent someone due to technical or resource constraints: "The depression and sadness, because it's not the death penalty, but these people are going to go to prison for decades possibly because [...] I don't have the time to make this thing work" [P11]. Giving defenders who work on non-capital felony crimes even half the resources of capital defenders would be a radical departure from the status quo. Still, if the goal is simply representation, both sides' full ability to review every piece of evidence should be required before someone is deprived of liberty for years or decades.

### 6.2 Requirement for Legal and Structural Changes as Well as Technical Solutions

As we strive to help public defenders reckon with the fire hose of novel surveillance data, we must not forget that we might have the legal and political means of turning off the hose. There is a risk that increasing funding and IT solutions for public defenders leads to an expensive technological arms race as well as to an increasing need for automatic tools to process new data, which have their own drawbacks. A better solution could be to meaningfully limit and make more transparent the data law enforcement can access, while bringing public defenders to parity in data access. Similarly, in addition to better funding for public defenders, policy reforms which reduce the number of cases that move through the criminal justice system, particularly for minor infractions, could achieve the same result. In discussing technical solutions in general, Participant 18 explained that a reduction in caseloads and in bureaucracy would be preferable to technical solutions:

> "I feel [with some of the technical solutions] it'd be great to have a system where people are texted before their court date, but even better would be a system where 90 percent of the court dates don't happen because they're totally useless."

Not only does the participant argue that policy solutions might better handle the problem of defendants failing to appear in court, he shows how focusing on the technical may further entrench and normalize broken systems, in this case a process of requiring many procedural pre-trial hearings.

*6.2.1 Policy Recommendations.* In addition to big-picture reforms to reduce caseloads and divert clients outside of the criminal justice system, we identify several more specific areas for policy work, including transparency laws and amendments to additional privacy legislation.

First, many of public defenders' difficulties with surveillance data stem from a lack of transparency about what law enforcement has access to and how it works. We recommend advocating for local ordinances to provide transparency and regulation around local acquisition of surveillance data systems. Two important models are Oakland's PAC Surveillance Technology Ordinance[19]—which requires disclosure of new technologies and prohibits non-disclosure agreements—and Seattle's municipal code, which requires city council approval for the acquisition of new technologies (Seattle, Washington Municipal Code §14.18.20 [2013]).[20] However, our research reveals the importance of extending these disclosure rules to places that are semi-public but where indigent people are

[19]See Privacy Advisory Commission, City of Oakland California https://www.oaklandca.gov/boards-commissions/privacy-advisory-board

[20]A similar ordinance has been adopted by Santa Clara County (Santa Clara County, California Ordinance Code §A40-2 [2017])

commonly surveilled, such as jails, prisons, and public housing. Public defenders should also be involved as stakeholders in the acquisition process for new technologies. Another avenue to explore is abolishing private companies' ability to invoke trade secret protections on any data-processing tool used in a criminal court [39, 76].

Second, there are specific areas where legal frameworks should be amended to provide public defenders equal access to surveillance data and tools for processing it. One is in social media, where defense attorneys cannot request data from anyone other than their client [77]. In general, privacy advocates should be careful that public defenders have the same exemptions as law enforcement and should minimize law enforcement exemptions whenever possible. Lastly, any solutions which reduce the number of times defendants must appear in court and the amount of paperwork public defenders must complete will help reduce the load on the system overall.

### 6.3 Implication for Discussions of Privacy

This work highlights the limitations of the current deeply individual model of privacy rights as well as the importance of considering interpretation and control to the same extent as visibility.

A few of the solutions discussed above—including limits to exceptions in privacy laws for law enforcement and tighter regulations on police partnerships with private companies—reduce the amount of data to which the state has access. However, others—such as amendments to privacy laws that seek to allow public defenders access to the same data as law enforcement and force private companies to more readily respond to PD subpoenas—put more data into the system. More than anything, public defenders' challenges with data highlight the importance of interpretation above and beyond mere visibility. Rather than more or less data, what public defenders need are mechanisms to decode what is already available. In this section, we discuss how our findings have two major implications for a larger discussion of privacy. First, the finding that an increase in information and sense-making tools for some public actors might help victims of over-surveillance reinforces critiques of an anti-surveillance paradigm built around individual privacy rights. Second, the extent of public defenders' data challenges illustrates a need for complicating the discussion of data marginalization away from a discussion of seeing or not seeing, and toward one that focuses on control and interpretation of information.

