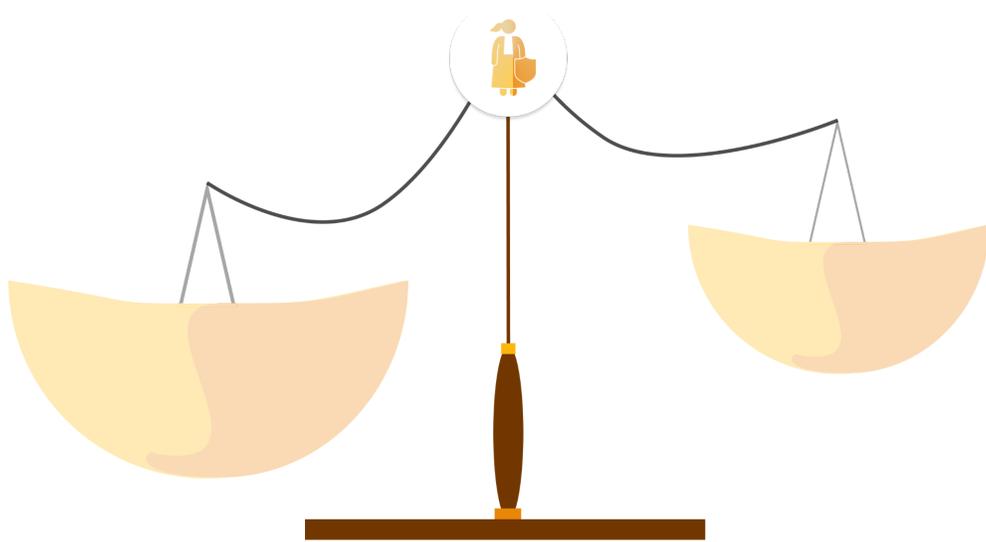


The Public Defense Project

Exposing the technology needs of Public Defenders & their community



Team Members

Jyen-Yiee Wong | Rachel Warren | Sneha Chowdhary | Tiffany Pham

Faculty Advisor & Mentor

Prof. Niloufar Salehi | Steve Trush



Acknowledgements

We would like to thank Brian Hofer, executive director of Secure Justice, for the opportunity to collaborate on this project and for providing us with early feedback on how best to highlight opportunities for technologists and privacy advocates to support public defense work. We would like to thank Steve Trush and Professor Niloufar Salehi for their support throughout the project—their willingness to provide guidance and feedback to the team, from beginning to end, is deeply appreciated. We are also grateful to the entirety of the ISchool faculty, who shared their knowledge with us over the past two years and whose courses directly informed the execution of our project.

Furthermore, we would like to thank the Center for Technology, Society, and Policy and the Center for Long-term Cybersecurity for their initial funding of our project which propelled our initiatives even further.

Lastly, we would like to thank all of the public defenders, public defense staff, legal scholars, and technologists who trusted us to listen to them and tell their stories through The Public Defense Project.

Acknowledgements	1
Abstract	3
Background & Motivation	4
Problem Space	5
Motivation	8
Process	8
Methods	8
Needs Assessment	12
Findings	13
Surveillance Data	13
Case Management Capabilities	21
Information Sharing Tools	26
Depicting Power Imbalance in the Criminal Justice System	29
Website Design	32
Discussion & Impact	44
Design Implications	44
Policy Implications	46
Conclusion & Recommendations for Future Work	49
MIMS Impact	51
Works Cited	52
Appendix	54
Appendix A: Link to The Public Defense Project Website	54
Appendix B: Interview: Participant Consent Form	54
Appendix C: Link to all Surveillance Technologies & Resources Encountered	54
Appendix D: Public Defender Interview Guide	54
Appendix E: Storyboard Images	54
Appendix F: Data Visualizations	56
Appendix G: Final Deliverable - Website Screenshots	58



Abstract

Public defenders serve as an essential bulwark against wrongful arrest and incarceration for low-income and marginalized people accused of crimes. Though public defenders have long been overworked and under-resourced, these issues have been compounded by boosts in the volume and complexity of data in modern criminal defense cases. For example, new technologies such as historical cell site information, GPS location history, automatic license plate readers, and social media data are now commonly used to build a case. As the technology landscape changes, we must address the consequent technical and political needs of public defenders. We, therefore, outline the significant challenges that public defenders face when handling data and technology, identify opportunities for technical and political solutions, and describe constraints that technologists and privacy advocates should consider as they pursue solutions. We focus, in particular, on opportunities to improve surveillance data extraction and processing methods for public defenders, opportunities to expand case management and database management capabilities, and opportunities to explore data and resource sharing for public defenders within and between public defense offices.



Background & Motivation

Our capstone project stems from an interest in understanding how public defenders manage data and technology in modern criminal defense cases. The goal of our project was to identify opportunities—both technical and political—that could help public defenders navigate the use of data and technology in their cases. With rises in the volume and complexity of data used by law enforcement and prosecutors—and, in turn, rises in the volume and complexity of data received by public defenders, we believe that outlining opportunities to improve public defender data workflows is crucial to greater criminal justice reform.

Finally, our project is in partnership with Secure Justice, an Oakland-based nonprofit that advocates for greater privacy reforms, and in particular, the regulation of surveillance technologies in the criminal justice and immigration systems. In collaboration with Secure Justice and with advice from Professor Niloufar Salehi and Steve Trush, we outline the major challenges that public defenders face when handling data and technology, identify opportunities for technical and political solutions, and describe constraints that privacy advocates and technologists should consider as they pursue solutions.

Ultimately, we hope that our work can lay some groundwork for more outstanding technical and political advances in this space.

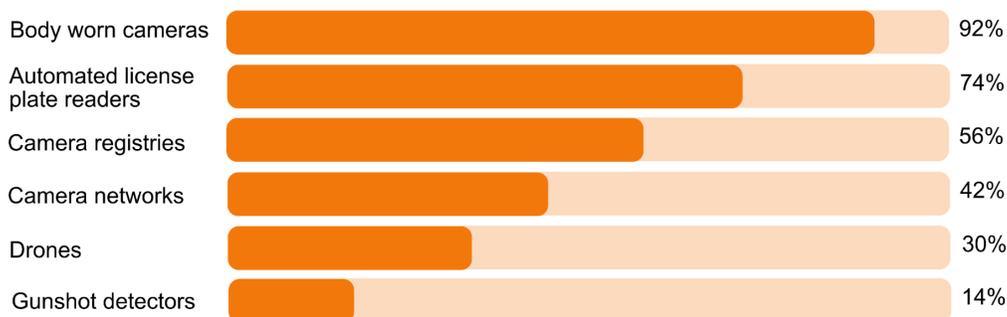
Problem Space

Though public defenders have long been overworked and under-resourced, these issues have been compounded by rises in the volume and complexity of data in modern criminal defense cases. New technologies such as historical cell site information, GPS location history, automatic license plate readers, and social media data are now commonly used to build a case. Legal scholars and activists have also raised alarm that data increasingly flows into the criminal justice system by opaque partnerships between law enforcement and private technology companies.¹

Below, you can see how the use of data and technology by law enforcement has manifested in the Bay Area. The use of these technologies, and the data collected from them to build a prosecutor's case, directly impacts the ability for public defenders to adequately defend their clients.

Popular Technologies Used by Bay Area Law Enforcement

In an analysis of technologies used by agencies within 50 Bay Area cities, the percentage who use the following:



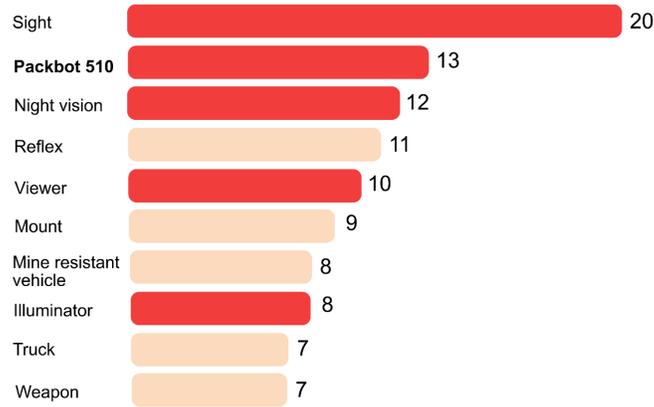
Source: Shelby Perkins and Craig Nelson, Stanford University's Freeman Spogli Institute

FIGURE 1. Visualization depicting popular technologies used by the Bay Area Law Enforcement

¹ See Joh 2017 for an in depth discussion of body cameras, cell site simulators and algorithmic technologies built by private (usually monopoly) companies and purchased by law enforcement.

Many of the most common federally granted technologies concern surveillance

An analysis of the most frequently cited words in federal grants given to Bay Area law enforcement



Source: ABC7-I Team Analysis of Records from the Defense Logistics Agency

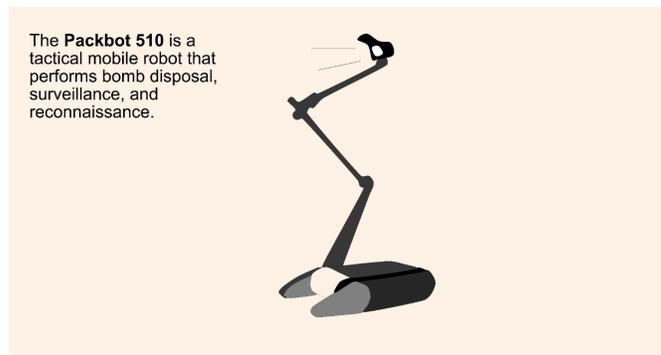


FIGURE 2. Visualization depicting federally granted technologies concerning surveillance

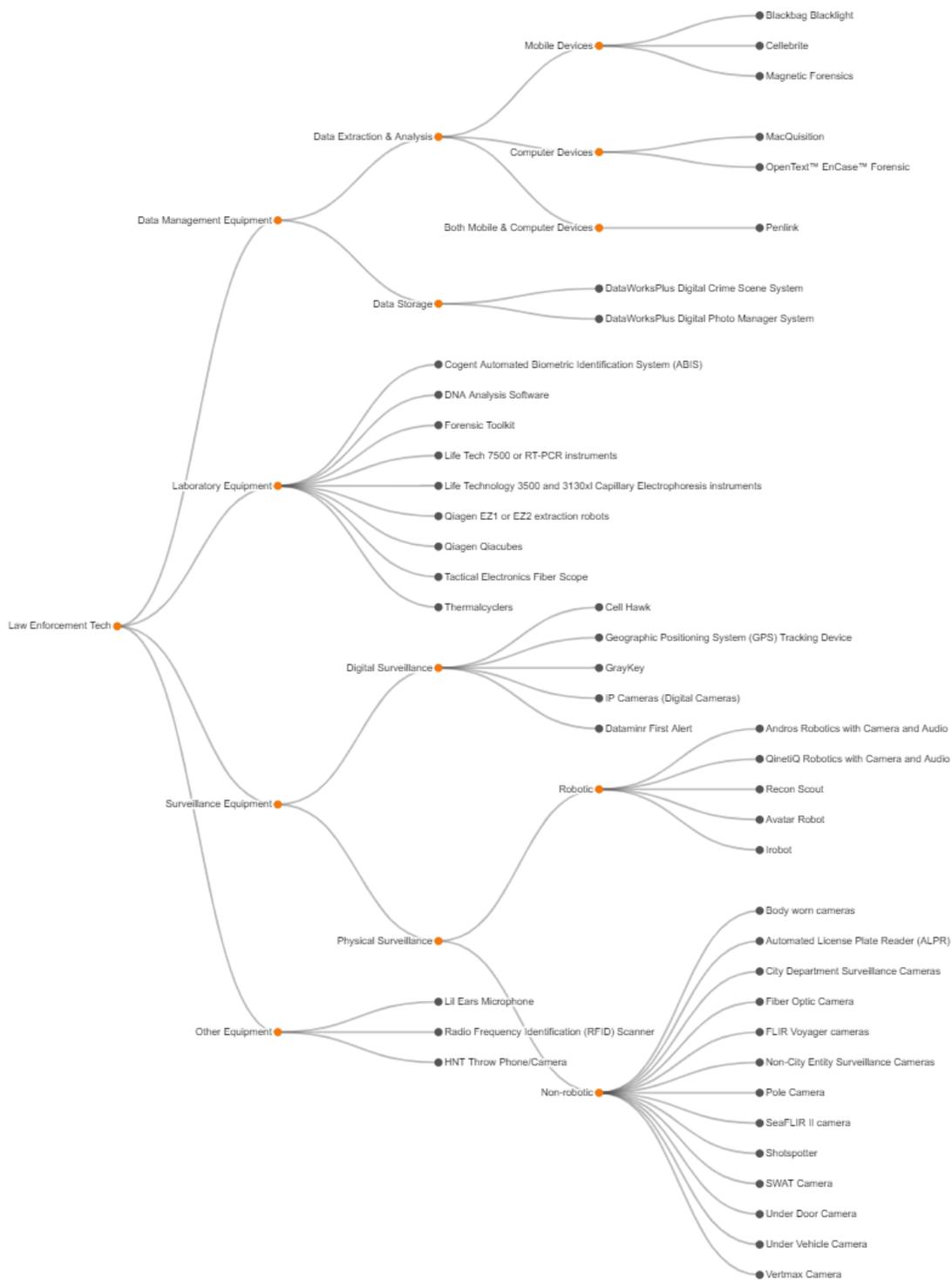


FIGURE 3. Visualization depicting Bay Area Law Enforcement technologies



Motivation

While prosecutors may receive internal data resources from federal organizations as well as insights about said resources from technology providers, public defenders often have neither the data analysis skills nor the external support to apply those resources in their cases. Public defenders may also be ignorant of the existence of emerging technologies or unable to identify the limitations of said technologies as they are presented or deliberated on by law enforcement, prosecution, judges, and juries. For these reasons, we were interested in understanding how public defenders currently manage data in their cases, with the hopes of identifying opportunities—technical and political—to support their work.

