THE DIGITAL TURN IN PUBLIC CRIMINAL DEFENSE

By

FANNY ANNE RAMIREZ

A dissertation submitted to the

School of Graduate Studies

Rutgers, The State University of New Jersey

In partial fulfillment of the requirements

For the degree of

Doctor of Philosophy

Graduate Program in Communication, Information and Media

Written under the direction of

Jeffrey Lane

And approved by

____

____

____

____

New Brunswick, New Jersey

October, 2019

ABSTRACT OF THE DISSERTATION

The digital turn in public criminal defense

By FANNY ANNE RAMIREZ

Dissertation Director:

Dr. Jeffrey Lane

This dissertation studies the digital turn in public criminal defense. It focuses on public defenders, who are court-appointed attorneys, and their indigent clients, who come primarily from minority populations. I argue that the defining feature of the digital turn is that it brings judicial actors into contact with increasingly personal parts of defendants' lives. As part of handling cases, both the prosecution and the defense interact with photos, conversation records, and location information, and use these pieces of digital evidence to understand the people, events, and circumstances around alleged crimes. I situate my study at the intersection of communication scholarship, socio-legal studies, and critical race theory. I draw on the latter's legal storytelling framework to help make sense of how public defenders and prosecutors use digital evidence to create competing narratives about poor defendants and their alleged crimes.

To examine the digital turn in public criminal defense, I conducted an ethnographic study of a public defender office and its in-house, digital forensics laboratory. The goal was to understand how digital evidence is shaping criminal case processing, especially defense work, and the relationship between public defenders and their indigent clients. I developed an original framework called the "life cycle." This framework makes an important contribution to socio-legal studies and scholarship in the area of communication and technology by presenting a process-oriented approach that allows scholars and legal practitioners to understand how different moments in the life of a case unfold in the digital turn. Using the life cycle approach, I trace the life of digital evidence in public criminal defense, from the evidence's arrival in the public defender office to its eventual application during hearings, plea negotiations, and trials. Throughout the analysis, I highlight the challenges and opportunities public defenders experience in the digital turn.

ACKNOWLEDGEMENTS

First, I would like to thank the defense attorneys, digital forensic analysts, and investigators at the Northeastern Defender Association for welcoming me into their office and giving me the opportunity to learn about the digital turn in the criminal justice system by observing their day-to-day work. Their continued enthusiasm for my research project and kindness towards me as an emerging scholar have been a great motivating force throughout the writing of this manuscript.

I would also like to thank my dissertation committee, Jeffrey Lane, Jennifer Gibbs, Todd Wolfson, and Jorge Schement for their support over the years.

My advisor, Jeff, brought me onto a project about the use of social media evidence in gang prosecution my very first semester in the PhD program at Rutgers. I was so fascinated by this area of research that I decided to align my own work to explore more deeply how new technologies were shaping criminal justice. I am grateful to Jeff for sharing his passion for ethnography and storytelling, and for introducing me to key members of what became my dissertation field site. Through his guidance, I have become a more observant scholar and a better writer. My outside committee member, Jenn, has been pushing me to think critically about technology since my early days in the MCIS program, and my dissertation has been strengthened by her keen insights. I had the pleasure of taking two classes with Todd, one on cyberethnography and one on new media and global cities, and he's been a supporter of my research throughout my time at Rutgers. I met Jorge at an event about video games at Alexander library. He encouraged me when I organized the third installment of the Extending Play conference, and he generously agreed to serve on my committee even when my focus shifted from game studies to socio-legal scholarship.

I am thankful for my friends in the PhD program in the School of Communication and Information at Rutgers with whom I've shared this journey: Alexa Bolaños, Stephanie Mikitish, Darcey Searles, Joy, Cox, Wan Wei, Henry Boachi, Jack Harris, Teis Kristensen, Inyoung Shin, Amana Kaskazi, Sarah-Rose Marcus, Heewon Kim, Maggie Boyraz, John Leustek, Aaron Trammell, Wei Shi, Ian Dunham, Frank Bridges, Andrew Salvati, and James Hodges, among many others. I am glad we were all in this together!

Many family members and friends outside of academia helped me throughout the PhD program, and especially during the dissertation writing process. My friend Yubiditza Willard sent me encouragement all the way from Texas via funny snaps and text messages, and my sister Audrey was always only a phone call away. My parents, Michèle Schmitz and Paco Ramirez were an invaluable source of support, and so were my parents-in-law, Liz and Tony Earwood. My grandmother, Moune, regularly called me on Skype to make sure I was taking care of myself. Finally, my deepest gratitude to my husband, Nick Earwood, and my son, William Earwood, for their love and reassurance. I couldn't have made it this far without family trips to the farm, playground adventures, and pizza nights to balance out the long writing days.

DEDICATION

This dissertation is dedicated to my parents. Thank you for supporting my education and for all the sacrifices you have made along the way.

Table of Contents

Chapter 1: Problem Statement

The Digital Turn

In 2017, Michelle Carter was found guilty of the involuntary manslaughter of her boyfriend, Conrad Roy. The smoking gun was a series of text messages sent to the deceased in the weeks and months preceding his death. Dubbed the "texting suicide" by the popular press, Carter's conviction relied primarily on text messages in which she encouraged her boyfriend to commit suicide by carbon monoxide poisoning (Bever & Phillips, 2017; LeBlanc, 2017). Although the interactions between Carter and Roy were mediated by technology, they were seen as akin to urging another person to commit suicide by whispering in his/her ear (Bever & Phillips, 2017). The court found that the text messages demonstrated that Carter "had placed [Roy] in a situation that led to his suicide" and were therefore responsible for his death (Bever & Phillips, 2017). The reliance on evidence from technology-mediated communication as outlined in Carter's case is not an isolated incident. Across the country, evidence in criminal cases comes increasingly from smartphones and social media in what has been termed a "digital turn" in the U.S. criminal justice system (Carlson, 2015; Lane, 2018; Lane, Ramirez, & Pearce, 2018; Sholl, 2013). In New York City, the Manhattan district attorney's office estimates that more than 25% of its annual cases include digital evidence (Farrell, 2018). For criminal cases, that number is much higher. According to the digital forensics company, Cellebrite, between 80% and 90% of all criminal cases include some form of digital evidence (Watson, 2018).

Digital evidence is an umbrella term for any type of data stored or transmitted in digital form and may refer to text messages, social media content, browsing histories, backups of various programs, and calendars, among other things (Casey, 2011; National Institute of Justice, 2016; Pendleton, 2013). This criminal justice development is tied to communication practices concerning new technologies, and, in particular, the growing popularity of smartphones (Quick & Choo, 2017; Sammons, 2014). As of 2017, 95% of American adults owned some type of cell phone, and 77% owned a smartphone (Rainie & Perrin, 2017). Smartphones enable cheap and efficient communication across a range of channels. This versatility has led scholars to describe them as social mediators - technologies that drive interaction and shape how people relate to each other and to their surroundings (Baym, 2015; Ling, 2012; Verbeek, 2015).