*6.3.1 The Limitations of Individual Privacy Rights.* Though perhaps individual privacy rights are ends in themselves, none of the public defenders we interviewed mentioned individual privacy rights as an important part of making the criminal justice system more fair for their clients. This may be partly because recent legal victories for individual privacy, such as the European Union's General Data Protection Regulation (GDPR)[21] and the California Consumer Privacy Act (CCPA)[22], include sweeping exceptions for law enforcement [10, 15]. Another reason that "notice and choice" paradigms of privacy are so woefully unhelpful is that the clients of public defenders rarely have much choice in avoiding surveillance. Individuals who are in constant contact with the carceral state—e.g., unhoused people, those living in public housing, and relatives of incarcerated people—live in a sort of incarceration by proxy, in which they are denied legal and practical privacy protections even if they have never been convicted of a crime. For example, one in 14 Americans has a family member who is currently in jail or prison, and almost half of all Americans have at one point had an incarcerated family member [23]. At least one of the two companies that provide

[21] GDPR requires "controllers and processors" to offer a number of protections to consumers, such as transparency about data use. However, law enforcement and intelligence agencies are not considered controllers or processors. See: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/ .

[22] CCPA, which offers consumers the right to know what information is collected about them as well as rights to fight bias in data use, does not apply to non-profits or government agencies.

services for inmates to call from jails and prisons requires callers to share their location with the system when calling family members in jail, not just during a call but for a full hour after it [59]. Based on our interviews with public defenders, it seems likely that this location data is freely and easily shared with police and prosecutors, but not with public defenders.

*6.3.2 Design Patterns impact Data Access and Interpretation.* Our interviews also highlight how the legal reality of what someone *can access* might not match the practical reality of the data they are *able to use*. People working for private data providers have unique power to level the scales of data justice by easing the process of data requests for public defenders. Public defenders seemed to lack meaningful access to data less often due to explicit "privacy asymmetries" in the law [77] or nondisclosure agreements [39], and more often due to practical resource constraints, e.g., lack of resources to enforce their legal rights (in particular, to compel companies to promptly respond to subpoenas) or insufficient funding to purchase the equipment or expertise necessary to process data received in discovery. Sadly, our findings indicate that some efforts to explicitly restrict law enforcement's access to data may have backfired. For example, search warrants represent a higher legal standard than subpoenas, and laws requiring a search warrant for law enforcement to gain access to data (such as the Stored Communications Act) were heralded as privacy wins. However, Participant 21's assertion that his technology provider prioritizes responding to law enforcement requests—and public defenders' experience that slow responses to subpoenas could effectively deny them data—suggest that this higher legal standard alone does little to block law enforcement access, and may in fact prevent access by defense counsel.

*6.3.3 Interpreting the Data is as Important as Seeing It.* No amount of regulation of the entry of data into the criminal justice system eliminates questions of interpretation. Requiring a warrant for police to access a particular data source does not guarantee that the data is interpreted fairly. In some instances, public defenders we interviewed were struggling to make a case out of information that was already public or in law enforcement's hands by default. Gang task forces monitor public Instagram profiles, often including the profiles of youth or music artists who have other incentives for being visible, such as safety or artistic self-promotion [60, 61]. What is seen in body cameras is, by construction, already known to police; the cameras themselves are tools introduced to offer the opportunity to more fairly interpret what police see. As data sources become more complicated, access to meaning-making becomes a necessary part of taking power over one's own information. Thus, the deprivation of liberty in a individual person's case may have less to do with *how much* data law enforcement may have about them, their consent in the collection of that data, or even how much of that data they might be able to see—and more to do with *who* controls how that information is made sense of.

*6.3.4 On Abolition.* We find that our focus on technical challenges for public defenders is a useful window into systemic and organizational inequality in the criminal justice system, as well as into the inadequacy of a privacy rights framework focused on individual choice. However, Abebe et al. warn that using computational research as synecdoche for research into societal problems may drive attention away from institutional and political solutions [1]. Public defenders' difficulties are artifacts of an all-too-large policing and criminal justice apparatus. Still, even if the criminal punishment system in its current incarnation is abolished, our findings regarding the nuance of how data is interpreted are still likely to be relevant as considerations for those navigating other public institutions. In the best case, public defenders use their skills to help indigent people navigate a well-designed social safety net, and it will remain our responsibility as technologists to ensure that vulnerable people and their advocates have easy access and control of their data.