Process

Methods

Semi-structured Interviews

We conducted a series of semi-structured interviews with technologists, privacy advocates, legal scholars, and members of the public defense community to surface insights about the use of data and technology in modern criminal defense cases. We chose to conduct semi-structured interviews because very little literature



exists concerning data workflows for public defenders and as such, our research was highly generative.

In total, we conducted semi-structured interviews with 22 participants. The participant breakdown was as follows: 15 former or current public defenders, 2 paralegals, 2 investigators, 1 legal scholar, 1 privacy advocate and technologist, and 1 policy specialist at a major tech company. The public defenders were a mix of federal and state public defenders. Of the current and former public defenders we interviewed, 9 were located in the Bay Area.

Sampling

The first eight interviewees were selected through a snowball sample from our network focusing on experts and people with a range of experience around indigent defense (Lofland & Lofland 1995). For example, we interviewed senior public defenders, someone who had built technology for the Electronic Frontier Foundation (EFF), and someone who worked with the nationally renowned Bronx Defenders non-profit.

For the second phase of the project, we sought out currently practicing Public Defenders (PDs). We posted in the public defender subReddit *r/public_defenders*, asking for volunteers to talk about their work experience. We received enough responses to conduct some focused sampling. We focused on public defenders who would have experience working on cases with higher volumes of discovery -- including cyber crimes and felonies, as well as those who had previous experience



working in prosecutors or district attorneys' offices. After interviewing participants working across the country we also conducted 6 interviews from people working in the same jurisdiction in northern California in order to develop a full picture of one PD office.

Interview Format

18 of the 22 interviews were conducted remotely. Each interview was approximately one hour long. For each interview, we prepared an interview guide catered to that participant's background (e.g. as a public defender, a paralegal, or other role). Ahead of each interview, we acquired written and verbal consent from the participant to conduct (and, when permission was granted, record) the interview. We also shared a subset of the questions we would be asking them during the interview in advance.

A **sample set of questions** we shared with public defenders can be reviewed below:

1. We're interested in the use of data resources or technology in prosecution and public defense. Can you describe a past case that stands out to you in terms of its use of data resources?
2. What information resources/data do you normally refer to or respond to during a case?
3. Have you encountered any challenges with collecting or using data or information technology in a case?
4. Do you use any tools or technologies to help you do your work?



5. What types of data do you encounter from prosecutors or law enforcement?

After conducting the interviews, we applied a modified version of the Grounded Theory Method to analyze the data, most closely resembling the approach described in Charmaz's 'Constructing Grounded Theory: A Practical Guide through Qualitative Analysis'. Specifically, we (for recorded interviews) uploaded interviews into automated transcription software, corrected for errors in transcription, reviewed interview transcripts, and developed codes concerning data workflows and stoppages in the criminal justice system and as experienced by public defenders.

More granularly, we reviewed transcripts for information about organizational structures (e.g. participants' understanding of structures and dynamics within a public defense office and outside of an office), specific stories about a participants's experiences encountering various technologies in their work, and stories about their data management workflows and access to resources. We further divided stories by topic (most commonly, by technology implicated in the story). For some technologies, we 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 footage in discovery, but their process of selecting videos and the extent to which they felt their representation suffered due to this filtering varied.



Next, we built a spreadsheet organized by the participant, type of technology referenced, and the type(s) of problems associated with that technology. Each team member reviewed interview transcripts and notes and extracted relevant information to be added to the spreadsheet. Further, team members rotated the review of an interview transcript, such that each interview transcript had several layers of analysis and extraction from multiple team members. We also collated the numerous suggestions for tools and advocacy work proposed by the participants. We used this process of coding as the basis for our needs assessment.

Needs Assessment

After applying the Grounded Theory Method to surface themes from our interviews, we wrote an initial whitepaper outlining the structural and technical challenges that public defenders face.

In terms of the structural challenges that public defenders face, the whitepaper highlighted the poor systems for communication between and within public defense offices, as well as the lack of investment in opportunities for public defenders to acquire knowledge, training, and resources on data and technology. The whitepaper also touched upon technical challenges, such as public defenders' difficulties engaging in data extraction, processing, and management.

Writing the whitepaper helped us, at a high level, create a framework for understanding some of the major structural and technical needs that public defenders had. And by reviewing our whitepaper as well returning to our other



research artifacts (such as our notes, annotated transcripts, and coding spreadsheets), we were able to select a subset of the major problem areas and engage in deep dives of how these problems manifest in public defenders' day-to-day work and their needs.

Findings

Of the major problem areas for public defenders, we selected three areas to focus in on: surveillance data extraction and analysis, case management capabilities, and resource coordination and sharing within and between public defense offices.

We selected the three problem areas after considering the *frequency* with which public defenders cited them as first-hand problems, as well as the *significance* of these problems (as they concern public defenders' abilities to defend their clients). In addition, we believe these specific problem areas are rich with opportunities for technologists and advocates to engage in meaningful technical and political work. We outline our findings in the three major problem areas below.

Surveillance Data

Public defenders uniformly felt that the ability to review new surveillance data such as body camera footage, surveillance videos, and social media reports was critical to adequately representing their clients. However, a lack of time and resources made it difficult for this opportunity to be realized.



Interpretation Matters

Public defenders were clear that spending time reviewing new evidence improved their likelihood of winning cases. In particular, most, but not all forms of discovery come in two parts: “raw data”, e.g., body camera footage, social media feeds, or blood samples, and a “report” such as a police report or lab report. Public defenders uniformly felt that these reports and summaries—surveillance video complications from private vendors, breathalyzer results, police reports—could be untrue, or unfair to their clients and that it was useful for them to examine that “raw” data to make their own story.

For example, although a description of interviews and arrest is provided in the police report, body-worn cameras very often provided valuable information for public defenders: revealing inaccuracies in police reports, identifying new witnesses, and simply in context for future interviews with victims and witnesses. “It’s a significant amount of video... And you are required to watch it. It can break a case,” summarized one public defender.

Use of social media data in a case illustrates the dangers of allowing prosecutors the only interpretation of raw data. Several participants explained how, armed with access to the full history of someone’s social media, law enforcement officials and prosecutors could often extract a few exchanges to paint a narrative of criminal intent. For example, a public 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." However, upon examining their full social media records and public records from the client's peers, the public defender found that the language the client used was routine amongst his acquaintances, who made similar "shock value" jokes. Several public defenders described arguing over the meanings of emojis or slang posted on social media, for example whether a gun emoji and the "hundred percent" emoji were sufficient evidence that a client was armed 100 percent of the time or if both were merely used for emphasis.

The importance of providing an opposing interpretation to the same data was not unique to video and social media data. Now that he has more resources, a capital defender explained that he hires his own expert to go over 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?”



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

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), would include several hours of video. Felony cases could have up to 150 or 200 hours. The pain points around surveillance video were not just related to quantity, but included technical problems playing, transferring, downloading, and editing video. Most talked about spending hours and days trying to watch videos from private surveillance companies, which often could only be viewed in proprietary software. Though all agreed that these technical hurdles rarely prevented them from ever watching videos, these issues could certainly slow down a case and can delay a client's release from jail.

As with body camera footage, adequately parsing through social media reports could be prohibitively time consuming and cumbersome. Public defenders stated that Facebook and Instagram feeds, received through prosecutor's warrants, were often delivered as unstructured PDFs and might be tens of thousands of



pages long. A public defender clarified that discovery laws did not require prosecutors release this discovery in its native more structured format and that, in these cases, they just had to "deal with it." A few younger defenders and paralegals described writing scripts to parse through social media PDFs, duplicate body camera footage, and digital forensics reports.

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, public defenders often do not have access to digital forensics tools such as Cellebrite machines which are used to extract data from physical devices. 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 shots spotter history. One public defender described being "laughed" at when he gave experts a quote for what he could pay them.

Structural Advantages of Prosecutors

Interviewing public defenders illuminated the extent to which defense and local district attorneys are part of a larger 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. Public defenders most



commonly interact with data as it is delivered as discovery from prosecutors, which allows prosecutors greater control over the format and structure of the data.

As it concerned receiving data through discovery, public defenders described many instances of how this process led to deep data processing disadvantage. For example, a public defender noted that the prosecutor's office could internally tag text conversations which they extracted from Cellebrite (mobile device data), but would provide the defense counsel with the original un-tagged and unsorted version as a PDF. Senior Public defenders in California described how, due to an upgrade to the jail calls database in their area, they received hundreds of hours of jail calls in a file format they didn't have the tools to play—just a few weeks before an important court date. Regardless of ill intent, public defenders often receive data from complex, multi-stakeholder technical systems for which they were provided very little input.

Public defenders felt particularly disadvantaged with regards to interacting with private companies, who often work in proximity to law enforcement. Public defenders most often see third hand data—having been collected by a private institution, subpoenaed by law enforcement, and then shared to public defenders. Worse, some data comes through law enforcement via contracts.

For example, an investigator described an instance where public housing units contracted with WatchTower, a private video surveillance provider.² Police

² See: the 2017 SF housing authority report <https://sfha.org/PROPOSED%20ANNUAL%20PLAN/Annual%20Plan%202017.pdf>



may call WatchTower 24 hours a day to describe an incident they believe to have occurred. The company will then provide police with a video montage of the incident, who after an arrest may share the video with prosecutors, who then discover the highly edited video to public defenders. Thus, the montage enters the public defense office after passing three adversarial hands: the police, the private company, and the prosecutor's office.

Partnerships with Private Companies

Public defenders' frustrations with public and private partnerships took three forms, all with legal origins. The first perceived problem was companies' unwillingness to comply with subpoenas and limited legal mechanisms to get the same data as prosecutors. Public defenders directed animosity toward private companies rather than the legal structures in place. When asked if legal or technical hurdles prevented him from getting full access to social media data, a public defender replied:

“ *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.”*

While laws could be passed requiring Facebook to respond to subpoenas from the defense and penalizing slow or incomplete response, the spirit of this



comment speaks to a 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 District Attorney (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.

Second, public defenders resented being denied access to surveillance tools for intellectual property reasons. One public defender stated,

“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.”

Although a federal public defender we spoke with did have access to a Cellebrite machine there are other instances, such as shot spotter data and stingray machines where companies have argued that trade secrets prevent them from revealing the data or workings of technology in court (Joh 2017). Another public defender stated that although he felt the DNA lab in his district was unbiased, he wanted access to the analysis software, which is “trade secrets that the company



will not allow us to look at.” In short, public defenders felt that the black box of surveillance tools made addressing potentially faulty data evidence difficult.

Third, public defenders were concerned that the federal government had a “voice at the table” when designing surveillance infrastructure such as cell phone towers, and that prosecutors were then aided or trained by the federal government. Pressure from law enforcement can indirectly lead companies to build technical infrastructure to support law enforcement surveillance. In our interview with a policy specialist at Google, they explained that Google had needed to build new technical infrastructure in order to process geofencing warrants when the volume of these warrants—which require searching on a bounding box rather than by user ID—increased dramatically. It is worth noting that concerns about how indirect and direct pressure from law enforcement can expand and tailor surveillance infrastructure is well documented through independent reporting and the legal literature.³

Case Management Capabilities

Public defenders and public defense staff frequently expressed a need for better case management and database management software. Several factors exist to make case management and database management uniquely challenging for public defenders.

³ See: Joh 2017. A stark example of this is E-911 technology which enables emergency calls to be traced but also includes a mechanism for revealing the geolocation of a phone. See Futch 2012.

First, public defenders grapple with extremely high caseloads—often exceeding the recommended maximums for a public defender.⁴ For example, below you can see the extent that public defenders' caseloads consistently exceed or nearly exceed recommended maximum caseloads in Alameda County.

Public defender annual caseloads in Alameda County

The U.S. Department of Justice's National Advisory Commission (NAC) on Criminal Justice Standard and Goals has recommendations on maximum annual caseloads for a public defender office. Below is a chart comparing Alameda's public defenders to the recommended amount.