In the past two decades, digital technologies have become embedded in people's day-to-day interactions at the social, personal, and professional level (Hampton, 2016; Wang & Stefanone, 2013; Wright & Webb, 2011). Smartphones are now used to stay in touch with friends, family members, and colleagues. But social interaction is not their only utility; smartphones also play a key role in helping people access health services, apply for jobs, engage in civic participation, and even request government services (Hofmann, Selbst, & Data & Society Research Institute, 2017). Given the prevalence of smartphones in daily life, it is not surprising that law enforcement is turning to technology-mediated communication to answer questions about the "who, how, what, why, when, and where" of an investigation (Quick & Choo, 2017). And mobile forensics, which focuses on the recovery of data from phones and other portable devices, is one of the fastest growing branches of digital forensics (Chernyshev, Zeadally, Baig, & Woodward, 2017).

Although smartphone ownership is high across all populations in the United States, non-white and lower-income Americans are more likely to have Internet access only through their smartphones, thus making them more reliant on the devices to fulfill basic social and professional needs (Pew Research Center, 2018; Tsetsi & Rains, 2017). This dependency also puts poor, non-white individuals in a more precarious position in the context of the digital turn, because their phones, as primary sources of communication, reveal a lot of personal information.

Study Intervention

Law enforcement and prosecutors have generally met the digital turn with praise. For them, evidence from smartphones, social media, and other new media technologies has become highly valuable for gathering information for investigations, solving crimes, and securing convictions (Trottier, 2012). Large amounts of case-relevant data, from geographical location to personal statements made by suspects, can be gleaned from a person's social media account (Parker & Swearingen, 2012). In fact, the pool of information available is often so vast and so varied that prosecutors refer to technology-mediated interactions as a "goldmine of witness blunders" (Dean, 2013, p. 49). In drug-related criminal cases for example, text messages from interested buyers inquiring about the price and availability of products have been used by prosecutors to demonstrate the existence of a dealer/customer relationship (Hirst, 2011). And status updates, photos, and private messages from social media have been used to establish associations between gang members and criminal activity as part of police efforts to combat street violence (Lane et al., 2018; Patton et al., 2017; Patton, Leonard, Cahill, et al., 2016; Patton, Leonard, Lane, Macbeth, & Smith Lee, 2016).

The proponents of the digital turn see the growth of technology-mediated communication as a new and innovative way to acquire case-related information and improve police efficiency (Trottier, 2012). However, scholars and civil rights organizations have raised concerns about the intrusiveness and potential, racial biases behind such methods (Baym, 2015; Cagle, 2016; Wressler, 2018). Many of these concerns stem from the manner in which digital evidence is acquired. The search warrants issued for digital content tend to be overbroad (Denney, 2018), which means that they often grant permission to "search and download any and all electronic data" or access "all electronic equipment, computers, and cell phones" (Gershowitz, 2016, pp. 18-19). When requests are formulated so broadly, it is inevitable that personal information unrelated to investigations becomes available to criminal justice personnel. Critics of the digital turn worry about the risks of exposure and privacy disruptions from overbroad search warrants. There are also concerns that these practices will encourage phishing expeditions and lead to additional police scrutiny of racial minorities who are already experiencing high levels of surveillance (Bloss, 2007; Joh, 2016; Mateescu et al., 2015). Indeed, current research shows that the record management systems and geographic information systems used by police to aggregate, store, and analyze data are rife with bias and overwhelmingly contain information about low-income and racial minority populations (Joh, 2018; Sanders & Hannem, 2012). As the breadth of digital evidence expands, this trend is likely to continue and exacerbate racial discrimination in the criminal justice system. In fact, research shows that in large urban areas, such as New York City and Chicago, low-income youth of color are already the targets of systematic, online monitoring in addition to street-level surveillance (Lane, 2018; Patton, Leonard, Cahill, et al., 2016). The intrusiveness of overbroad search warrants and the reports that marginalized populations are experiencing higher levels of police surveillance of their technology-mediated interactions call for a closer examination of how digital evidence is acquired and used against such groups in the digital turn. Furthermore, since research on digital evidence has predominantly focused on the appeals of such evidence for law enforcement and prosecutors, there is a need to understand how this evidence is perceived and used by defense attorneys who are on the other side of the adversarial criminal justice system.

Study Focus and Significance

This dissertation is a study of the digital turn in public criminal defense. It focuses on public defenders, who are court-appointed attorneys, and their indigent clients who come primarily from minority populations. In the digital turn, public defenders are facing cases backed by digital evidence. To defend their clients, defense attorneys work on two fronts: they challenge the incriminating digital evidence introduced by the prosecution and they collect digital evidence that may be helpful to their case. Their work as public defenders is shaped by the social and economic circumstances of the indigent clients they represent. These clients are mostly poor, black people. They are a population overrepresented in the court system that has experienced sustained discrimination at the hands of the American criminal justice system (Alexander, 2012). Because of this longstanding history of injustices, this population is often skeptical about the law and distrustful of judicial actors on both sides of the system.

In the context of the digital turn, prosecutors and defenders are increasingly using the digital footprints of poor, non-white defendants as part of handling cases. In the process, they come into contact with digital evidence, such as photos, conversation records, and location information, and learn to understand the people, events, and circumstances in question on the basis of these personal pieces of digital evidence. The growth of digital evidence as a tool of the criminal justice system raises questions about how attorneys on both sides gain access to the lives of indigent defendants and make sense of their digital footprints as evidence in cases.

In this dissertation, I examine the digital turn in the criminal justice system through an ethnographic study of a public defender office and its in-house, digital forensics laboratory. The goal was to understand how digital evidence is shaping criminal case processing, especially defense work and the relationship between public defenders and their indigent clients. I purposely chose to focus on public defenders and their clients to gain a deeper insight into how the digital turn is reproducing and intensifying mechanisms of inequality and discrimination in the criminal justice system. Through the development of what I call the "life cycle" of digital evidence, I present a process that allows scholars and legal practitioners to understand how different moments in the life of a case unfold in the digital turn. Using the life cycle approach, I trace the life of digital evidence in public criminal defense, from the evidence's arrival in the public defender office to its eventual application during hearings, plea negotiations, and trials. Throughout the analysis, I highlight the challenges and opportunities public defenders experience in the digital turn. I situate my study at the intersection of communication scholarship, socio-legal studies, and critical race theory. I draw on the latter's legal storytelling framework to help make sense of how public defenders and prosecutors use digital evidence to create competing narratives about poor defendants and their alleged crimes in the digital turn (Delgado & Stefancic, 2012; Fajans & Falk, 2009). I argue that each stage in the life cycle corresponds to different moments in legal storytelling. The acquisition stage is about gathering the pieces of the story, the analysis phase is about organizing those pieces into a persuasive narrative, and the application stage is where both sides present their competing narratives and the case reaches a conclusion.

Field Contribution: The Life Cycle Approach.

To understand the implications of the digital turn for public criminal defenders and their clients, I conducted an ethnographic study of a public defender office and its in-house, digital forensics laboratory. During my fieldwork I noticed turning points in digital evidence use. Digital evidence seemed to have different impacts on different actors (attorneys, digital forensic analysts, investigators) at different moments in the case. Based on these observations, I developed the “life cycle” approach, to separate those turning points and present them in a way that limited legal jargon and would be intuitive to a wide readership. I realized that digital evidence had a “life” in a case. It entered the system, was analyzed, and then found its end when applied towards the closing of the case. Thinking of this process as a “life cycle” was a simple way to trace the implications of digital evidence from start to finish in the defense context. The creation of this approach is a major contribution to the field of socio-legal studies. Through the “life cycle” approach, I present a process that allows scholars and legal practitioners to understand how different moments in the life of a case unfold in the digital turn.