## 7 CONCLUSION

Public defenders do not have the necessary tools to defend clients in the face of a growing public-private surveillance apparatus. In particular, public defenders struggle to process body camera footage and social media data. We find that public defenders' primary structural disadvantages are a lack of control over the data law enforcement has access to as well as a relative lack of power when dealing with private data providers. While we do advocate for transparency laws in surveillance data acquisition as well as tighter regulations on the type and extent of data law enforcement may access, we find that technologists may have an important role in assisting public defenders in two ways. First, we find opportunities for the development of narrow, technical solutions. Second, and more importantly, creators of data-collecting systems can work to make sure that public defenders and law enforcement can request data in a lawful, fair, and narrow way. Technologists should carefully consider (and limit) the generation of data artifacts which may be easily accessed by law enforcement.

## 8 ACKNOWLEDGEMENTS

This work was supported by the Center for Technology, Society, and Policy at UC Berkeley. Steve Trush, Brian Hofer, and Secure Justice were instrumental in providing project direction and in providing access to early introductions to members of the public defense community. Tiffany Pham, Jyen Yiee Wong, and Sneha Chowdhary provided important help conducting early interviews. Dr. Jenna Burrell and Dr. Rebecca Wexler provided important feedback on early drafts. Tommy Alexander and Nicole Updegrove provided copy-editing and writing assistance. Finally, this work would not be possible without the research participants who lent us their time and insights.

## REFERENCES

[1] Rediet Abebe, Solon Barocas, Jon Kleinberg, Karen Levy, Manish Raghavan, and David G. Robinson. 2020. Roles for computing in social change. In *Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency*. ACM, Barcelona Spain, 252–260. https://doi.org/10.1145/3351095.3372871

[2] Michelle Alexander and Cornel West. 2012. *The new Jim Crow: mass incarceration in the age of colorblindness* (revised edition ed.). New Press, New York. OCLC: ocn656451603.

[3] James M. Anderson and Paul Heaton. 2011. *How Much Difference Does the Lawyer Make?: The Effect of Defense Counsel on Murder Case Outcomes*. Technical Report. Rand Corporation. https://www.rand.org/pubs/working_papers/WR870.html

[4] Mariam Asad. 2019. Prefigurative Design as a Method for Research Justice. *Proc. ACM Hum.-Comput. Interact.* 3, CSCW (Nov. 2019), 200:1–200:18. https://doi.org/10.1145/3359302

[5] Natasha Babazedeh. 2018. Concealing Evidence: Parallel Construction, Federal Investigations, and the Constitution. *Va. J.L. & Tech.* 22, 1 (2018), [i]–59.

[6] Chelsea Barabas. 2020. Beyond Bias: Re-Imagining the Terms of 'Ethical AI' in Criminal Law. *Georgetown J. of L. & Modern Critical Race Perspectives* 12, 2 (2020). https://doi.org/10.2139/ssrn.3377921

[7] Valerio Baćak, Sarah E. Lageson, and Kathleen Powell. 2020. "Fighting the Good Fight": Why Do Public Defenders Remain on the Job? *Criminal Justice Policy Review* 31, 6 (July 2020), 939–961. https://doi.org/10.1177/0887403419862317 Publisher: SAGE Publications Inc.

[8] Beth Bechky. 2021. *Blood, powder, and residue: how crime labs translate evidence into proof*. Princeton University Press, Princeton.

[9] Howard S. Becker. 2014. The Epistemology of Qualitative Research. *Braz. J. Empirical Legal Stud.* 1, 2 (2014), 185–199. https://heinonline.org/HOL/P?h=hein.journals/brzjemls1&i=429

[10] Ruha Benjamin. 2019. *Race after technology: abolitionist tools for the new Jim code*. Polity, Medford, MA.