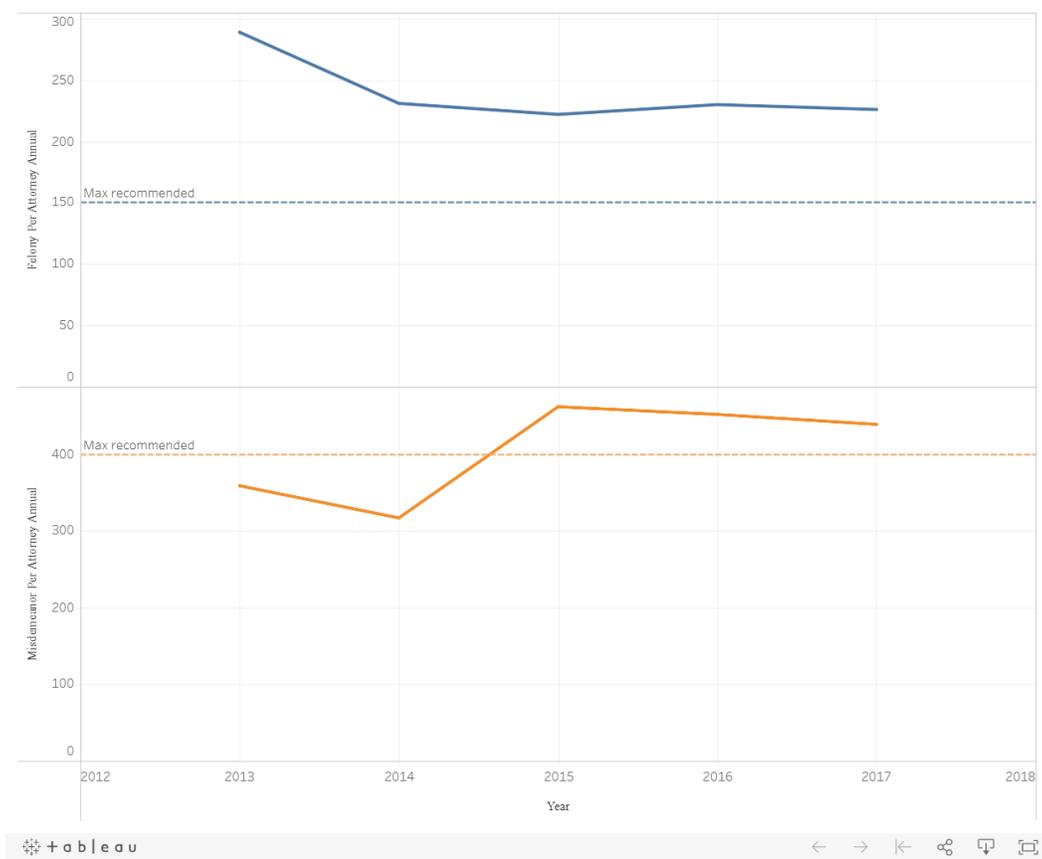


FIGURE 4. Public defenders annual caseloads in Alameda County

Having high caseloads amplifies any potential pain points with case management and database management software. For public defenders, existing

⁴ See the 2010 census of the public defender, which estimates that 70% of public defense offices exceed per-attorney caseload recommendations of 400 misdemeanours and 150 felonies.

case management and database management software fails to accommodate for the sheer volume of cases they have. One public defender shared,



There is our internal database where we have notes on what we do in clients' cases. Then there's another database where we can see people's criminal history and custody status. And there's a third database where we see people's court dates and court papers. And it's like... if you just have 10 clients [that's] not a problem, but caseloads are looking more like 150 to 200 misdemeanor cases per attorney in the office I'm working in."

Public defenders and staff consistently discussed the “scavenger hunt” nature of managing their cases. Rather than have a consolidated or centralized system to access relevant information for their cases, public defenders instead have to search through upwards of five different database systems and repositories to carry out work on a particular case. The databases and repositories that a public defender must access on a daily basis can include: an internal database for client information and attorney notes, a law enforcement database with criminal history and custody status, a court database with minute orders and filings, an internal shared drive for miscellaneous items and files too large for the internal client database, and an



online legal research suite. While accessing these multiple databases and repositories may be tenable for a public defender working a handful of cases, many public defenders are working upwards of hundreds of cases. Public defenders would greatly benefit from a case management system that reduces the burdens of having multiple, independent points of data access.

“ I think we in the public defense world do live in a constant state of tech, jealousy, and bitterness. I remember the Denver DA's office, we're in court with them every day. I saw their laptops. I saw, they had this sparkly case management system and they had all these cool tech things. They had this special in-office phone app and stuff and, and just all these nice things that we just never would get.”

Second, with the vast and varied forms of data that now characterize modern criminal defense cases, public defenders would benefit from a system to integrate disparate data types. From jail call recording to social media reports, public defenders are managing increasingly voluminous and complex data using systems neither equipped nor optimized to manage them within a case (and across multiple cases). One public defender exclaimed,



I'm not so dissatisfied with the lack of training as I am with the actual software that we use."

Third, a single case can be managed by multiple members of a public defense office. In addition to a public defender, other parties involved in a single case can include paralegals, investigators, and experts. Furthermore, the structure of the public defense office, such as whether it is vertical (i.e. a public defender handles a case from start to end) or horizontal (i.e. multiple public defenders handle a case, with each public defender responsible at a specific stage), can also complicate the use of case management and database management software. As such, public defenders lack comprehensive systems to coordinate shared work in a case. This challenge is amplified by inconsistent standardization of file naming formats among the different people involved in a case, as well as their different approaches to data entry.



Some people would write in the physical file. Other people write it on the electronic database sometimes not at all. So, it's a little all over the map."

To carry out their work, public defenders must use case management and

database management software on a daily basis. As such, improvements in this area would significantly and very meaningfully impact public defender workflows. Meaningful improvements in this space would concern case management that optimizes specifically for managing large caseloads, integrate multiple sources of data, and afford for easier coordination of work.

Information Sharing Tools

A common theme in our interviews was a lack of knowledge and a lack of ability to share knowledge. A better network for information sharing between public defenders would be useful in three areas: for sharing example case law and resources about new forms of technical and scientific evidence, a place to find and vet experts, and a place to organize around structural problems.

A lack of information resources about new technologies was a common source of difficulty for public defenders. Participants expressed a need for information resources to guide early motions and briefs, before they would have time to hire an expert. Some also struggled to understand the science behind routine evidence such as blood tests and breathalyzers.



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,”

explained a misdemeanor defender. This participant felt she fundamentally lacked the scientific training to make sense of the breathalyzer and blood test results which made up a significant part of her caseload. Other participants felt that this process was a matter of learning by doing.

Connecting public defenders who are more comfortable with different kinds of evidence to those who are not might help new public defenders come up to speed. Furthermore, public defenders seem to move jobs and offices relatively often. Several participants described collating resources about particular technologies or developing expertise at previous jobs without ever passing along that knowledge.

Another common pain point was **finding reliable and trustworthy expert witnesses**. Experts are needed for a variety of data and technology analyses, and there is no easy way for public defenders to identify experts who are willing to testify in court. In addition, public defenders cited difficulties in assessing when an expert is qualified to conduct data and technology analyses—what type of experience and credentials, for example, should an expert have in order to speak on a particular data or technology. Currently, word-of-mouth is the most common means through which public defenders acquire experts for their cases.



Lastly, public defenders have an important vantage point into bias and equality in the criminal justice system, but they often lack the write forum to document their findings, compare stories across offices or organize. For example, one Bay Area public defender described how attorneys in his office were concerned about bias in sentencing and had decided to keep records, but were doing so in an individual ad hoc way.

“ So each attorney will be told, ‘Hey, we are seeing that clients with X and Y charges, um, who are black, are being denied bail really often. Could you keep a spreadsheet of these cases?’ And then individual attorneys will keep spreadsheets and then we’ll send these spreadsheets [to] one person to consolidate the data. I just wonder if there is a more efficient way to do that.”

Similarly, a federal public defender explained that sometimes he would talk to state defenders who were seeing different records in discovery, but that these relationships were ad hoc. “Communication definitely happens,” he explained, “but that’s more on a personal.. micro level, rather than ... like let’s all band together and, you know, have presented a united front.” In an ideal world, public defenders across offices, especially those in places where algorithmic tools are increasingly being deployed, would have a unified mechanism for recording their observations.



Design Process

After developing our findings, our goal was thereafter to communicate them as effectively as possible to technologists and advocates. In our approach to communicating our findings, we collaborated with Secure Justice—specifically, Brian Hofer, executive director of Secure Justice—to best frame our findings in support of Secure Justice’s work.

Depicting Power Imbalance in the Criminal Justice System

As a major theme in our findings, we wanted to call attention to the information disparity between public defenders and prosecutors. A core assumption of all social exchange theories is that “exchange relations develop within structures of mutual dependence between actors,” though actors need not be equally dependent on one another (Molm, Cook 1995).

From our interviews, we understood that exchanges and transactions between public defenders and other key actors in the system (such as law enforcement and prosecutor) were reciprocal direct exchanges⁵. Prosecutors receive internal data resources from federal organizations as well as insights about technology resources from tech providers. Public defenders sparingly receive the same information or access to it. In order to present this data disparity in the criminal justice system and the flow of information between involved actors, we

⁵ In **Reciprocal Direct Exchanges** the contributions to the exchange are separately performed and non-negotiated. One actor initiates the process without knowing whether or when the other will reciprocate (Molm, Cook 1995)

sketched out a flow diagram (left below). The diagram indicates what is being exchanged in terms of private and public data sources, between whom, and whether this exchange is legally or non-legally mandated.

Through initial rounds of feedback, we learned that viewers found it challenging to grasp the concept of social information exchange and felt a lack of context.

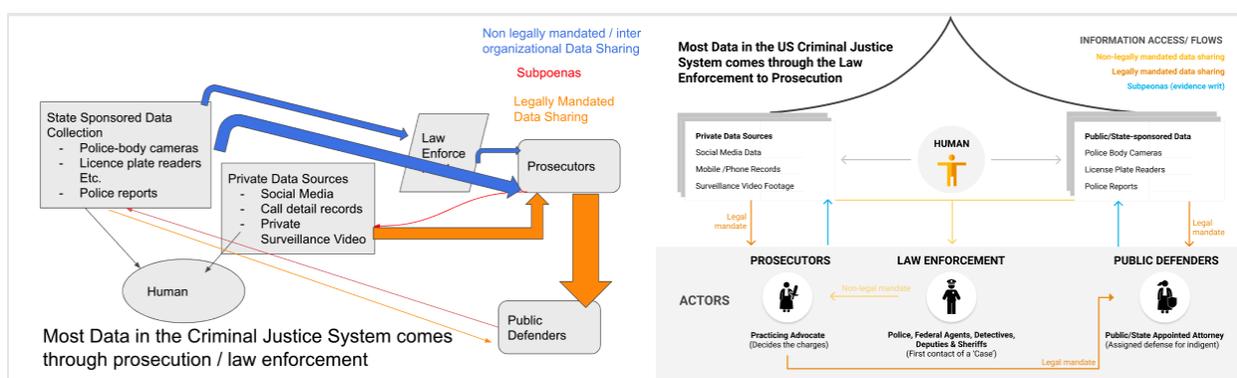


FIGURE 5. Iteration 1 & 2: Social Information Exchange in the US Criminal Justice System.

We decided to iterate on our flow diagram, creating an information visualization using Visualization Heuristics⁶ picked up in our Information Visualization and Presentation class. Heuristics we particularly focused on, included:

- (1) Supporting key visual insights of qualitative data involved (types of private and public sources, actors) and highlighting comparisons (using the balance scale to depict where the weight of information disproportionately sits)

⁶ Heuristic Evaluation & Visualization Heuristics, Course: *Information Visualization and Presentation* by Prof. Marti Hearst. Week 4, Slide 15

- (2) Using principles of organization and color consistency to reduce clutter and improve blank space
- (3) Presenting visual information honestly based on findings from our interviews and with an exception for slanted text
- (4) Communicating to engage the viewer while also telling a story with the qualitative data we collected. We curated the graphic below.

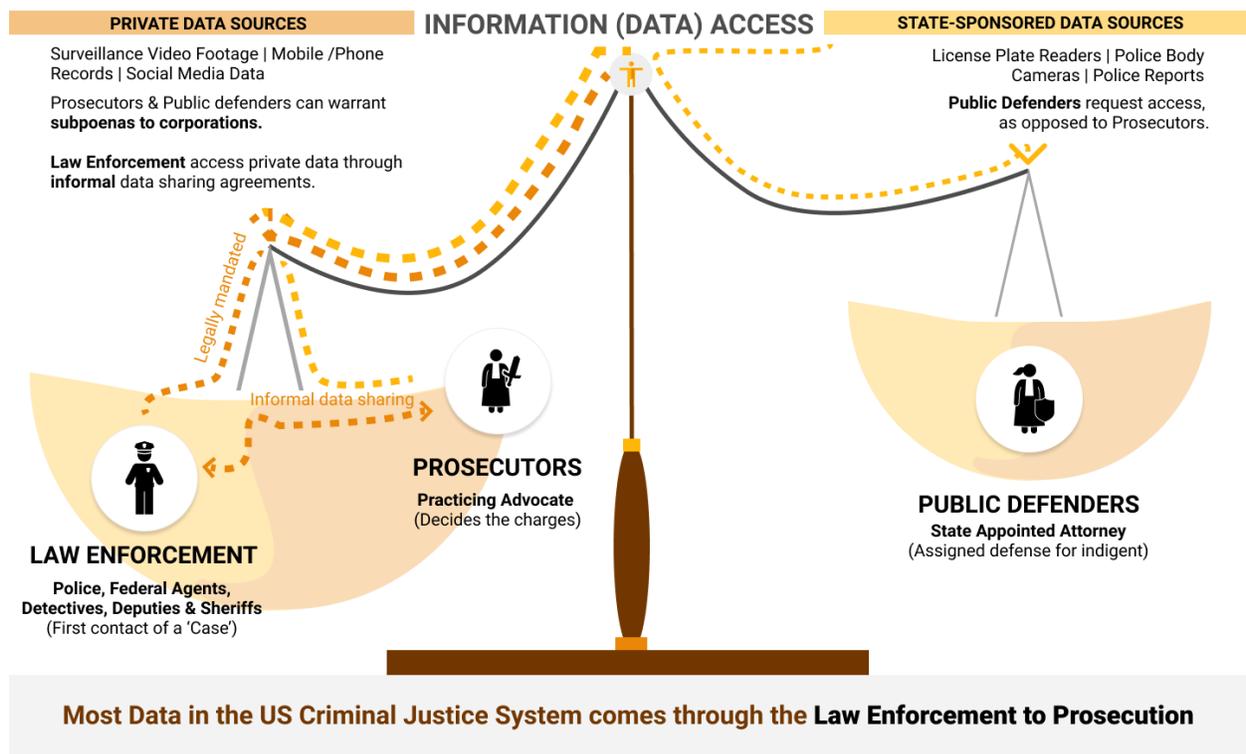


FIGURE 6. Final Iteration: Infographic depicting the Social Information Exchange in the US Criminal Justice System & Power Imbalance between the actors.