The framework breaks down into the following phases the key moments at which digital evidence appears in criminal defense: acquisition, analysis, and application. This approach follows digital evidence, from the initial acquisition of the evidence to its application during hearings, plea negotiations, and trials. It is a broad, holistic framework that makes sense of complex legal developments in approachable terms. Each phase of the life cycle presents its own challenges and opportunities. In the next paragraphs, I describe the three phases and explain their relevance to the study of how public defenders and their clients navigate the digital turn.

The acquisition phase. The acquisition phase is the first stage in the life cycle. During this phase, public defenders work closely with digital forensic analysts and investigators to acquire digital evidence that could be beneficial to a defendant’s case. In other words, this is where the storytelling building blocks are gathered. In this phase, digital forensic analysts recover information from smartphones and social media accounts (Sammons, 2014). In the context of the digital turn, I anticipate that some defendants, out of fear, discomfort, or uncertainty may be reluctant to turn over their smartphones or other electronic devices for forensic examination. Some defendants may also face social and institutional barriers, such as parole restrictions, odd working hours, or lack of family support, which complicate the task of dropping off devices with the public defender office. I also stipulate that how people use technology may affect what evidence can be recovered in the acquisition phase, e.g., deleting texts may make the extraction of messages more difficult or even impossible, whereas meticulously saving pictures may simplify the preservation work.

The analysis phase. This is the second phase of the life cycle. During this stage, public defenders make sense of the digital evidence in the case. They examine extensive records from smartphones, social media accounts, computers, video surveillance systems, and other sources (Nelson & Simek, 2014; Sholl, 2013), and assess how this evidence might factor into the case. This is about sorting and organizing the pieces of the narrative. During this phase defenders also meet with clients to discuss the case and what kind of defense to present. Digital evidence from social media and smartphones may cover months or even years of data (Nelson & Simek, 2014; Sholl, 2013). Analyzing such documents represents a considerable time investment. Consequently, I anticipate that defense attorneys have had to readjust their work practices and may have adopted new strategies for managing large amounts of data. Lastly, I expect that the digital turn may bring new professional dynamics for public defenders and their clients. For example, it is possible that in some cases, access to personal communications leads to closer, more human relationships between attorneys and clients, whereas in other instances, that same level of access may be perceived as a privacy violation and hurt attorney-client interactions.

The application phase. This phase describes the points at which digital evidence is used to further the legal development of a case during hearings, plea bargains, and at trials. It involves the use of digital evidence against the defendant by the prosecution as well as in favor of the defendant by the defense. This is where the two sides present their competing narratives about the defendant and the alleged crime. I expect that some applications of digital evidence will be perceived as more objective, while others may be “grayer” and more open to interpretation. I stipulate that personal communications and photographs, in particular, will be viewed by both the prosecution and the defense as a “grayer” type of evidence, open to alternative narratives.

Although I have described the three phases of the life cycle as distinct moments in the processing of a case, I recognize that they cannot be fully disassociated from each other. The three phases are logically connected: the acquisition phase shapes what records attorneys examine and discuss with their clients, which, in turn, shapes the kind of digital evidence used during the development of the case. The breakdown into phases, however, helps identify how the digital turn shapes different points in criminal defense differently. Such a comprehensive perspective provides a detailed picture of how public defenders and their indigent defendants experience the digital turn.

Organization of the Dissertation

The structure of this dissertation is as follows: Chapter 2 reviews relevant literatures on the everyday use of technology, digital evidence in the criminal justice system, and socio-legal studies about punishment and legal cynicism. I conclude the chapter with a presentation of my research questions. Chapter 3 includes details about my fieldsite, participants, and methods. I describe how data were collected and my procedures for analyzing fieldnotes and interview transcripts. Chapters 4, 5, 6 are organized around the life cycle approach. Chapter 4 focuses on the acquisition phase, Chapter 5 on the analysis phase, and Chapter 6 on the application stage. In each of those three chapters, I first describe and analyze findings from the respective phase in the life cycle, then I discuss those findings in the context of socio-legal studies as well as critical race theory and communication scholarship. Chapter 7 focuses on concluding remarks. Here I briefly review findings for each phase of the life cycle, then I discuss the limitations of the dissertation project, and lastly, I present future research directions.

Chapter 2: Literature Review

Technologies of Social Mediation

In the introduction, I noted that the digital turn in the criminal justice system is closely tied to the growing popularity of smartphones and the communication practices people have developed around new technologies. Although digital evidence can come from a range of sources, some of the fastest growing branches of digital forensics are mobile forensics and social media preservation (Chernyshev et al., 2017; Mateescu et al., 2015; Murphy & Fontecilla, 2012), which indicates that smartphones and social media are key sources of digital evidence in the digital turn. It is important to note here that smartphone and social media use are often combined into one activity. In fact, accessing social media applications like Facebook, Twitter, or Instagram from one's phone is an integral part of smartphone use, and studies have shown that most social media time is spent on smartphones rather than desktop computers (Sterling, 2016). Now, I review the centrality of smartphones, and by extension, social media, for how people organize their social, personal, and professional lives.

A defining feature of smartphones, and cell phones in general, is that they allow us to be connected to people, information, and services while in transit. Cell phones are small, portable, and offer convenient "person-to-person accessibility" (Ling, 2012, p. 123), giving people who may otherwise be alone or isolated the opportunity to interact with their contacts (Hampton, Goulet, & Albanesius, 2015). The diffusion of internet-capable smartphones has increased the scope of mobile communication beyond calls and text messages. Smartphones enable communication through email, social media, video chats, and other media typically associated with personal computers (Aaron Smith, 2015), thus blurring the line between computer-mediated communication and mobile communication (Humphreys, Von Pape, & Karnowski, 2013; Lu, 2017; Purcell, Entner, & Henderson, 2010).

Studies suggest that people have even developed emotional attachments to their phones, because of the connection to the outside world they provide and the amount of personal information they hold (Konok, Gigler, Bereczky, & Miklósi, 2016; Turner & Turner, 2013). Holte and Ferraro (2018) describe college students as being “tethered” to texting. Clayton, Leshner, and Almond (2015) found that when people were unable to pick up a ringing phone because they were playing a game, they experienced feelings of anxiety and unpleasantness, and their heart rate and blood pressure increased, suggesting there are psychological and physiological outcomes associated with the attachment to cell phones. People have grown used to having these devices readily available and struggle when faced with separation from them.