[11] Simone Browne. 2015. *Dark Matters: On the Surveillance of Blackness*. Duke University Press. https://doi.org/10.2307/j.ctv11cw89p

[12] Lincoln Caplan. 2013. Opinion | The Right to Counsel: Badly Battered at 50. *The New York Times* (March 2013). https://www.nytimes.com/2013/03/10/opinion/sunday/the-right-to-counsel-badly-battered-at-50.html

[13] Stevie Chancellor, Shion Guha, Jofish Kaye, Jen King, Niloufar Salehi, Sarita Schoenebeck, and Elizabeth Stowell. 2019. The Relationships between Data, Power, and Justice in CSCW Research. In *Conference Companion Publication of the 2019 on Computer Supported Cooperative Work and Social Computing (CSCW '19)*. ACM, New York, NY, USA, 102–105.

https://doi.org/10.1145/3311957.3358609
[14] Kathy Charmaz. 2006. *Constructing Grounded Theory: A Practical Guide through Qualitative Analysis*. SAGE Publications.
[15] Kami Chavis. 2014. Future of the Fourth Amendment: The Problem with Privacy, Poverty and Policing. *U. Md. L.J. Race Relig. Gender & Class* 14, 2 (Jan. 2014). https://papers.ssrn.com/abstract=2873829
[16] Andrew Clarke, Cameron Parsell, and Lutfun Nahar Lata. 2021. Surveilling the marginalised: How manual, embodied and territorialised surveillance persists in the age of 'dataveillance'. *The Sociological Review* 69, 2 (March 2021), 396–413. https://doi.org/10.1177/0038026120954785
[17] John W. Creswell and J. David Creswell. 2017. *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. SAGE Publications.
[18] Julia Deeb-Swihart, Alex Endert, and Amy Bruckman. 2019. Understanding Law Enforcement Strategies and Needs for Combating Human Trafficking. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. ACM, Glasgow Scotland Uk, 1–14. https://doi.org/10.1145/3290605.3300561
[19] Criminal Justice Information Services Division. 2020. *Uniform Crime Report: Crime in the United States, 2019*. Technical Report. U.S. Department of Justice—Federal Bureau of Investigation. 3 pages. https://ucr.fbi.gov/crime-in-the-u.s/2019/crime-in-the-u.s.-2019/topic-pages/persons-arrested
[20] Lynn Dombrowski, Ellie Harmon, and Sarah Fox. 2016. Social Justice-Oriented Interaction Design: Outlining Key Design Strategies and Commitments. In *Proceedings of the 2016 ACM Conference on Designing Interactive Systems (DIS '16)*. ACM, New York, NY, USA, 656–671. https://doi.org/10.1145/2901790.2901861
[21] Paul Dourish. 2006. Implications for design. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, Montréal Québec Canada, 541–550. https://doi.org/10.1145/1124772.1124855
[22] M. S. Elliott. 1997. Moving from paper-based to digital documents: case study of public defenders using case management and legal research tools. In *Proceedings of the Thirtieth Hawaii International Conference on System Sciences*, Vol. 6. 97–106 vol.6. https://doi.org/10.1109/HICSS.1997.665491 ISSN: 1060-3425.
[23] 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 (Jan. 2019), 2378023119829332. https://doi.org/10.1177/2378023119829332 Publisher: SAGE Publications.
[24] Virginia Eubanks. 2018. *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*. St. Martin's Publishing Group.
[25] Donald J. Farole and Lynn Langton. 2010. *County-based and Local Public Defender Offices, 2007*. Technical Report NCJ 231175. Bureau of Justice Statistics (BJS). https://www.bjs.gov/index.cfm?ty=pbdetail&iid=2211
[26] Marion Fourcade and Kieran Healy. 2016. Seeing like a market. *Socioecon Rev.* (Dec. 2016). https://doi.org/10.1093/ser/mww033
[27] Sarah Fox, Mariam Asad, Katherine Lo, Jill P. Dimond, Lynn S. Dombrowski, and Shaowen Bardzell. 2016. Exploring Social Justice, Design, and HCI. In *Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems (CHI EA '16)*. ACM, New York, NY, USA, 3293–3300. https://doi.org/10.1145/2851581.2856465
[28] Sarah Fox, Jill Dimond, Lilly Irani, Tad Hirsch, Michael Muller, and Shaowen Bardzell. 2017. Social Justice and Design: Power and oppression in collaborative systems. In *Companion of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing (CSCW '17 Companion)*. ACM, New York, NY, USA, 117–122. https://doi.org/10.1145/3022198.3022201
[29] Diana Freed, Sam Havron, Emily Tseng, Andrea Gallardo, Rahul Chatterjee, Thomas Ristenpart, and Nicola Dell. 2019. "Is my phone hacked?" Analyzing Clinical Computer Security Interventions with Survivors of Intimate Partner Violence. *Proceedings of the ACM on Human-Computer Interaction* 3, CSCW (Nov. 2019), 1–24. https://doi.org/10.1145/3359304
[30] Bryan Furst. 2019. *A Fair Fight: Achieving Indigent Defense Resource Parity*. Report. Brennan Center for Justice. https://www.brennancenter.org/our-work/research-reports/fair-fight
[31] Aaron Futch and Christine Soares. 2001. Enhanced 911 Technology and Privacy Concerns: How Has the Balance Changed Since September 11? *Duke L. & Technology Rev.* 1, 11 (2001), 10. https://scholarship.law.duke.edu/dltr/vol1/iss1/38/
[32] Daniel Gardiner, Jason MacMorran, and Stephen F. Hanlon. 2017. *The Louisiana Project*. Technical Report. American Bar Association Standing Committee on Legal Aid and Indigent Defendants. 64 pages.
[33] Janne E. Gaub, Carolyn Naoroz, and Aili Malm. 2019. Understanding the impact of police body-worn cameras on Virginia public defenders. (2019). https://doi.org/10.13140/RG.2.2.18210.79044
[34] Michele Gilman and Rebecca Greenco. 2018. The Surveillance Gap: The Harms of Extreme Privacy and Data Marginalization. *N.Y.U. Rev. L. & Soc. Change* 42, 2 (2018), 57.
[35] Benjamin Goodman. 2021. Shotspotter: the Newest Tool to Degrade What is Left of the Fourth Ammendment. *UIC L. Rev.* 54, 3 (2021), 797 –828. https://repository.law.uic.edu/lawreview/vol54/iss3/5/