We used **iconography** and **illustrations** to depict the story of **power imbalance in the information flow**, depicting scales of justice to convey where different actors lie on this scale, providing context as short descriptions for their roles, how they



receive client information from private data sources (depicted in orange), and how heavily weighted the information flow is on the side of law enforcement and prosecutors (as opposed to public defender).

Website Design

In order to encourage civic participation by technologists and privacy advocates, we moved to create a website to share our learnings with these audiences.

Empathizing & Defining

We iterated through multiple phases of the design thinking process⁷, starting with empathizing. Empathy was the center of our approach to understanding public defenders, what they do and why, their technical and structural needs and constraints, and how they think about the criminal justice system.

In developing a framework for our insights, we arrived at major categories of (1) technical problems such as body camera surveillance, social media data analysis, online case management and (2) structural problems such as hiring experts, external relationships (with district attorneys, law enforcement, investigators), policy administration, training & resource sharing.

Ideation: Brainstorming

To transition our work to the drawing board, we began by conducting a rapid brainstorming session to sprout ideas that might help us build our website. Our

⁷ <https://web.stanford.edu/~mshanks/MichaelShanks/files/509554.pdf>

team product designer, Jyen, facilitated a brainstorming session where we were each given our own drawing boards and walked through what the flow of a technical solution for public defenders' data analysis might involve. After a phase of individual ideation, we then reconvened to discuss our flows. We diverged again to generate our How Might We's for a collective user flow and discover which parts of the process we could call attention to and present on the website.

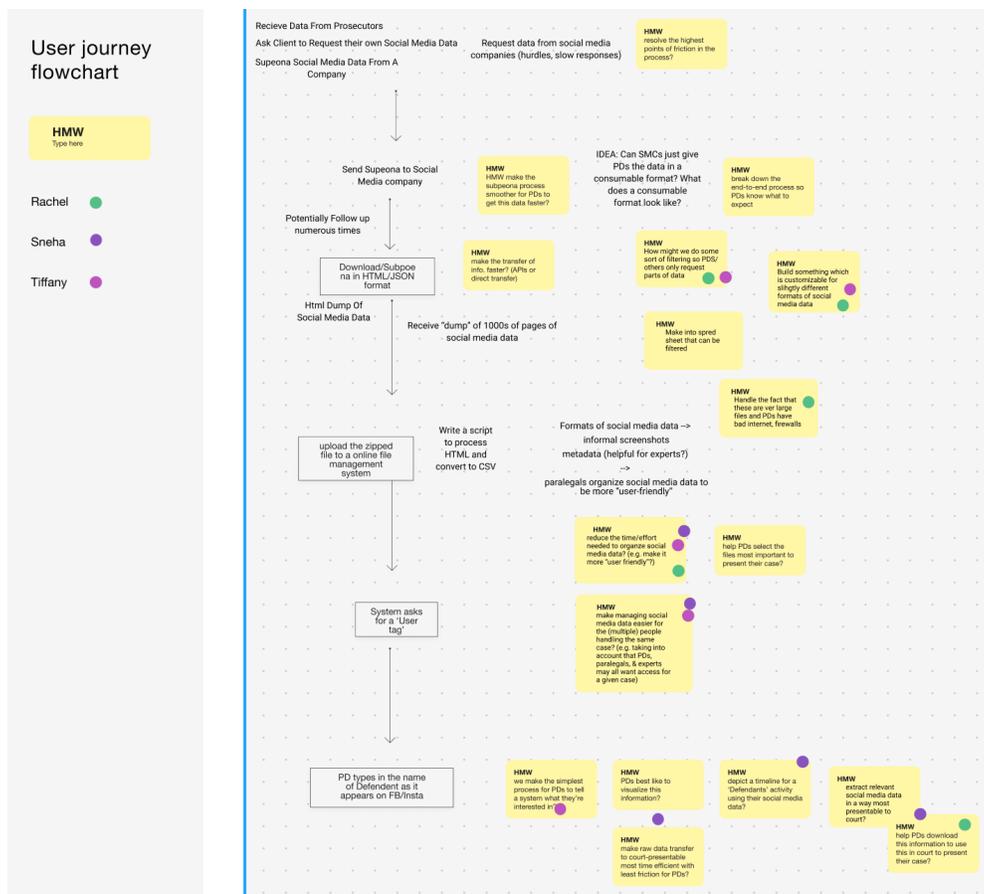


FIGURE 7. Ideation Workshop/Design Sprint artifact, to collectively diverge and converge in on ideas



Information Architecture & Design Decisions

Using a double diamond⁸ design model to discover and define the problems experienced by public defenders and how we might navigate a user on our website, as viewers we felt overwhelmed by the sheer volume of data collected. We realized, in order to avoid any unintended information overload⁹ For viewers, we would need to refine our problems areas.

At this point, we also considered the needs of our non-profit partner, who was specifically interested in presenting the work of public defenders in a more humanizing and relatable context. Thus, we honed in on selecting 3 critical problem areas from a pool of 16 discovered.

We laid out the initial website architecture with the aim to achieve goals to:

1. Educate people and initiate civic movement in technologists and policy advocates
2. Navigate viewers through the findings of The Public Defense Project, its key takeaways, potential solutions and technology constraints that bind public defenders
3. Share resources, policy advocacy concerns, and mechanisms to support the public defense community through their skills

With these goals, we laid out our initial website information architecture, as shown below. Each page had a purpose—whether it be to present the primary challenges

⁸ The Double Diamond model in UX: <https://www.nngroup.com/articles/discovery-phase/>

⁹ The History of information overload: <https://fs.blog/2014/09/the-history-of-cognitive-overload/>



Low fidelity wireframing & Iteration

Transitioning the sitemap to a website prototype, we asked what our prototype was prototyping¹⁰ (Houde & Hill, 1997) by focusing on the role we hoped this website would play in educating technologists and advocates and initiating civic engagement. We considered the content we were communicating and the experience we wanted users to have as they navigated through our website, as well as how the website would actually work in implementation.

We cover the majority of these changes in the presentation of the actual website. Converting the sitemap to low-fidelity wireframes kept our focus on the content, which was most important. We used Figma to collaboratively work on designing and iterating on both the copy and the wireframes. Wireframes were maintained in grayscale to seek functional feedback on the content—which was a prime motivator for promoting advocates to take action. For more information, refer to the Appendix section for all versions of the wireframe.

¹⁰ Houde, Hill. [What do Prototypes Prototype?](#)

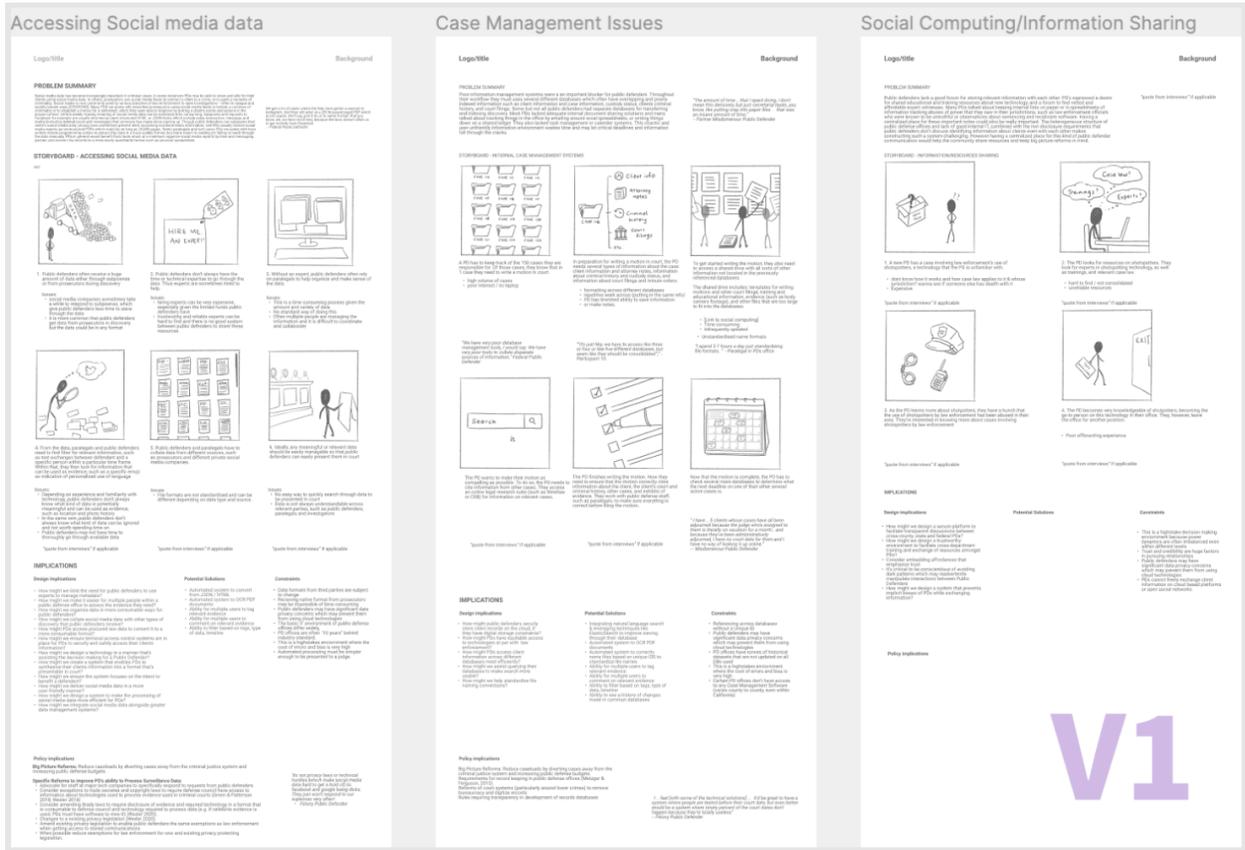


FIGURE 9. Initial Low-fidelity wire-framing of our problem areas in focus
 Based on the feedback we received from early viewers in the technology and advocacy community, the key design decisions we made included:

- (1) Eliminating information overload to avoid overburdening the user and allow them to focus on the story

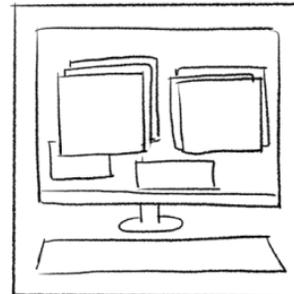
STORYBOARD - ACCESSING SOCIAL MEDIA DATA



1. Public defenders often receive a huge amount of data either through subpoenas or from prosecutors during discovery



2. Public defenders don't always have the time or technical expertise to go through the data. Thus experts are sometimes hired to help.



3. Without an expert, public defenders often rely on paralegals to help organize and make sense of the data.

Issues:

- social media companies sometimes take a while to respond to subpoenas, which give public defenders less time to sieve through the data
- it is more common that public defenders get data from prosecutors in discovery but the data could be in any format

Issues

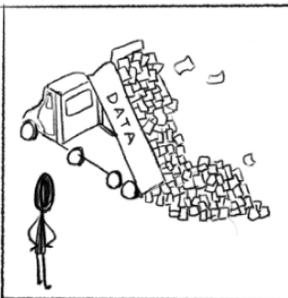
- hiring experts can be very expensive, especially given the limited funds public defenders have
- trustworthy and reliable experts can be hard to find and there is no good system between public defenders to share these resources

Issues

- This is a time consuming process given the amount and variety of data
- No standard way of doing this
- Often multiple people are managing the information and it is difficult to coordinate and collaborate

1. Eliminating Information Overload in limited real-estate, to focus on just the story within the storyboard.

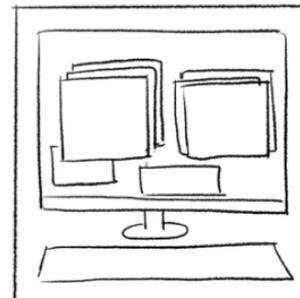
STORYBOARD - ACCESSING SOCIAL MEDIA DATA



1. Public defenders often receive a huge amount of data either through subpoenas or from prosecutors during discovery.



2. Public defenders don't always have the time or technical expertise to go through this. Thus, experts can be hired to help.