Ling (2012) considers cell phones to be technologies of social mediation. He argues that their ubiquity and taken-for-grantedness have rearranged how people think about and manage relationships in society. Communication via cell phones, he says, has become part of social organization. Our phones mediate how we interact with each other and with information, and we rarely stop to think about the central function they play in day-to-day undertakings (Forgays, Hyman, & Schreiber, 2014; Ling, 2012; Ramirez Jr, Dimmick, Feaster, & Lin, 2008). On the surface, this mediation may seem beneficial, yet there is a darker side to the embeddedness of technology in everyday communication. As technologies of social mediation, cell phones do not only enable interactions, they also “restrict them by demanding [people] be users” (Ling, 2012, p. 33). Ling (2012) means that owning a cell phone is a requirement for functioning in society. Others have echoed this sentiment, noting that cell phones are not a mere convenience, but have, in fact, “become essential to fulfill basic needs such as communications with family, safety, health, employment, commerce, civic participation, and government services" (Hofmann et al., 2017, p. 14). In many homes, cell phones are replacing landlines as the primary telephone for families. According to recent reports by the National Center for Health Statistics, 65% of children and 55% of adults in the United States live in wireless-service-only homes (Blumberg & Luke, 2018). For adults living in poverty, that number is 67% (Blumberg & Luke, 2018). These findings highlight the vital role of smartphones as social instruments. The demand to be a cell phone user in order to function in society matters in the context of the digital turn, because the more we rely on cell phones for various essentials, the more information is being collected about all aspects of our lives. Poor people for whom smartphones are a primary source of contact and information find themselves in a vulnerable position when these devices enter the judicial context.

The Appeals of Digital Evidence

Prosecutors and law enforcement have met the digital turn with excitement, and most research about digital evidence to date, has focused on the usefulness of smartphones and social media for fighting crime and catching criminals (Brunty & Helenek, 2013; Parker & Swearingen, 2012). In order to understand what cases public defenders face in the digital turn, it is important to understand how law enforcement and prosecutors use digital evidence in investigations and to mount cases against defendants. In this section, I review the appeals of smartphones and social media as sources of evidence for law enforcement and prosecutors in the digital turn.

One of the appeals of evidence from phones and social media is persistence - the fact that information remains available for retrieval and can be recovered through forensics techniques (Brunty, 2016; Murphy & Fontecilla, 2012). Thanks to this persistence, it is often possible to go back in time and retrace someone's steps and activities weeks, months, or even years after they’ve taken place (Trottier, 2012). Although all technology-mediated interactions leave behind some kind of trail, how much of a given interaction can be recovered, and how far back that record goes, varies greatly. Sometimes, all that remains available is evidence that a communication took place. This is the case for call detail records (CDRs) obtained from cell phone service providers, for example (ACLU, 2010). These records hold details about the time, place, and length of a conversation, yet they typically do not include the content of conversations (Sammons, 2014). The ACLU published retention periods for all major cell phone service providers and noted that only Verizon and Virgin Mobile retain text message content; Verizon keeps the data for three to five days and Virgin Mobile for ninety days (ACLU, 2010). Written communications, such as text messages and pictures, have a better chance of being recovered through mobile forensics (Nelson & Simek, 2014; Sholl, 2013).

When it comes to social media, law enforcement have different options for accessing potentially valuable content. Depending on a user’s privacy settings, law enforcement may be able to view someone’s profile and posts simply by relying on what is open to the public. The Georgia Bureau of Investigation, for example, admits to regularly using social media to view publicly available information that may be relevant to ongoing investigations (Keenan, Diedrich, & Martin, 2013). On Facebook, some details of a person’s profile, such as their username, profile picture, and cover photo, are publicly available independently of the user’s privacy settings and can be a starting point for information gathering (Sholl, 2013). Some social media companies, like Facebook, have an online request form readily available on their website that law enforcement can use to request records. Sometimes, these companies can even provide content that was deleted by the user but is still stored internally (Trottier, 2012).

Beyond the ability to go back in time when searching for data, persistence also allows for the creation of repositories (Ellison, Gibbs, & Weber; Treem & Leonardi, 2012). Law enforcement has quickly recognized this asset and used it to assemble databases of people of interest by combining publicly available data and officer-collected information (Sanders & Hannem, 2012). Another affordance of persistence is searchability. Stored content can be filtered for keywords, dates, names, and even geo-location information (boyd, 2010; Parker & Swearingen, 2012; Trottier, 2012). Such information can be used in the criminal justice context to tie someone to the time and place of an alleged crime (Hoffmeister, 2014; Trottier, 2012). Besides tying people to places and activities, persistence also ties people to each other through email lists, social media friends, or even phone contacts (boyd, 2010).

Besides persistence, a second reason why smartphones and social media are appealing sources of digital evidence is that they include data about a wide range of activities and behaviors (Grosdidier, 2016; Murphy & Fontecilla, 2012; Quick & Choo, 2017). People rely on their phones to maintain family connections, to stay in touch with friends, for work responsibilities, to shop online, and to seek out information on topics as varied as health and politics (Park, Chung, & Lee, 2012; Park, Lee, & Chung, 2016; Silver & Matthews, 2017). That they cover such a wide range of activities makes them useful to prosecutors and law enforcement for various investigative needs. A time-stamped photo uploaded to Facebook may show someone was participating in a rally or protest, and be used by law enforcement to locate witnesses (Trottier, 2012). In a different instance, cell tower information from phone records could tie a suspect to the location of a crime based on his/her cell phone activity (Goodison, Davis, & Jackson, 2015; Sammons, 2014). In addition to tying someone directly to a crime, technology-mediated communication records may also hold clues about a person’s past behaviors and activities. This kind of evidence could be valuable in establishing intent, motive, or state of mind (Grimm, 2014). Reflecting on what makes digital evidence valuable for prosecutors, Dean (2013) notes that, due to “the real-time capabilities” of mediated communication, people share things in the moment, often without thinking about the potential ramifications of their interactions. In other words, digital evidence is valuable because of the breadth and candidness of the personal information it contains.

Because evidence in support of guilt could come from a wide range of smartphone activities, no list of communication behaviors could ever be exhaustive. The value of mobile communication in the criminal justice context lies in the habitual, almost automated use of smartphones. Valuable information could come from pieces of evidence as varied as text message conversations between couples (Laliker & Lannutti, 2014), an email or calendar note about a business meeting, (Brown & Palvia, 2015; Funtasz, 2012), and browsing histories that show online searches (Seigfried-Spellar & Leshney, 2016).

Concerns about Digital Evidence

Critics of the digital turn have raised concerns about how and against whom digital evidence is used in the criminal justice context. Research suggests that law enforcement is going undercover on social media using fake accounts to monitor online behavior, and to follow the coming and goings of suspects (Joh, 2016; Keenan et al., 2013). To access information, police officers befriend persons of interests using fake identities, and then track their online posts and interactions with social media friends (Trottier, 2012). Studies have found that such online monitoring is highly targeted, and that people of color, especially black and brown youth, face systematic scrutiny from law enforcement (Lane, 2018; Patton et al., 2017).

Another common method of accessing digital evidence is through search warrants. Digital evidence from smartphones and other electronic devices is often acquired through overbroad search warrants which do not set limits on the scope or type of data being collected (Denney, 2018; Gershowitz, 2016). This leads to large amounts of personal data that are not relevant to the investigation to become available to judicial actors. People who are served such overbroad search warrants face unimaginable privacy intrusions. Critics of the digital turn worry that overbroad search warrants will not only unnecessarily expose people's private lives to judicial actors, but that the practice will encourage phishing expeditions, where law enforcement search through anything and everything in the hopes of finding something incriminating (Denney, 2018; Mateescu et al., 2015).