[36] Daniel Greene and Genevieve Patterson. 2018. Can we trust computer with body-cam vidio? Police departments are being led to believe AI will help, but they should be wary. *IEEE Spectr.* 55, 12 (Dec. 2018), 36–48. https://doi.org/10.1109/MSPEC.2018.8544982

[37] 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 *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. ACM, Montreal QC Canada, 1–15. https://doi.org/10.1145/3173574.3173688

[38] Caroline Wolf Harlow. 2000. *Defense Counsel in Criminal Cases*. Technical Report NCJ 179023. Bureau of Justice Statistics (BJS). https://www.bjs.gov/index.cfm?ty=pbdetail&iid=772

[39] Elizabeth E. Joh. 2017. The Undue Influence of Surveillance Technology Companies on Policing. *N.Y.U. L. Rev.* 92 (Sept. 2017). https://doi.org/10.2139/ssrn.2924620

[40] Orin S. Kerr. 2003. A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It. *G.W. Law Rev* 72, 1208 (2003), 36. https://doi.org/10.2139/ssrn.421860

[41] Sandjar Kozubaev, Fernando Rochaix, Carl DiSalvo, and Christopher A. Le Dantec. 2019. Spaces and Traces: Implications of Smart Technology in Public Housing. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. ACM, Glasgow Scotland Uk, 1–13. https://doi.org/10.1145/3290605.3300669

[42] Lynn Langton and Donald J. Farole. 2010. *State Public Defender Programs, 2007*. Technical Report NCJ 228229. Bureau of Justice Statistics (BJS). https://www.bjs.gov/index.cfm?ty=pbdetail&iid=2242

[43] Jennifer E Laurin. 2017. Data and Accountability in Indigent Defense. *Oh. St. J. of Criminal L.* 14 (2017), 30.

[44] Rachel Levinson-Waldman. 2018. *Government Monitoring of Social Media: Legal and Policy Challenges | Brennan Center for Justice*. Expert Brief. Brennan Center for Justice. https://www.brennancenter.org/our-work/research-reports/government-monitoring-social-media-legal-and-policy-challenges

[45] J. Lofland and L.H. Lofland. 1995. *Analyzing Social Settings: A Guide to Qualitative Observation and Analysis*. Wadsworth.