3. Without an expert, public defenders often rely on paralegals to help organize and make sense of the data.

FIGURE 10. Design decision to remove 'Issues' from the storyboard section and avoid a cognitive overload

(2) Promoting a 'needs-focused' approach over early solution-fixation helped us stay grounded and open-minded to divergent possibilities that may support public defenders. We also substantiated user quotes in-place to act as evidence for our needs, where appropriate.

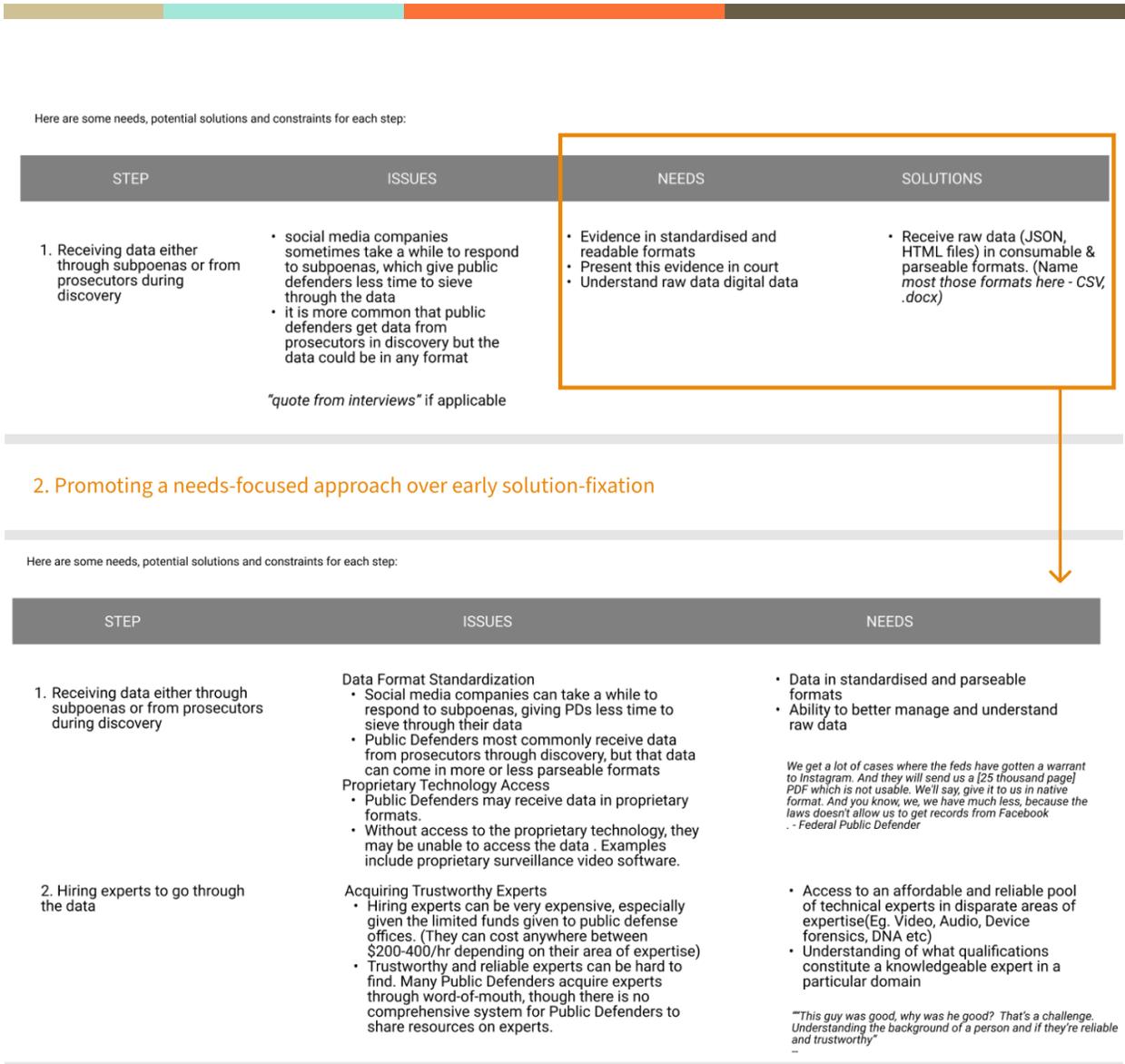


FIGURE 11. Design decision to remove 'Issues' from the storyboard section and avoid a cognitive overload

(3) Adopting an inclusive and universal approach, we generalized our implications by reframing them into design and policy constraints to engage wider audiences.

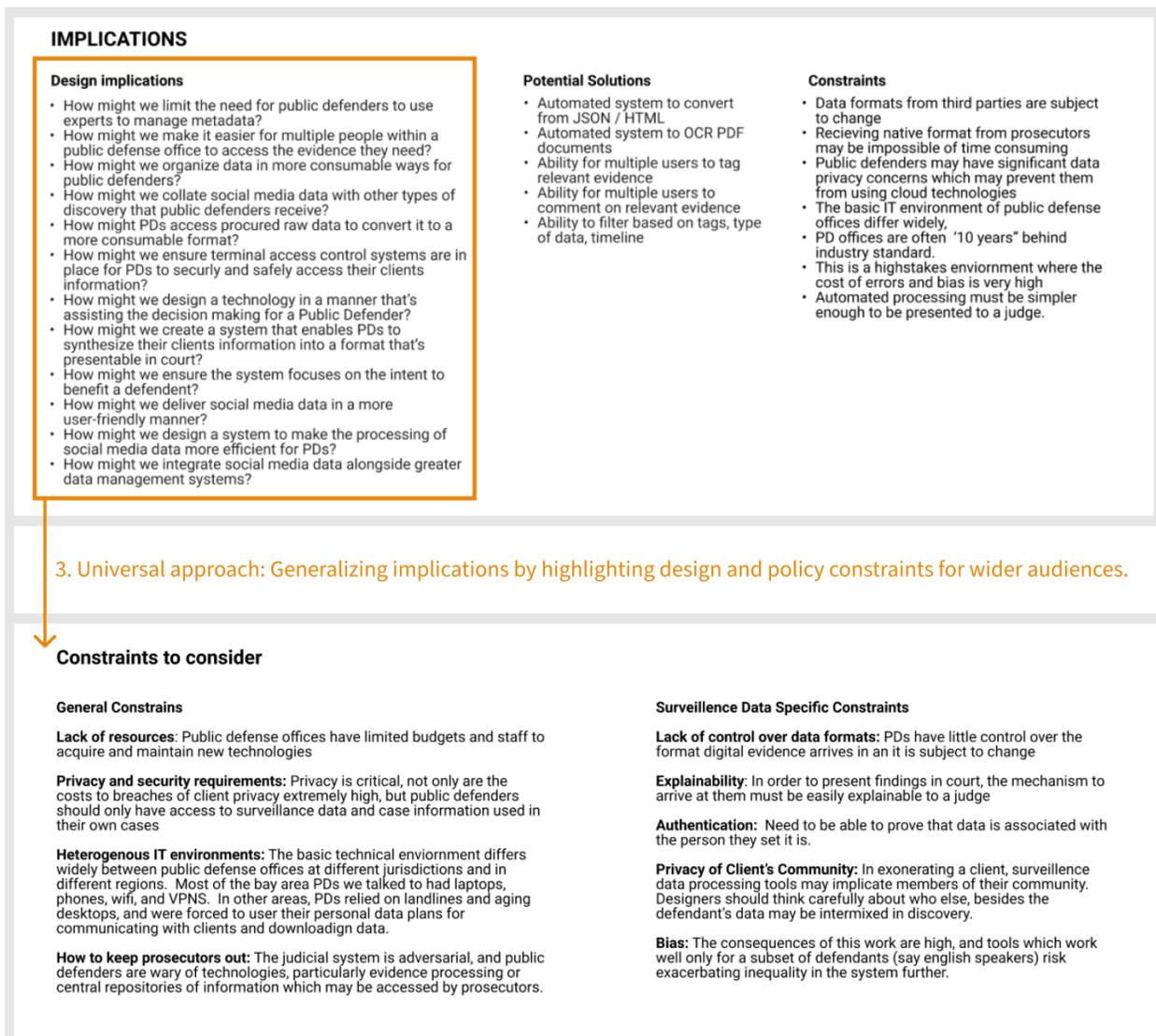


FIGURE 12. Design decision to generalize implications by highlighting design and policy constraints for wider audiences

Final Deliverable

In addition to the above considerations, our final website deliverable incorporated principles from Design Justice¹¹ specifically, centering a call to action based on the stories of those who were directly impacted by the outcomes of this

¹¹ <https://designjustice.org/read-the-principles>

design process, the Public Defenders. We prioritized the needs and the impact on the public defense community over our intentions in this process. We played the roles of facilitators, as designers and researchers, rather than experts in this field by listening to and integrating their lived experiences. Lastly, we shared knowledge and learning from our practice to strive for a community-led and controlled outcome, engaging technologists and policy advocates. Attached below are a few of the screenshots for references. Our website can be viewed here: <https://sites.ischool.berkeley.edu/publicdefense/> . Few screenshots depicting key design decisions to tell the story are depicted below. Refer to the Appendix G for more details on the website.

Three Important Areas of Need

We present user stories, highlighting opportunities for technical and policy work, touching on three major problem areas.

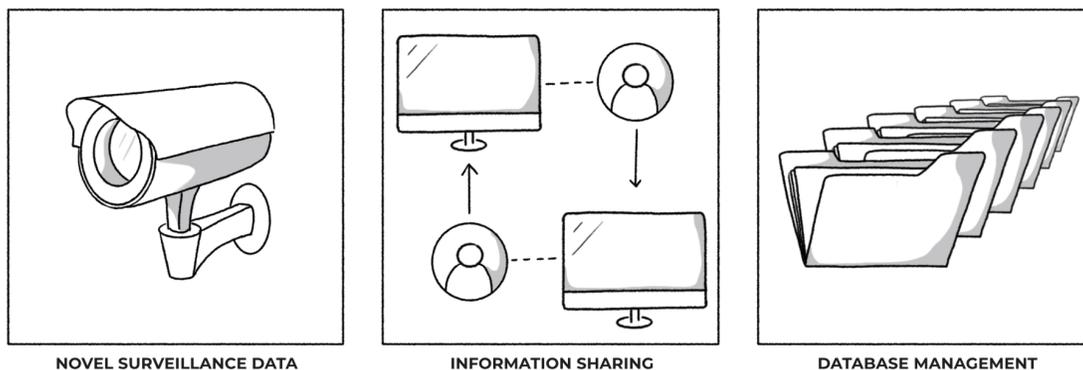


FIGURE 13. Landing page: Choice architecture between just 3 problem areas of need, that we honed in on

Who are public defenders?

Public defenders or 'indigent defense council' represent clients charged with crimes who cannot afford a private attorney. "Public Defender" usually refers to full time public employees who work exclusively to defend poor clients charged in criminal cases.



In the United States adversarial criminal legal system, defense counsel are the sole actors tasked with investigating evidence of innocence. Law enforcement has no constitutional, statutory, or formal ethical duty to seek out evidence of innocence. Therefore, selectively suppressing defense investigations means selectively suppressing evidence of innocence

- Rebecca Wexler, Assistant Professor of Law at UC Berkeley

- ▶ Who qualifies for a public defender?
- ▶ Are there other types of indigent defense?

FIGURE 14. Background page: Highlight relevant contextual information for any visitors new to this space

Working With Novel Surveillance Data

We outline public defender's needs around working with novel surveillance data, relevant design constraints for system designers and opportunities for policy advocacy.

- OVERVIEW
- STORYBOARD
- ISSUES AND NEEDS
- CONSTRAINTS
- POTENTIAL SOLUTIONS
- POLICY IMPLICATIONS

Surveillance data and discovery: Public Defenders are overwhelmed by the volume and complexity of data that characterizes modern criminal cases. They would benefit from technical tools to process and analyze that data for their clients. Though public defenders can subpoena for evidence from private companies and collect other kinds of evidence through independent investigations, they receive the majority of their data as "discovery"[1] from prosecutors—who acquire that data through partnerships with law enforcement, public surveillance systems, or directly from private companies. Thus, public defenders often have very little control over the format or (enormous) volume of data they receive. The two most important (and burdensome) forms of discovery were body camera footage and social media data, though public defenders have similar



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 accurate depiction?... Or were they trying to kind of

FIGURE 15. On click of a specific problem area of need, in this case the viewer is exploring "Working with Novel Surveillance Data"

Issues & Needs

See the issues and needs associated with each step of the process.