Beyond concerns about how digital evidence is acquired, there are worries that such data are prejudicially applied against marginalized groups. Research suggests that the breadth of information available through social media, in particular, allows prosecutors to curate pictures and posts based on what best fits their narrative of the defendant. In the context of gang prosecutions, social media photos in which black youth pose with weapons or throw hand gestures have been used to make moral arguments about them as dangerous and threatening (Patton, Eschmann, & Butler, 2013; Patton, Leonard, Lane, et al., 2016). Scholars have pushed back against these uses of social media in the criminal justice system by arguing that they are prejudicial and often rely on unfair stereotypes of criminals and criminal behavior. These critics of the digital turn worry about the implications of interpreting social media posts after-the-fact and out of context (Nissenbaum, 2010). The persistence of mobile communication means that, as part of criminal case processing (boyd, 2010), it can be "excavated" and re-interpreted at a different time and under very different circumstances. The concern with such a practice is that important contextual and temporal cues get lost in the process. Interpretations done outside of the original context may be misleading and incomplete. If taken at face value, such interpretations may have dangerous ramifications for those involved and lead to prison time or other punishment (boyd, 2010; Lane, 2018).

Mateescu et al. (2015) note that interpreting social media communications after-the-fact is problematic because people curate their online identities to certain presentations of the self. She believes making inferences based on social media presentations is especially perilous in youth cases, because young people, more so than adults, carefully craft their self-presentation according to the changing norms of their social groups. Minority youth from disadvantaged neighborhoods are in an especially difficult position when it comes to managing online impressions. Studies have shown that youth who live in gang-affiliated areas feel the need to portray a tough image online to fit in with others from their neighborhood. This can give the impression that they are involved with drugs and violence (Stevens, Brawner, Gilliard-Matthews, Dunaev, & Woods, 2017), when, in fact, they are merely following community behavioral norms about posturing (Mateescu et al., 2015; Patton et al., 2013; Patton, Leonard, Cahill, et al., 2016; Smiley, 2015).

The Context of Public Defense

In previous sections of this chapter, I described the appeals of digital evidence for law enforcement and prosecutors. I also pointed to major concerns about how and against whom digital evidence is used in the digital turn. Now, I turn my focus to the context of public defense. To understand how public defense has been affected by the digital turn, it is important to consider the work conditions of public defenders and the longstanding history of discrimination that many of their poor, black defendants have experienced at the hands of the criminal justice system, and which they bring to their interactions with public defenders.

The work of public defenders. Although the adversarial criminal justice system of the United States assumes a level playfield between the defense and the prosecution, the reality is far different (Wice, 2005). Public defenders are public servants who operate with limited resources and carry heavy caseloads. National assessment studies have shown that, across the board, public defenders face unreasonably high caseloads and work expectations (Farole & Langton, 2010; Weiss, 2005). According to research by Farole and Langton (2010), public defenders in state-based programs received an average of 358 new cases per attorney in 2007. Such assignments do not allow public defenders to spend much time on individual cases. This is especially true when one considers the range of activities involved in processing a case, including, pre-trial preparations, attorney-client meetings, filing motions, engaging in legal research, and spending time in court (Farole & Langton, 2010). When comparing the actual number of caseloads to the number recommended by the U.S. Department of Justice's National Advisory Commission on Criminal Justice Standards and Goals (NAC), Farole and Langton (2010) found that the median, state-based, defender program operated at about 66% capacity, meaning it had only 128 attorneys instead of the 151 recommended by the NAC. These numbers do not account for other activities, such as office meetings, administrative responsibilities, and continuing legal education programs in which many public defenders participate as part of their work responsibilities.

It is also worth noting that, although the prosecution has some discretion to choose which cases it wants to take on, public defenders have to represent all defendants whom the DA's office wantts to convict (Wice, 2005). Given these work conditions, many public defenders find themselves strapped for time and having to engage in triage to prioritize those cases in highest need of attention (Wice, 2005). It is estimated that 95% of criminal cases end in plea bargaining largely because of heavy caseloads (Van Brunt, 2015). Since Farole and Langton (2010) conducted their assessment of public defender office caseloads, many programs have faced additional budget cuts, leaving them with even fewer resources (Elm & Dellinger, 2013).

In addition to heavy caseloads, public defenders often have to contend with clients who are distrustful, uncooperative, and doubt the loyalty of an attorney for whom they are not directly paying (Davis, 2007). This places an additional strain on their work conditions. Surveys of defendants serviced by public defenders found that only 20% felt their attorney was on their side (Casper, 1972; Weiss, 2005). Most of these fears are based on false public perceptions. Research has shown no discernable differences in case outcomes between public defenders and those who are privately retained (Wice, 2005). The only major difference in the service provided by public defenders compared to private defense attorneys was the amount of time each group spent with clients (Wice, 2005). Studies have shown that private attorneys were able to dedicate more time to face-to-face meetings and hand-holding than their public defender counterparts (Wice, 2005). Despite these findings public defenders still face clients who question the quality of their representation. In public defense, it is not uncommon for court-appointed attorneys to be insulted by their clients or to be accused of not being “real lawyers” (Davis, 2007).

The punitive turn. Public defenders represent indigent defendants, people who cannot afford to pay for a private attorney. Because of high poverty rates among Hispanics and African Americans, racial minorities make up the vast majority of those using the public defense system in the United States (Renter, 2010; Wice, 2005). To understand why public defenders are faced with clients who are skeptical of their loyalties or doubt their willingness to represent them fairly and equitably, one must turn to the longstanding history of continued discrimination and injustices at the hands of the criminal justice system that poor people and people of color have experienced. The 1970s and 1980s mark what is known as “the punitive turn” in American, criminal justice. This era was characterized by aggressive, legal control practices, such as tough on crime policies, mandatory sentencing, increased punishment, and the growth of law enforcement surveillance (Alexander, 2012; Stevenson, 2014; Stuart, Armenta, & Osborne, 2015). Broadly, legal control refers to the use of government regulation to enforce social order and curb deviant behavior. Legal control is executed through the application of strict sanctions against those who are perceived as non-compliant with the law (Fagan, 2008). Justified by way of arguments about public safety and the need to protect citizens from street crime, throughout the 1970s and 1980s, the state deployed regulatory measures linked to legal control to increase its punitive-control apparatus while simultaneously tightening access to government services, such as welfare and healthcare (Fagan, 2008). These developments have been disproportionately directed at low, socioeconomic (SES) neighborhoods of color, causing lasting harm and widening the inequality gap between the rich and the poor (Alexander, 2012; Stevenson, 2014).