[46] Ermus St Louis, Alana Saulnier, and Kevin Walby. 2019. Police Use of Body-Worn Cameras: Challenges of Visibility, Procedural Justice, and Legitimacy. *Surveillance & Society* 17, 3/4 (Sept. 2019), 305–321. https://doi.org/10.24908/ss.v17i3/4.8649

[47] Mary Madden, Michele E. Gilman, Karen Levy, and Alice E. Marwick. 2017. Privacy, Poverty and Big Data: A Matrix of Vulnerabilities for Poor Americans. *Wa. U. L. Rev.* 95, 53 (March 2017), 73. https://papers.ssrn.com/abstract=2930247

[48] Gary T Marx. 1988. *Undercover: Police Surveillance in America*. University of California Press, Berkeley. OCLC: 869722469.

[49] Gary T. Marx and Keith Guzik. 2017. The uncertainty principle. In *The Routledge Handbook of Technology, Crime and Justice* (1 ed.), M. R. McGuire and Thomas J. Holt (Eds.). Routledge, Abingdon, Oxon; New York, NY: Routledge, 2017. | Series:, 481–502. https://doi.org/10.4324/9781315743981-29

[50] Nora McDonald, Karla Badillo-Urquiola, Morgan G. Ames, Nicola Dell, Elizabeth Keneski, Manya Sleeper, and Pamela J. Wisniewski. 2020. Privacy and Power: Acknowledging the Importance of Privacy Research and Design for Vulnerable Populations. In *Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems*. ACM, Honolulu HI USA, 1–8. https://doi.org/10.1145/3334480.3375174

[51] Pamela Metzger and Andrew Guthrie Ferguson. 2015. Defending Data. *Southern Cal. L. Rev.* 88, 1057 (July 2015), 69.

[52] Alexandra Natapoff. 2018. *Punishment Without Crime*. Basic Books. https://www.basicbooks.com/titles/alexandra-natapoff/punishment-without-crime/9780465093809/

[53] Bryce Newell. 2017. Collateral Visibility: A Socio-Legal Study of Police Body Camera Adoption, Privacy, and Public Disclosure in Washington State. *Ind. L. J.* 92, 4 (Oct. 2017). https://www.repository.law.indiana.edu/ilj/vol92/iss4/2

[54] Chris Oakes. 1998. 'E911' Turns Cell Phones into Tracking Devices. *Wired* (Jan. 1998). https://www.wired.com/1998/01/e911-turns-cell-phones-into-tracking-devices/

[55] J C O'Brien. 2008. Loose Standards, Tight Lips: Why Easy Access to Client Data Can Undermine Homeless Management Information Systems. *Fordham Urb. L.J.* 35, 3 (2008), 29. https://ir.lawnet.fordham.edu/ulj/vol35/iss3/5

[56] Ihudiya Finda Ogbonnaya-Ogburu, Angela D.R. Smith, Alexandra To, and Kentaro Toyama. 2020. Critical Race Theory for HCI. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. ACM, Honolulu HI USA, 1–16. https://doi.org/10.1145/3313831.3376392

[57] Thomas O'Malley. 2011. Using Historical Cell Site Analysis Evidence in Criminal Trials. *The United States Department of Justice Attorney Bulletin* 59 (Nov. 2011), 16–35. www.usdoj.gov/usao/reading_room/foiamanuals.html

[58] Richard A. Jr. Oppel and Jugal K. Patel. 2019. One Lawyer, 194 Felony Cases, and No Time. *The New York Times* (Jan. 2019). https://www.nytimes.com/interactive/2019/01/31/us/public-defender-case-loads.html,https://www.nytimes.com/interactive/2019/01/31/us/public-defender-case-loads.html

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

[60] Desmond Upton Patton, Douglas-Wade Brunton, Andrea Dixon, Reuben Jonathan Miller, Patrick Leonard, and Rose Hackman. 2017. Stop and Frisk Online: Theorizing Everyday Racism in Digital Policing in the Use of Social Media for Identification of Criminal Conduct and Associations. *Social Media + Society* 3, 3 (July 2017). https://doi.org/10.1177/2056305117733344