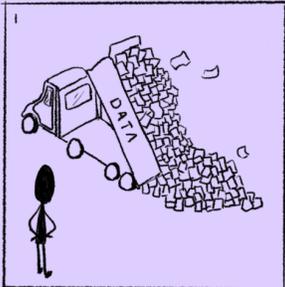
STEP	ISSUES	NEEDS
 <p>1. Public defenders often receive a huge amount of data either through subpoenas or from prosecutors during discovery.</p>	<p>Data Format Standardization</p> <ul style="list-style-type: none"> • Social media companies can take a while to respond to subpoenas, giving PDs less time to sieve through their data • Public Defenders most commonly receive data from prosecutors through discovery, but that data can come in more or less parseable formats <p>Proprietary Technology Access</p> <ul style="list-style-type: none"> • Public Defenders may receive data in proprietary formats. • Without access to the proprietary technology, they may be unable to access the data . Examples include proprietary surveillance video software 	<ul style="list-style-type: none"> • Data in standardised and parseable formats • Ability to better manage and understand raw data <p>“ <i>We get a lot of cases where the feds have gotten a warrant to Instagram. And they will send us a [25 thousand page] PDF which is not usable. We'll say, give it to us in native format. And you know, we, we have much less, because the laws doesn't allow us to get records from Facebook</i> – Federal Public Defender</p>

FIGURE 16. Surveillance Data Issues & Need Grid with a substantiating pain point to present the impact of the issue

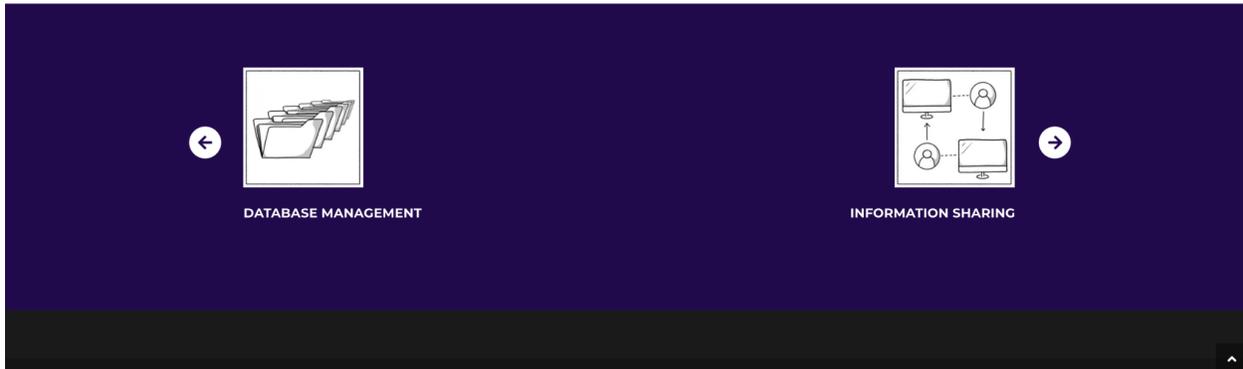


FIGURE 17. Navigating the viewers experience from one problem area to the next to discover all the cases from one to the next

Discussion & Impact

Design Implications

In developing these solutions, technologists should be mindful of the stakes involved in defense work and the complexity of the work environment. Public defenders are subject to resource and legal constraints in terms of procurement, presentation of evidence, and privacy.

Technical & Legal

Public defense offices are underfunded, but can also have little control over technology acquisition.



You're sort of stuck with the tools you have...you can't use just whatever open source thing you want to use"

explained a long time public defender. For example, technical tools in federal defense offices are procured at the national level. Furthermore, strict privacy requirements may prevent public defenders from storing technology in the cloud. Legal codes around presentation of evidence were a major constraint for automated analysis for many participants. A complicated, jurisdiction and technology specific set of regulations dictate how evidence may be presented in court. For example, editable transcripts are required in most places. In some areas,



public defenders don't have the technical resources to play video and have to come armed with exact timestamps. To be useful in court, tools and data must be explainable to a judge and facilitate the presentation of evidence in court.

Organizational & Personal

Perhaps the largest constraint for anyone hoping to scale tools in this system are the heterogenous IT environments of different public defense offices.

Furthermore, the technical literacy of public defenders differs widely. Many of the younger, less experienced public defenders we spoke with described needing to write scripts or provide technical support for older public defenders who had learned the trade in a radically different technology context. Said one tech savvy public defender:

“ *We have attorneys in our office, who've been there for 20 years, you know, and they are not as familiar or comfortable with the technology that they're used to taking their notes in hand, on the yellow pads.”*

Further complicating this uneven tech literacy is the adversarial nature of the criminal justice system. This warriness is documented in other qualitative research of public defense offices such as (Metzger and Furgeson, 2018) and was also



demonstrated in our interviews. One participant explained that periodically, information “boards” hosted by the NACDL were shut down when “cops showed up” even though they attempted to screen participants for public defense credentials. For all of these reasons, system designers are most likely to be successful developing solutions in close partnership with a few offices.

High Stakes and Bias

Several misdemeanor public defenders described how, even amongst 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 to rely on the public defender to subpoena them. However, this option may be difficult for mentally disabled, non English speaking, or homeless clients—and is impossible in instances where defendants use older, cheaper devices such as pre-paid phones. Technical solutions which only work for some clients risk exacerbating these inequalities. Another worry is that, in acquiring data about one person, data tools violate the privacy or security of another.

Policy Implications

An important finding from our research is the importance of non technical and policy solutions to aid public defenders. It is tempting to conclude from the woeful



and consequential state of technology in the public defense system that the best way forward is to improve the state of technology in public defense offices through more funding and tool building. However there is a risk that increasing funding and IT solutions for public defenders leads to an expensive technological arms race and an increasing need for automatic tools to process new data -- which have their own drawbacks.

A better solution would be to both limit the data law enforcement can access and significantly reduce the number of cases that move through the system and the consequences of lower crimes. That way, in cases that posed a significant loss of liberty, indigent clients could be sure that their counsel can fully examine every piece of evidence. At the end of one interview, the attorney I was talking to explained that a reduction in caseload 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 ninety 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 appeal in court, he shows how focusing on the technical may further entrench and normalize broken systems. We devoted time to



reviewing some of the criminology and legal literature for specific policy and advocacy solutions. In addition to big picture political action to reduce caseloads and divert clients outside of the criminal justice system we identify several more specific areas for policy work.

First, much of public defender difficulties with surveillance data come from a lack of transparency about what law enforcement has and how it works. We recommend advocating for local ordinances to provide transparency and regulation around local acquisition of surveillance data systems (Greene & Patterson, 2018, Joh 2017). Two important models are Oakland's PAC Surveillance Technology Ordinance which requires disclosure of new technologies and prohibits not disclosure agreements¹² and Seattle's municipal code which requires city council approval for acquisition of new technologies.¹³

However, our research reveals the importance of extending these disclosure rules to places that are semi-public but where indigent people are commonly surveilled such as jails, prisons, and public housing (Owens et al 2021). Public defenders should also be involved early as stakeholders in the acquisition process for new technologies (Wexler 2017). Another avenue to explore are rules prohibiting trade secrets from covering any data processing tool used in a criminal court (Joh 2017, Wexler 2017).

¹²<https://www.oaklandca.gov/resources/pac-surveillance-technology-ordinance-approved-by-city-council>

¹³ SEATTLE, WASH., MUN. CODE § 14.18.20 (2013)



Second there are particular specific areas where legal frameworks should be amended to provide public defenders equal access to surveillance data and tools of processing it. One is in social media -- where public defenders cannot request data from anyone other than their client (Wexler 2019). 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. Evidence rules should also be tightened, Brady laws generally do not cover data housed by third parties and also might be expanded to clarify that data handed in discovery has to be in a usable format and that tools used in a prosecution office to process discovery should be made available to public defenders. Lastly -- any solutions which reduce the number of times defendants have to appear in court and paperwork public defenders have to complete will help reduce load on the system overall.

Conclusion & Recommendations for Future Work

Our project surfaced numerous challenges for public defenders when involving data and technology in their work. In particular, public defenders are not equipped with the technology to meaningfully process and analyze much of the data they encounter in their cases, they lack comprehensive procedures and tools for case management, there are wide differences in the level of knowledge public defense offices have about various data and technologies, and they lack mechanisms to meaningfully communicate between public defense offices.



By outlining opportunities for technologists and advocates to engage in work to support public defenders, we hope to lay the groundwork for material efforts in the space. Our hope is that, through our project and site, technologists and advocates can identify starting points for enacting policy, developing technology, or—at a minimum—simply considering how the technologies they may currently be developing could potentially be wrangled with by public defenders (through the flow of use from consumers to law enforcement to public defenders).

Beyond technical efforts, we maintain that efforts to support public defenders through policy are just as, if not more, important. In 2019, the Ensuring Quality Access to Legal Defense Act was introduced as a bill in Congress.¹⁴ The EQUAL Defense Act would have provided resources to public defenders, provided funding to reduce caseloads, and offered them greater training and support. While it did not pass, we believe that similar policy efforts to improve the working conditions of public defenders is necessary in order to defend low-income and marginalized peoples impacted by the criminal justice system.

In the future, we envision a community task force to actively strengthen connections within the public defense community and its members—compensating community members for their knowledge, expertise, and time. Additionally, we hope that this network can facilitate members' capacity to create their own solutions, which are flexible and customizable to accommodate their diverse working and learning styles.

¹⁴ Jonathan Rapping. "Reforming Public Defense is Crucial to Criminal Justice," *Law360*. <https://www.law360.com/access-to-justice/articles/1307528/reforming-public-defense-is-crucial-for-criminal-justice>



We hope that potential solutions that arise on account of this work critically consider representation across all levels of their systems and consider how they might build trustworthy relationships. We urge technologists to be mindful and inclusive as they rethink system defaults. We hope technologists are cognizant of the power they hold to present information in a manner that is neutral and unbiased, to avoid manipulating the decision making process through the technologies they design for information exchanges in vulnerable networks.

MIMS Impact

Our project was deeply informed by MIMS coursework. As it concerned our approach to conducting research, of particular importance were the classes UX Research, Research Topics in HCI, and Qualitative Research Methods. In particular, the structure of the second half of our interviews was influenced by literature on open ended interviews from Qualitative Research Methods. Similarly, our techniques for coding and building analysis from the data was informed by both Research Topics in HCI and Qualitative Research Methods. Our analysis and understanding of our findings, and in particular our understanding of interrelated structural and technical concepts, was shaped by the classes Social Psychology in Information Technology, Applied Behavioral Economics, Information Law and Policy, Technology and Delegation, and Data, Power, and Infrastructure.

Finally, our approach to designing a website to communicate our findings to technologists and advocates was directly informed by the classes User Interface



Design and Development, Information Visualization, Product Design Studio and Interface Aesthetics . We are deeply appreciative of the I School faculty for their guidance and support.

Works Cited

1. Charmaz, K. (2006). *Constructing Grounded Theory: A Practical Guide through Qualitative Analysis*. SAGE.
2. Farole, D. J., & Langton, L. (2010). *County-based and Local Public Defender Offices, 2007*. Bureau of Justice Statistics (BJS).
3. Fienberg, S. E. (1990). Interactional Troubles in Face-to-Face Survey Interviews: Comment. *Journal of the American Statistical Association*, 85(409), 241.
<https://doi.org/10.2307/2289551><https://www.bjs.gov/index.cfm?ty=pbdetail&iid=2211>
4. Futch, A., & Soares, C. (April 2012). Enhanced 911 Technology and Privacy Concerns: How Has the Balance Changed Since September 11? *Duke Law & Technology Review*, 1(11), 10.
5. Harlow, C. W. (2000). *Defense Counsel in Criminal Cases* (NCJ 179023; Special Report). Bureau of Justice Statistics (BJS).
<https://www.bjs.gov/index.cfm?ty=pbdetail&iid=772>
6. Houde, S., & Hill, C. (1997). *Handbook of Human-Computer Interaction: What do prototypes prototype?*



<https://www.itu.dk/people/malmborg/Interaktionsdesign/Kompendie/Houde-Hill-1997.pdf>.

7. Joh, E. E. (2017). The Undue Influence of Surveillance Technology Companies on Policing. *New University Law Review*, 92.
<https://doi.org/10.2139/ssrn.2924620>
8. Langton, L., & Farole, D. J. (2010). *State Public Defender Programs, 2007* (NCJ 228229; Census of the Public Defender). Bureau of Justice Statistics (BJS).
<https://www.bjs.gov/index.cfm?ty=pbdetail&iid=2242>
9. Lofland, J., Lofland, L. H., & Lofland, P. L. H. (1995). *Analyzing Social Settings: A Guide to Qualitative Observation and Analysis*. Wadsworth.
https://books.google.com/books?id=IN_qAAAIAAJ
10. Marcus, R. (1994). Racism in Our Courts: The Underfunding of Public Defenders and Its Disproportionate Impact Upon Racial Minorities Student Notes. *Hastings Constitutional Law Quarterly*, 22(1), 219–268.
11. Metzger, P., & Ferguson, A. G. (2015). Defending Data. *SOUTHERN CALIFORNIA LAW REVIEW*, 88(1057), 69.
12. Molm, Linda D., and Karen S. Cook. "Social exchange and exchange networks." *Sociological perspectives on social psychology* 2 (1995): 209-235
13. Rapping, J. (2020) "Reforming Public Defense is Crucial to Criminal Justice," *Law360*.
<https://www.law360.com/access-to-justice/articles/1307528/reforming-public-defense-is-crucial-for-criminal-justice>

14. Wexler, R. (2017). Life, Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System. *Stanford Law Review*, 70.

<https://doi.org/10.2139/ssrn.2920883>

15. Wexler, R. (2019). *Privacy Asymmetries: Access to Data in Criminal Investigations* (SSRN Scholarly Paper ID 3428607). Social Science Research Network.