The consequences of the punitive turn are reflected in the incarceration rates of people of color. According to recent statistics, African Americans are incarcerated at seven times and Hispanics at three times the rate of Caucasians (Pager, 2007; Stuart et al., 2015). Noncitizen offenders don’t fare much better, and are four times more likely to be imprisoned than citizen offenders (Stuart et al., 2015). It is important to point out that the costs of incarceration reverberate beyond the individuals sent to prison to those closest to them (Christian, Martinez, & Martinez, 2015; Stevenson, 2014). Family members and friends are often left to bear the financial, emotional, and psychological burdens of punitive measures (Alexander, 2012). Witnessing the incarceration of a loved one is especially hard on children (Christian & Kennedy, 2011). Research shows that parental incarceration is associated with a string of negative outcomes for children, such as childhood development issues, school failure, delinquency, and drug use (Murray, 2005; Stuart et al., 2015).

The punitive turn was also felt outside of the prison context, most notably in terms of access to government services and welfare programs. Here, punishment came in the form of increased privacy violations and the loss of autonomy. Cummings (2018) notes that, to receive benefits, individuals of low SES still, to this day, must submit to unannounced home visits, the tracking of their spending habits, and invasive, monitoring practices, such as drug and parental testing. If a person has spent time in prison, he/she is in an even more disadvantaged position as far as government services are concerned. Felons, for instance, are denied the ability to receive public housing and public assistance, and are also ineligible for various federal education grants, such as the Pell Grant (Alexander, 2012; Wacquant, 2001). In addition, in most states, felons are deprived of citizenship privileges, such as voting and jury service, sometimes for life (Alexander, 2012). The punitive turn has made criminal justice contact costly, both figuratively and literally. In addition to the personal, civic, and social costs of criminal justice contact, defendants also struggle with legal financial obligations, such as fines and restitution orders imposed by the court in addition to one's criminal sentence. These monetary sanctions are a substantial, financial burden for the poor, and failure to pay these debts may lead to further incarceration (Martin, Smith, & Still, 2017).

Legal cynicism and other consequences. These extensive forms of punishment and discrimination have led to a climate of fear, vulnerability, and suspicion. Many members of minority groups feel uneasy about the role of law and order in their lives and take steps to stay out of sight (Stuart et al., 2015). The aversion to being surveilled, cataloged, and otherwise monitored by government and related organizations is known as system avoidance (Brayne, 2014). This phenomenon is characterized by the avoidance of institutions, such as hospitals, banks, schools, and even work services that keep formal records. Those who engage in system avoidance do so because they fear that being put into the system will make it easier for the government to track them (Brayne, 2014).

Disappointment in the criminal justice system is also reflected in what sociologists have termed legal cynicism. Legal cynicism refers to "a cultural orientation in which the law and the agents of its enforcement, such as the police and courts, are viewed as illegitimate, unresponsive, and ill equipped to ensure public safety" (Kirk & Papachristos, 2011, p. 1191). Various factors such as having been stopped by police as part of an investigatory stop and witnessing police violence in one's community contribute to the experience of legal cynicism (Brunson & Miller, 2006a, 2006b; Desmond, Papachristos, & Kirk, 2016; Kirk & Matsuda, 2011). Consistent racial bias in police-civilian interactions (e.g., Black drivers are more likely than their White counterparts to experience extensive policing and questioning during routine traffic stops) have led many to doubt the law's ability to provide fair and equitable treatment (Dixon, Schell, Giles, & Drogos, 2008). On the ground, legal cynicism has been associated with people deciding to take the law into their own hands, resorting to violence, and a drop in the cooperation between community members and law enforcement (Kirk & Papachristos, 2011).

Online, legal cynicism has been one of the driving forces behind the adoption of social media avoidance, self-censorship, and content obfuscation (Marwick, Fontaine, & boyd, 2017). In their study of the social media practices of low, SES urban youth, Marwick et al. (2017) note that legal cynicism is characterized by the adoption of privacy-protecting strategies, such as using different applications for different audiences, choosing strict privacy settings, controlling tags from friends, and deleting pictures or content “that may come back to haunt [you]” (p. 5). Underlying these strategies is the idea that, like interactions on the street, online interactions can potentially be scrutinized by police or other government agencies and must therefore be carefully monitored. Youth who expressed views in line with legal cynicism noted that online interactions can increase their vulnerability, and they considered it their personal responsibility to keep private information off the Internet. They accomplished this by keeping a low profile and assuming a range of privacy-protecting behaviors (like limiting the sharing of personal information) designed to limit their exposure (Hargittai & Marwick, 2016; Marwick et al., 2017).

This distrust of the law extends also to poor people’s attitudes towards their court-appointed attorneys. In his book on the American justice system, Wice (2005) notes that many indigent defendants have a “you pay for what you get” mentality and believe that their court-appointed attorneys aren’t as good as privately retained ones, because they don’t have to pay for the lawyers’ services. They assume that their public defenders won’t be dedicated to their case or willing to fight for them at trial in the same way a private attorney would. Disillusioned, indigent defendants have also expressed concerns that public defenders may be working with the prosecution, and arranging unfair plea bargains simply to bring cases to a close more quickly (Wice, 2005). This belief is motivated by the heavy caseload public defenders face and the limited amount of time defendants spend with their court-appointed attorney.

Fighting back and critical race theory. The precarity of racial minorities and individuals of low SES is real and often destructive yet reducing marginalized populations to a victim status is to discount the efforts of active resistance accomplished by these groups. Various scholars have noted the growth of creative strategies used to fight back against police misconduct, including, filming police officers who engage in unconstitutional behavior and posting counter-surveillance footage on social media to raise awareness about police brutality (Hermida & Hernández-Santaolalla, 2018; Stuart, 2011; Stuart et al., 2015). When defendants possess video evidence of this kind, their case is often strengthened by the presence of digital evidence which substantiates their personal narrative. The evidentiary value of the resistance tactics used to fight police brutality highlight the power of individual-level agency in bringing about justice in an era of digital evidence.

But marginalized groups don't have to stand alone in their fight against the system. Although the punitive turn and the rise of legal cynicism paint a bleak picture of the relationship between the criminal justice system and marginal groups, there are opportunities for public defenders and their clients to work together against a system that has repeatedly mistreated poor people and people of color. Once such possibility is the use of legal storytelling by defense attorneys to expose instances of discrimination and raise awareness about the plight of their indigent defendants. The use of storytelling in legal settings to shed light on issues of discrimination and inequality in society is rooted in critical race theory (Delgado & Stefancic, 2012; Dickinson, 2012). According to critical race theory, storytelling can be an opening to a deeper understanding of how biases operate in the world (Rideout, 2015). The theory suggests that telling stories can be a way to invite others into new, unfamiliar worlds and humanize the experiences of marginalized groups (Delgado & Stefancic, 2012).

Critical race theory posits the idea that racism is ordinary and embedded in the fabric of everyday life, that it is predictable, institutional, and mainstream (Delgado & Stefancic, 2012). According to critical race theory scholars, the "white-over-color" ascendancy that is rooted in society is difficult to challenge for two reasons: first, racism is not openly acknowledged in everyday life, and, second, too many white, middle- and upper-class people benefit from the status quo to want to eradicate it (Delgado & Stefancic, 2012, p. 7). This has led to the continued subjugation of people of color through various social and structural forces of inequality, such as the stereotyping in the media of black men as violent and dangerous (Oliver, 2003), and the racial disparities in the War on Drugs in the criminal justice system (Alexander, 2012).