[61] Desmond Upton Patton, Robert D. Eschmann, Caitlin Elsaesser, and Eddie Bocanegra. 2016. Sticks, stones and Facebook accounts: What violence outreach workers know about social media and urban-based gang violence in Chicago. *Computers in Human Behavior* 65 (Dec. 2016), 591–600. https://doi.org/10.1016/j.chb.2016.05.052

[62] Elissa M. Redmiles, Sean Kross, and Michelle L. Mazurek. 2017. Where is the Digital Divide? A Survey of Security, Privacy, and Socioeconomics. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (CHI '17)*. ACM, New York, NY, USA, 931–936. https://doi.org/10.1145/3025453.3025673

[63] J. Reidenberg, N. C. Russell, Alexander J. Callen, S. Qasir, and Thomas B. Norton. 2014. Privacy Harms and the Effectiveness of the Notice and Choice Framework. *Information Privacy Law eJournal* (2014). https://doi.org/10.2139/SSRN.2418247

[64] Aaron Shapiro. 2019. Predictive Policing for Reform? Indeterminacy and Intervention in Big Data Policing. *SS* 17, 3/4 (Sept. 2019), 456–472. https://doi.org/10.24908/ss.v17i3/4.10410

[65] Yotam Shem-Tov. 2018. *Are Public Defenders Better at Indigent Defense than Court-Appointed Attorneys?* Technical Report. California Policy Lab, UC Berkeley. 3 pages. https://escholarship.org/uc/item/8737p1hb

[66] Lahny R Silva. 2015. Collateral Damage: A Public Housing Consequence of the "War on Drugs". *U. Ca. Irvine L. Rev.* 5, 4 (Nov. 2015), 783–812.

[67] Angela D. R. Smith, Alex A. Ahmed, Adriana Alvarado Garcia, Bryan Dosono, Ihudiya Ogbonnaya-Ogburu, Yolanda Rankin, Alexandra To, and Kentaro Toyama. 2020. What's Race Got To Do With It? Engaging in Race in HCI. In *Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems (CHI EA '20)*. ACM, New York, NY, USA, 1–8. https://doi.org/10.1145/3334480.3375156

[68] Jennifer Lynch and Nathaniel Sobel. 2020. New Federal Court Rulings Find Geofence Warrants Unconstitutional. https://www.eff.org/deeplinks/2020/08/new-federal-court-rulings-find-geofence-warrants-unconstitutional-0

[69] Jay Stanley. 2015. *Police Body-Mounted Cameras: With Right Policies in Place, a Win For All.* Policy Report. American Civil Liberties Union. 6 pages. https://www.aclu.org/other/police-body-mounted-cameras-right-policies-place-win-all

[70] Angelika Strohmayer, Jenn Clamen, and Mary Laing. 2019. Technologies for Social Justice: Lessons from Sex Workers on the Front Lines. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. ACM, Glasgow Scotland Uk, 1–14. https://doi.org/10.1145/3290605.3300882

[71] Lucy Suchman and Brigitte Jordan. 1990. Interactional Troubles in Face-to-Face Survey Interviews. *J. of the American Statistical Assoc.* 85, 409 (1990), 232–241. https://doi.org/10.2307/2289550 Publisher: [American Statistical Association, Taylor & Francis, Ltd.].

[72] Jennifer Valentino-DeVries. 2019. Tracking Phones, Google Is a Dragnet for the Police. *The New York Times* (April 2019). https://www.nytimes.com/interactive/2019/04/13/us/google-location-tracking-police.html,https://www.nytimes.com/interactive/2019/04/13/us/google-location-tracking-police.html

[73] Cornelia Vismann. 2008. *Files: Law and Media Technology.* Stanford University Press, Stanford.

[74] Peter Wagner and Wendy Sawyer. 2020. Mass Incarceration: The Whole Pie 2020. https://www.prisonpolicy.org/reports/pie2020.html

[75] Robert Stuart Weiss. 1995. *Learning from strangers: the art and method of qualitative interview studies* (first free press paperback ed ed.). Free Press, New York. OCLC: 34292390.