<https://doi.org/10.2139/ssrn.3428607>

Appendix

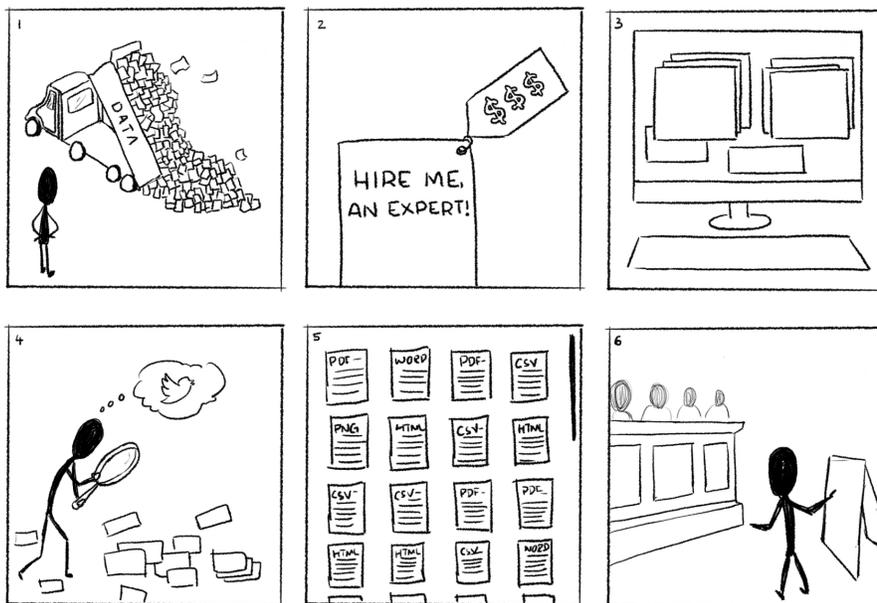
Appendix A: [Link to The Public Defense Project Website](#)

Appendix B: [Interview: Participant Consent Form](#)

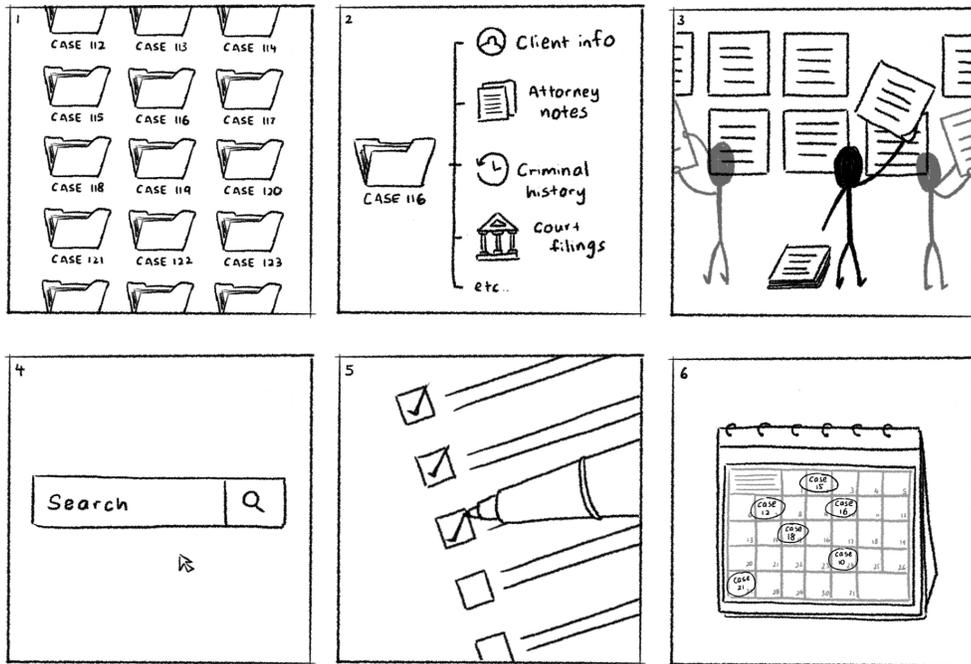
Appendix C: [Link to all Surveillance Technologies & Resources Encountered](#)

Appendix D: [Public Defender Interview Guide](#)

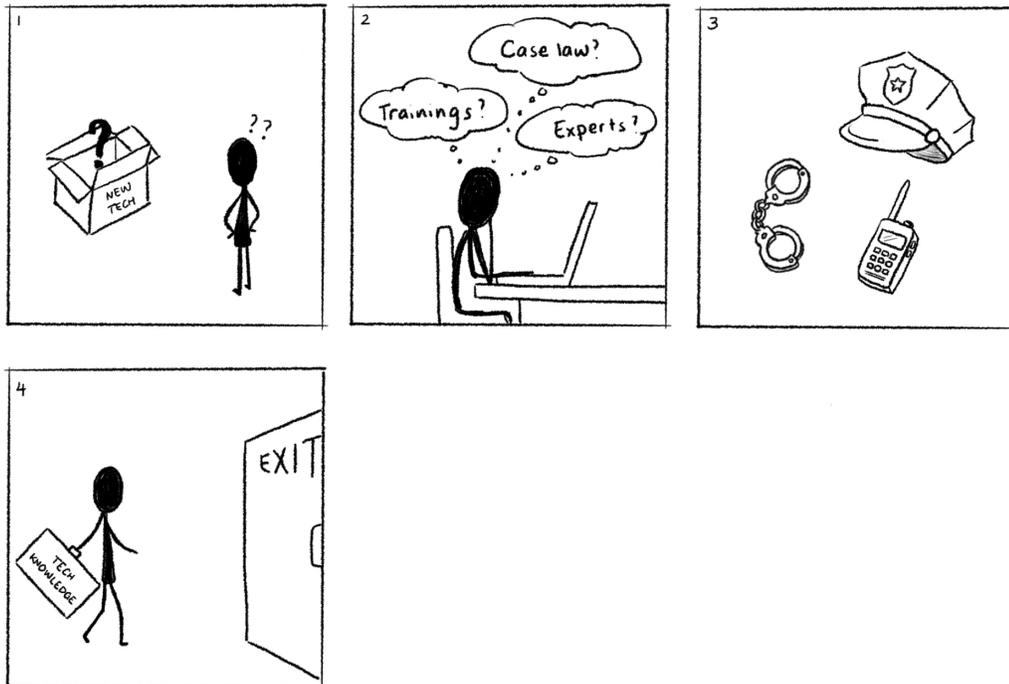
Appendix E: Storyboard Images



Storyboard depicting the data analysis struggle



Storyboard depicting issues with database management

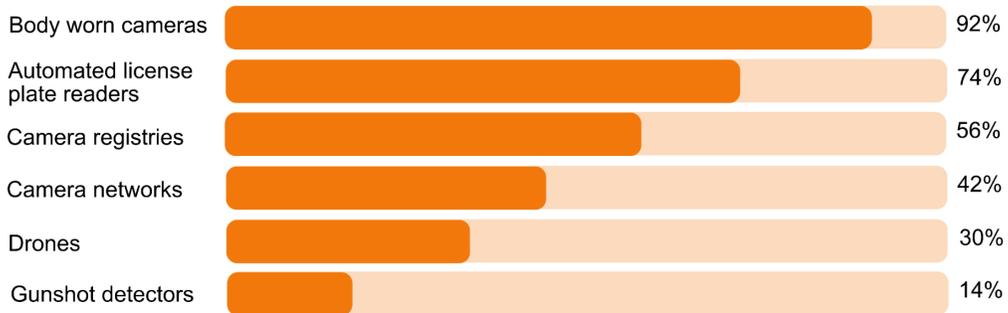


Storyboard depicting the discovery of experts and training material

Appendix F: Data Visualizations

Popular Technologies Used by Bay Area Law Enforcement

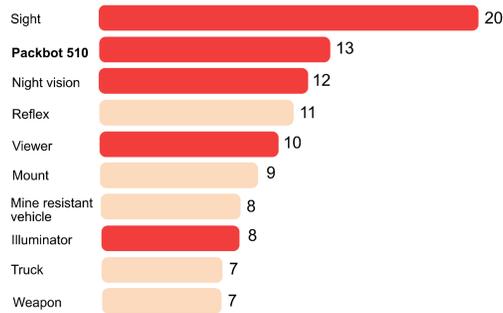
In an analysis of technologies used by agencies within 50 Bay Area cities, the percentage who use the following:



Source: Shelby Perkins and Craig Nelson, Stanford University's Freeman Spogli Institute

Many of the most common federally granted technologies concern surveillance

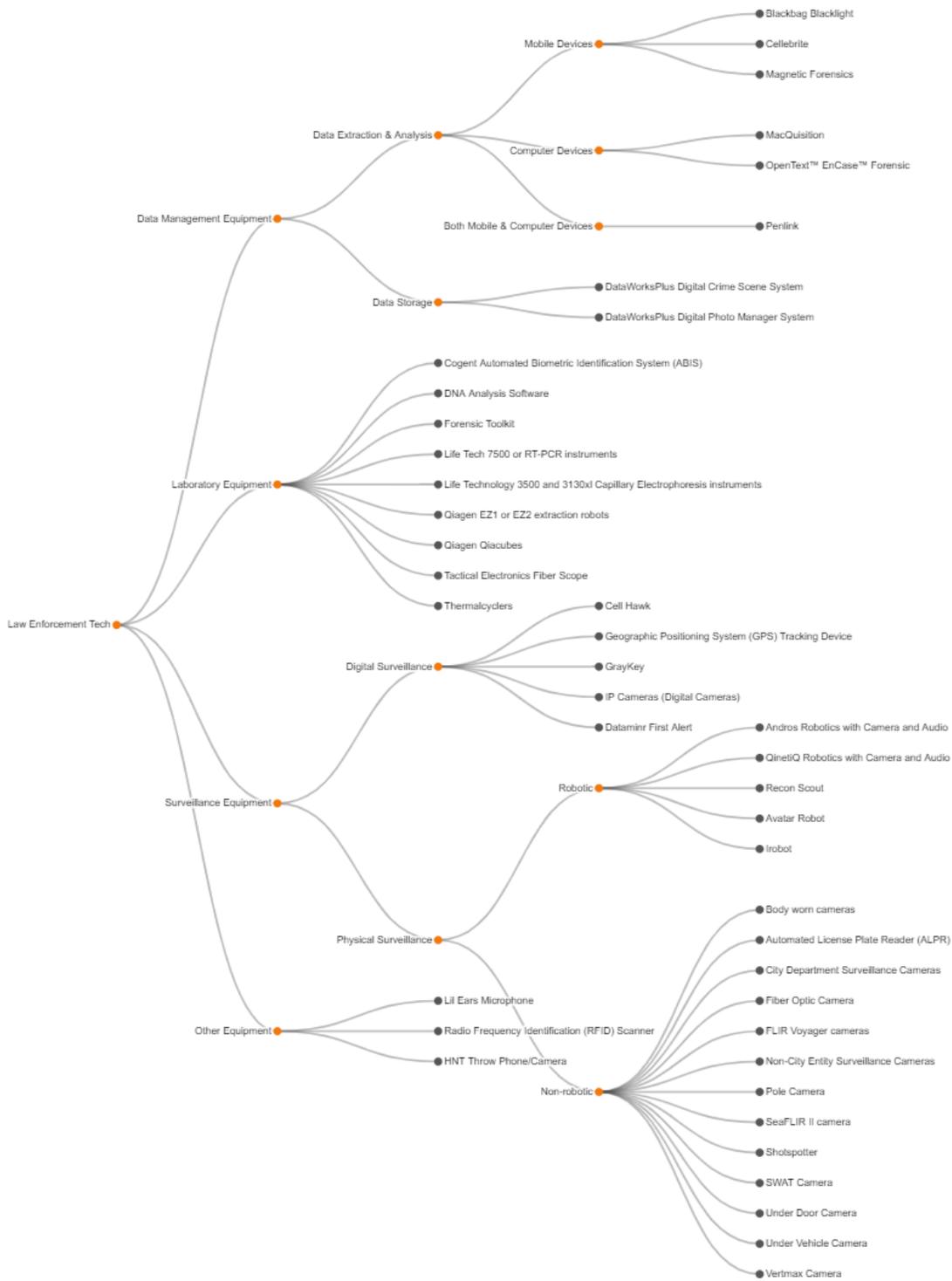
An analysis of the most frequently cited words in federal grants given to Bay Area law enforcement



Source: ABC7-I Team Analysis of Records from the Defense Logistics Agency

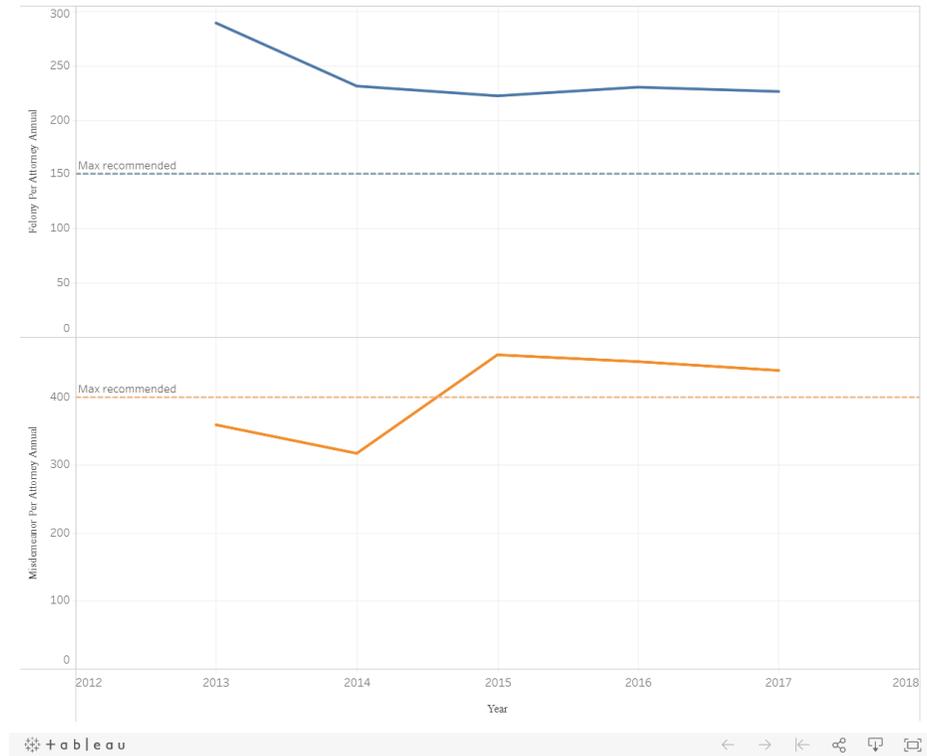
The **Packbot 510** is a tactical mobile robot that performs bomb disposal, surveillance, and reconnaissance.