Through legal storytelling however, there is the opportunity to bring these instances of discrimination to the forefront, to make visible the struggles of minority populations, and to draw on the often-difficult life circumstances of indigent defendants to argue for leniency. Although critical theory focuses on finding ways to combat racism specifically, I believe the theory can be applied more broadly to help situate public defenders as storytellers who gather, analyze, and present pieces of digital evidence to create nuanced and often humanizing narratives about their indigent clients and their alleged crimes (Fajans & Falk, 2009).

Framing the Digital Turn in Public Defense

In this dissertation, I examine the digital turn in public defense. I focus on how public defenders and their indigent defendants, who come primarily from minority populations, navigate a criminal justice system that relies increasingly on digital evidence as part of case processing. I draw on communication scholarship about people's everyday uses of technologies, socio-legal studies about punishment and legal cynicism, and critical race theory to situate my dissertation research within broader discussions about inequality and biases in the criminal justice system. I developed the "life cycle" approach introduced in the first chapter to break down three key moments in criminal case processing: acquisition, analysis, and application. In my work, I show how these stages are shaped differently by the digital turn. I ask the following research questions:

Research Questions

Broadly:

RQ 1: What are the various entry points of digital evidence in criminal defense?

RQ 2: How do public defenders make sense of their clients and defend them on the basis of digital evidence?

Acquisition phase:

RQ 3: What are the challenges of and opportunities for acquiring digital evidence in the digital turn?

RQ 4: What role, for better or worse, do defendants' communication practices play in the process of acquiring digital evidence?

Analysis phase

RQ 5: What are the challenges of and opportunities for attorney-client interaction in the digital turn?

RQ 6: How do public defenders analyze digital evidence as part of case processing? In what ways (if any) has the digital turn shaped how they approach their work?

Application phase

RQ 7: How is digital evidence applied to defense case arguments and strategy?

RQ 8: How do public defenders work with digital evidence that is used against their clients?

Chapter 3: Methodology

This study used ethnographic research methods, specifically observations and interviewing, to examine the implications of the digital turn in criminal case processing for public defenders and their indigent clients. The study was approved by the Rutgers University Institutional Review Board, and fieldwork took place between August 2017 and December 2018 at a fieldsite in New York City (NYC). There were two phases of the project. Phase one consisted of an ethnographic study of the day-to-day operations of the digital forensics laboratory of the Northeastern Defender Association (pseudonym), a large public defender office located in NYC. Phase two consisted of in-depth interviews with attorneys and investigators who worked for the public defender office. I purposely combined observations with interviewing to follow digital evidence as it moved through the public defender office, from its initial arrival in the digital forensics lab to its application towards case development by attorneys in later stages of the life cycle. In two instances, I was able to follow digital evidence all the way into the courtroom and conduct trial observations. When writing my findings, I drew on my ethnographic fieldnotes and the interview data to provide a more complete picture of the role of digital evidence at different moments in criminal case processing. Certain phases of the life cycle framework draw more heavily on one type of data. For example, the acquisition phase, since it focuses on how digital evidence finds its way to the public defender office and the processes behind recovering digital evidence, draws almost exclusively from my observations in the lab and the resulting fieldnotes. The other two life cycle phases rely on both interview data and ethnographic fieldnotes. In this chapter, I include details about the site of study, data collection, participants, and data analysis.

Phase 1: The Digital Forensics Laboratory

Site of study. In the summer of 2017, I established a partnership with the Northeastern Defender Association, a large public defender office located in NYC. My dissertation advisor, Jeffrey Lane, had previously developed a relationship with several attorneys from the office, and offered to act as an intermediary. He introduced me to the attorneys in charge of various units within the Northeastern Defender Office, and together, we developed project terms to ensure the study did not interfere with the work of the digital forensic analysts and attorneys and protected the privacy of the clients represented by the public defender office. The choice of this particular fieldsite was motivated by the fact that the Northeastern Defender Association had recently, in 2013, established a brand-new digital forensics lab, the first of its kind in a public defender office in the northeast. Most public defender offices outsource to offsite consulting firms their requests for digital evidence assistance. Partnering with the Northeastern Defender Association therefore represented a unique opportunity to study how public defenders and digital forensic analysts worked jointly with digital evidence as part of criminal case processing. The main office of the Northeastern Defender Association was located a few blocks from the criminal court in lower Manhattan, which also made it easy to walk over to the courtroom for trial observations when the opportunity arose.

The criminal practice branch of the Northeastern Defender Association represented indigent people who could not afford a private attorney. Clients were low-income New Yorkers, primarily from minority populations. The Northeastern Defender Association's primary office was in Manhattan, but there were satellite offices across all five NYC boroughs. All in all, the office employed more than 1,100 attorneys. The digital forensics laboratory (lab) was located on the second floor of the Manhattan office. Four digital forensic analysts and one supervising staff attorney operated the lab. The digital forensic analysts were professionals trained in the recovery of information from computers and other electronic devices. The lab, with its dull off-white walls and nondescript office furniture, had a minimalist feel. The desks of the four analysts were backed against the walls in a U-shape, and the fourth wall was occupied by various cabinets, shelves, and digital forensic equipment. The lab of the Northeastern Defender Association paled in comparison to the $10 million in-house cybercrime lab of the Manhattan district attorney's (DA's) office, which boasted a staff of 75 full-time specialists in cyber intelligence, mobile forensics, and cell site analysis (Taylor, 2016).

Within the Northeastern Defender Association, the digital forensics lab functioned as a hub of sorts. Defenders from all five boroughs sought the lab's assistance on cases with digital evidence. The digital forensics lab in the main office was created in 2013 in response to a growing demand for help with digital evidence in criminal cases. Having an in-house lab was a rarity in the context of public defense and it provided the attorneys at the Northeastern Defender Association an unparalleled advantaged compared to other public defenders. George, the lab's supervisor, explained that given the increasing presence of digital evidence across all cases, it made sense to have an in-house service to provide cheaper and faster support. The current team of analysts was gradually assembled over years. The first analysts to join the lab was Andrew. He held a bachelor's degree in digital forensics and started working for the Northeastern Defender Association right out of college in summer 2013. As the lab expanded, Kelly and Ben were added later that same year. Kelly had a master's degree in digital forensics and cybersecurity and had worked in several information technology jobs before becoming a digital forensic analyst. Ben had already been working with Northeastern Defender Association as an investigator specializing in digital evidence, when in 2013, he made the switch to the lab. Sarah was the latest addition to the team and was primarily trained in computer forensics.

The lab's purpose was to assist with the recovery, preservation, and examination of digital evidence. George described the work of the lab as revolving around three core responsibilities. First, they acquired or recovered evidence for clients, especially evidence which may help a case in some way. Second, given that they were a public defender office and thus focused on defending, they checked the authenticity and accuracy of any data they received from the prosecution and which may be used against their clients. And lastly, George saw it as the lab's responsibility to learn about technological flaws and limitations so that they could help defense attorneys spot overstatements and inaccuracies in cases with a digital evidence component. By positioning myself in the lab, I was able to observe the comings and goings of defense attorneys as they worked with the digital forensic analysts to recover and analyze digital evidence for their cases.