[76] Rebecca Wexler. 2017. Life, Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System. *Stan. L. Rev.* 70 (2017). https://doi.org/10.2139/ssrn.2920883

[77] Rebecca Wexler. 2019. Privacy Asymmetries: Access to Data in Criminal Investigations. *UCLA L. Rev* 68, 212 (July 2019), 76. https://doi.org/10.2139/ssrn.3428607

[78] Cedric Deslandes Whitney, Teresa Naval, Elizabeth Quepons, Simrandeep Singh, Steven R Rick, and Lilly Irani. 2021. HCI Tactics for Politics from Below: Meeting the Challenges of Smart Cities. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. ACM, Yokohama Japan, 1–15. https://doi.org/10.1145/3411764.3445314

[79] Stacy E. Wood. 2019. Policing through Platform. *Computational Culture* 7 (Oct. 2019). http://computationalculture.net/policing-through-platform/

Table 2. Coding for technology stories, with type of technology and type of challenge

| Types of Barriers | Types of Technology |
|---|---|
| **Resource Constraints**<br>• Lack time<br>• Lack specific tools<br>• Lack of scientific understanding<br>• Lack of technical knowledge or skills | **Audio & Video**<br>• Body camera footage<br>• Dash cameras<br>• Public surveillance cameras<br>• Private surveillance cameras<br>• Jail call recordings |
| **Organizational Constraints**<br>• Lack of process internally<br>• Lack of process in jurisdiction | **Digital Forensics**<br>• Social media data<br>• Device extraction (Cellebrite)<br>• Geo-location phone information<br>• Search, test, or call history |
| **Legal Barriers**<br>• Inability to subpoena<br>• Lack of legal access<br>• Intellectual property or trade secrets | **Forensics**<br>• Breathalyzer results<br>• Blood test results<br>• DNA test results<br>• Ballistics<br>• Medical reports<br>• Bite or bruise analysis |
| **Structural Barriers**<br>• Excluded from partnerships with private companies<br>• Lack of control over data format<br>• "Bunk science"<br>• Difficulty getting expert witnesses | • **Office Technology**<br>• Communicating with clients in jail<br>• Wifi<br>• Laptops or phones<br>• Case management software<br>• Criminal database access |
| | **Other**<br>• Historical cell site data<br>• Cell site simulators (stingrays)<br>• License plate readers<br>• Facial recognition technology |

## APPENDIX

Received July 2021; revised November 2021; accepted November 2021.

Table 3. Characteristics of participants

| | Title | Types of Cases | Jurisdiction | Region | Experience |
|---|---|---|---|---|---|
| P1 | Public Defender | Felony | County | Northeast (Urban) | >10 years |
| P2* | Chief PD | Felony | County | California (Urban) | >10 years |
| P3* | Deputy PD | Felony | County | Same as P2 | >10 years |
| P4* | Deputy PD | Felony | County | Same as P2 | >10 years |
| P5 | Federal Public Defender | Cyber Crimes | Federal | California | >10 years |
| P6 | Researcher, EFF | - | - | - | - |
| P7 | Paralegal | All | County | California (Urban) | 3 years |
| P8 | Indigent Assigned Council | Misdemeanors | State | Northeast | >20 years |
| P9 | Former Public Defender | Misdemeanors | County | Northwest | 2 years |
| P10 | Public Defender | Misdemeanors | County | California (Urban) | New |
| P11 | Public Defender | Capital Crimes (Formerly Felony) | State | Midwest | >10 years |
| P12 | Public Defender | Felony | County | Midwest | 2 years |
| P13 | Public Defender. | Felony (Formerly Misdemeanors) | County | Office X | 3 years |
| P14 | Public Defender | Misdemeanours | County | Northeast | 1 year |
| P15 | Public Defender | Misdemeanours | County | South West | 1 year |
| P16 | Investigator, PD office | Felony | County | Office X | ~years |
| P17 | Prosecutor | Felony, cybercrimes | County | Office X | >10 years |
| P18 | Public Defender | Felony (Formerly Misdemeanors) | County | Office X | 4 years |
| P19 | Public Defender Intern | Felony (Formerly Misdemeanors) | County | Midwest | 5 years |
| P20 | Investigator | Felony | County | Office X | >10 Years |
| P21 | Legal Services Rep at Tech Company | - | - | - | 3 years |