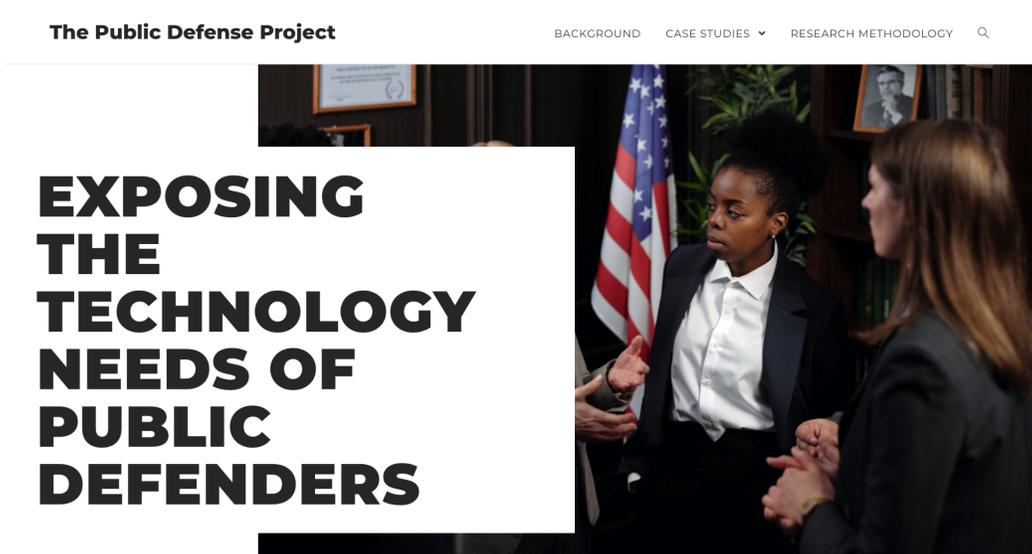


Public defender annual caseloads in Alameda County

The U.S. Department of Justice's National Advisory Commission (NAC) on Criminal Justice Standard and Goals has recommendations on maximum annual caseloads for a public defender office. Below is a chart comparing Alameda's public defenders to the recommended amount.



Appendix G: Final Deliverable - Website Screenshots



Information Sharing

Public defenders lack good mechanisms to share information and collaborate across offices. In this section, we outline opportunities and constraints for technologists interested in building social computing tools for public defenders.

- OVERVIEW
- STORYBOARD
- ISSUES AND NEEDS
- POTENTIAL SOLUTIONS
- CONSTRAINTS
- POLICY IMPLICATIONS

Public defenders frequently cite a lack of knowledge and a lack of ability to share knowledge with other public defenders. A better network for information sharing between public defenders would be useful in three areas: for sharing example case law and resources about new forms of technical and scientific evidence, a place to find and vet experts, and a place to organize around structural problems.

The heterogeneous structure of public defense offices and lack of good internal IT, combined with nondisclosure requirements that prevent public defenders from sharing identifying information about their clients, makes constructing such a system challenging. However, having a centralized platform to securely facilitate public defender communication would help the community share resources and keep big picture reforms in mind.



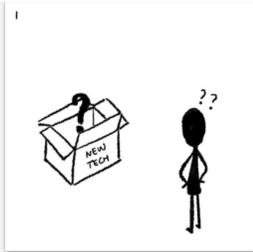
Oftentimes I'll ask the state court lawyers for the discovery that they got and they will have gotten [something] different, or there are records that they got that I didn't get. Communication definitely happens, but that's more on a person .. micro level, rather than ... like let's all band together and, you know, have presented a united front.

- Federal Public Defender

Storyboard

Explore this depiction of a public defender's experiences navigating, and attempting to access information about, unfamiliar technology.





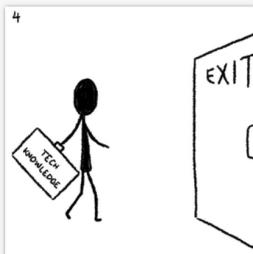
1. A new Public Defender has a case involving law enforcement's use of 'ShotSpotter', a forensic technological tool that the Public Defender is unfamiliar with.



2. The Public Defender looks for resources on ShotSpotter. They look for experts in ShotSpotter technology, as well as trainings, and relevant case law.



3. As the Public Defender learns more about ShotSpotter, they have a hunch that the use of ShotSpotter by law enforcement has been abused in their area. They're interested in knowing more about how Law Enforcement uses ShotSpotter in their cases.

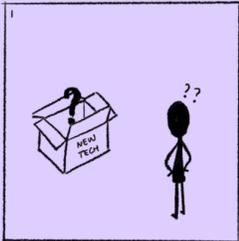


4. In due time this Public Defender becomes very knowledgeable in ShotSpotter as a tool & transcends into the go-to person for this technology in their



Issues & Needs

See the issues and needs associated with each step of the process.

STEP	ISSUES	NEEDS
 <p>1. New case with unfamiliar technology</p>	<p>Tech-Knowledge(y) Disparity</p> <ul style="list-style-type: none"> With prosecutors and law enforcement becoming increasingly equipped with emerging technologies and their operation, Public Defenders are often left playing catch-up 	<ul style="list-style-type: none"> Greater transparency around new technologies in use by prosecutors and law enforcement <p>“ [In a DUI Homicide we got these car black boxes and then] We're scrambling to figure out how the heck do we even read these? – Felony Public Defender</p>
	<p>Knowledge Building</p> <ul style="list-style-type: none"> It can be difficult for Public Defenders to access reliable information about an unfamiliar technology –such as how it works, the legality of its use, the case law that applies to it, and if any Public Defenders in their network have dealt with it 	<ul style="list-style-type: none"> Accessible, updatable, central location for reliable information about unfamiliar technologies–how they work and the legal contexts in which they've been used before <p>“ I don't really understand how torrenting works, you know, like, and I don't really feel qualified,</p>



Solutions

Below, we provide a few potential approaches to addressing public defenders' challenges working with information sharing. We encourage you to consider these approaches as well as your own.

- A platform for sharing information, such as example redacted briefs and case law, that is usable and secure for public defenders
- A platform for information sharing within jurisdictions for concerns and instances of abuse (by law enforcement and other parties and systems)
- A secure network to exchange knowledge on emerging technologies and the laws that govern them
- Collaborative workshops with technical experts in diverse fields of emerging technologies to foster engagement between public defenders and experts
- An authenticated repository to access shared, relevant training resources



We've been like collecting data ourselves. Each attorney will be told, 'Hey, we are seeing that clients with X and Y charges, who are black, are being denied bail really often. Could you keep a spreadsheet of like these cases?' And then individual attorneys will keep spreadsheets, and we'll send these spreadsheets into like one person to consolidate [it]. I just wonder if there is a more efficient way to do that

– Bay Area Public Defender

Constraints

GENERAL CONSTRAINTS

Lack of resources: Public defense offices have limited budgets and staff to acquire and maintain new technologies

Privacy and security requirements: Privacy is critical, not only are the costs to breaches of client privacy extremely high, but public defenders should only have access to surveillance data and case information used in their own cases

Heterogenous IT environments: The basic technical environment differs widely between public defense offices at different jurisdictions and in different regions. Most of the bay area PDs we talked to had laptops, phones, wifi, and VPNs. In other areas, PDs relied on landlines and aging desktops, and were forced to user their personal data plans for communicating with clients and downloading data.

How to keep prosecutors out: The judicial system is adversarial, and public defenders are wary of technologies, particularly evidence processing or central repositories of information which may be accessed by prosecutors

SOCIAL COMPUTING SPECIFIC CONSTRAINTS

Confidentiality and conflict of interests: It is illegal for defense council to share information about a case or client with anyone not working on the case

Maintaining accuracy: Outdated or in accurate technical information may be worse than no information — and designers must think carefully about how to maintain quality in user sourced content

Avoiding manipulation through dark-pattern designs: Any information exchanged between defenders should be presented in fair and neutral ways to avoid traditional dark-patterns (Eg. misdirection, trick questioning, confirmshaming or 'roach motel' user experience flows) that may often manipulate decision making behaviors when interacting on digital networks.

Policy Implications

Big Picture Reforms

- Reduce caseloads by diverting cases away from the criminal justice system and increasing public defense budgets.

Reforms to Improve Transparency in Surveillance Data Acquisition

- Advocate for ordinances to provide transparency and regulation around local acquisition of surveillance data systems.[1][2][3]. Two important models are Oakland's PAC Surveillance Technology Ordinance which requires disclosure of new technologies and prohibits not disclosure agreements and Seattle's ordinance which requires city council approval for acquisition of new technologies.
- Extend such ordinances to include disclosure rules for surveillance in jails prisons, and public housing [4, 5]
- Include explicit requirements for Public Defender engagement in the acquisition of surveillance data systems [6]
- Consider exceptions to trade secrets and copyright laws to require defense council have access to information about technologies used to process evidence used in criminal courts [3][5]

Specific Reforms to improve PDs Ability to Share Information

- Requirements for record keeping in public defense offices [7]



The DNA testing is done by the .. medical examiner's office, you know, which is supposedly an unbiased entity ... the information I'm not going to get access to that I would want is the actual software that they use to analyze [the] DNA... that's stuff that is trade secrets that the company will allow us to look at

– Bay Area Public Defender

Who are public defenders?

Public defenders or 'indigent defense council' represent clients charged with crimes who cannot afford a private attorney. "Public Defender" usually refers to full time public employees who work exclusively to defend poor clients charged in criminal cases.



In the United States adversarial criminal legal system, defense counsel are the sole actors tasked with investigating evidence of innocence. Law enforcement has no constitutional, statutory, or formal ethical duty to seek out evidence of innocence. Therefore, selectively suppressing defense investigations means selectively suppressing evidence of innocence

– Rebecca Wexler, Assistant Professor of Law at UC Berkeley

- ▶ Who qualifies for a public defender?
- ▶ Are there other types of indigent defense?
- ▶ What types of crimes do public defenders work on?
- ▶ What regions (jurisdictions) do public defenders operate in?
- ▶ How many cases do public defenders work on a year?
- ▶ What does 300 misdemeanor cases a year look like?
- ▶ What does 150 felony cases a year look like?

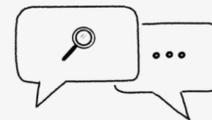
Research Methods

SEMI-STRUCTURED INTERVIEWS

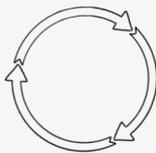
In total, we conducted semi-structured interviews with 22 participants. The breakdown was as follows: 15 former or current public defenders, 2 paralegals, 2 investigators, 1 legal scholar, 1 privacy advocate and technologist, and 1 policy specialist at a major tech company. The public defenders were a mix of federal and state public defenders. Of the current and former public defenders we interviewed, 9 were located in the Bay Area.

In the interviews we focused on public defenders technology needs both in their day-to-day workflow and in working with novel surveillance data. We focused on specific experiences and stories about technology, but also made space for participants to share their more general experience working in the public defense system.

We transcribed the interviews and applied qualitative methods to code our findings and identify emerging themes.



DESIGN & NEEDS ASSESSMENT



We iterated through multiple phases of the design thinking process, starting with empathizing. Empathy was the center of our approach to understanding public defenders, what they do and why, their technical and structural needs and constraints, and how they think about the criminal justice system.

Through our interviews and associated qualitative analysis, and in developing a framework for our insights, we arrived at major categories of:

1. technical problems such as body camera surveillance, social media data analysis, and online case management
2. structural problems such as hiring experts, external relationships (with district attorneys, law enforcement, and investigators), and training and resource sharing

At this point, we also considered the needs of our non-profit partner, who was specifically interested in presenting the work of public defenders in a more humanizing and relatable context.