Data collection. Between August 2017 and September 2018, I conducted twenty-five full-day observations in the digital forensics lab of the Northeastern Defender Association and two trial observations in the nearby criminal court. I went into the field typically once a week, with most field days being dedicated to observations in the digital forensics lab. My observations in the lab were overt, which means that I took notes openly in front of the analysts and attorneys. This technique allowed for detailed, handwritten fieldnotes to be taken. I followed the recommendation of Tracy (2013) to write "rich and thick" descriptions of my observations, including verbatim quotes (p.116). These raw records, which I recorded in a plain notebook, were turned into longer, typed fieldnotes within thirty-six hours of each field visit. A short turnaround time is essential for maintaining high accuracy as well as vividness and richness. All in all, my twenty-five visits to the digital forensics laboratory yielded 157 double-spaced pages of typed notes.

I selected observation as a research methodology, because such an approach is well-suited for the study of people and individuals as they go about their day-to-day lives and work responsibilities (Emerson, Fretz, & Shaw, 2011). Furthermore, scholars have argued that ethnography is most appropriate for "exploring complex phenomena about which there is little knowledge," because it allows researchers to build understanding of a phenomenon gradually through natural observations (Krathwohl, 2009, p. 236). The digital turn fit the description of such a phenomenon, it was a new development in criminal justice, and specialized digital forensics branches such as mobile device forensics and social media forensics were still in their infancy (Chernyshev et al., 2017). On my fieldwork days, I observed the work of the digital analysts and their interactions with the public defenders in the office. This observation process allowed me to develop an insider's perspective on digital evidence in criminal defense. Ethnography's trademark attention to detail also allowed me to portray the phenomenon of digital evidence in great depth and in context, and to illustrate it with comprehensive examples (Tracy, 2013). George, the analysts, and the defense attorneys at the Northeastern Defender Association were excited about the research project. Throughout the duration of the study, they were enthusiastic about my presence in the digital forensics lab and the public defender office more generally. On field days, I typically spent the entirety of the day in the lab. I would eat lunch with the analysts, and during moments of downtime we talked about personal interests and hobbies. I shared an interest in video and board games with Ben and Andrew. I enjoyed telling them about the college-level Serious Games course I taught, and Andrew would let me know when he came across an interesting new game or if there were any special game sales taking place. I also watched some of the same television shows as the analysts, and on more than one occasion we discussed the cybersecurity show Mr. Robot and its depictions of hacker culture. These non-research-based interactions helped me establish a strong rapport with the research participants and allowed me to connect with them on personal level.

Analysis. To make analytic sense of the observations and stories I recorded as part of my fieldwork, I used a grounded theory approach, as defined by Charmaz (2014), to code my fieldnotes. Charmaz (2014) defines coding as “naming segments of data with a label that simultaneously categorizes, summarizes, and accounts for each piece of data” (p. 111). As per Charmaz’s (2014) instructions, I completed my coding in two phases: initial coding and focused coding. In the initial round of coding, I printed out, and then read the entirety of my typed fieldnotes line by line with a focus on incidents and cases. In the margins, I took handwritten notes that described the content of the fieldnotes. This process generated an initial list of emerging labels or codes that were highly descriptive (Charmaz, 2014). As I made my way through the fieldnotes, I also used the constant comparative method and analyzed my data for similarities and differences, considering how incidents and cases related to each other. It is at this stage that I noticed the emergence of the life cycle as a framework for my findings. After completing the first round of coding, I discussed my preliminary notes with my advisor, and based on our conversations, I refined my conceptualization of the life cycle and made changes to the initial list of codes. Among other things, I started to keep track of certain recurrences, such as the number of cases that dealt with social media versus other types of digital evidence or how often I observed certain digital forensic examination techniques.

The second round of coding was more focused. In the focused coding phase, I re-read my fieldnotes line by line, and used “the most significant or frequent initial codes to sort, synthesize, integrate, and organize" the entirety of my data in an Excel sheet (Charmaz, 2014, p. 113). This second round of coding was a thorough analysis of all 157 pages of notes taken during my fieldwork. I recorded the codes in Excel along with page numbers for illustrative quotes and examples. I refined my preliminary codes and then organized my updated codes thematically around the life cycle approach, keeping track of where in the life cycle certain codes and categories occurred. Lastly, as part of my analysis, and as per my agreement with the Northeastern Defender Association, I changed all names to pseudonyms and, when needed, I altered case details to protect the identity of the clients of the public defender office. No real names were used in any parts of my findings.

Phase 2: Interviews

Participants. For the second part of the research project I interviewed defense attorneys and investigators from the Northeastern Defender Association about the role of digital evidence in their work, focusing on the opportunities and challenges they experienced in working with digital evidence, and how the digital turn had shaped attorney-client interaction. The decision to interview investigators and defense attorneys in addition to conducting observations in the lab was motivated by the desire to understand how digital evidence was handled at different moments of case processing and to learn the outcome of the cases I was introduced to in the lab. Charmaz (2014) notes that it is common for an ethnographer who chooses grounded theory to "move across settings to gain more knowledge of the studied process" (p. 23). To make sense of the life cycle of digital evidence, I needed to follow cases as they developed, which called for going beyond the lab and talking with defense attorneys and investigators who dealt with digital evidence in their day-to-day work. I spoke with 18 attorneys and 2 investigators for a total of 20 interviews. The sample included 13 women and 7 men. Participants ranged in age from 30 to 56

(*M*=40). On average, interviews lasted 52 minutes, and were conducted either in person (n=18) or on the phone (n=2), depending on the participant's availability and personal preference. For their time, research participants were compensated with a $50 Visa gift card.

Interview participants were recruited using a combination of purposeful sampling and snowball sampling. During my observations in the lab, I had the opportunity to meet attorneys and investigators who worked on cases with digital evidence. With the help of George, the staff attorney who supervised the digital forensics lab, I reached out to several of those attorneys about participating in interviews. These participants were purposefully invited to participate in the study because of they used the services of the digital forensics lab.

Then, to gain additional research participants, at the end of interviews, I asked attorneys to recommend colleagues who they thought would be interested in participating in the study. This type of snowball sampling method is a useful approach for populations where members are interconnected (Schutt, 2012). Attorneys and investigators who worked on cases with digital evidence often consulted with each other and were thus in a good position to recommend additional participants. Throughout the data collection process, I made to also recruit interviewees across a range of demographic factors and work experiences.

Data collection. Interviews were conducted in person or via phone and were audio recorded. In-person interviews took place either at the offices of the Northeastern Defender Association or at a nearby coffee shop. Interviews lasted an average of 52 minutes and were audio-recorded. Participants were given a copy of the informed consent form that included an overview of the research project, a business card with my contact information, and their participation incentive. They then verbally consented to participate in the study and to be recorded. No signatures were collected. Once each interview was completed, the audio-recording was sent out to a third party to be professionally transcribed. The service then returned a completed transcript in word document format. I continued to recruit interview participants until all aspects of the interview guide were illustrated with sufficient rich and detailed examples.

During the interview, participants were asked a series of semi-structured questions about the challenges and opportunities of using digital evidence in their cases and in criminal defense work more broadly. The interviews included questions such as: How did this particular case come to you and what was it about? What role did technology play in the case? What surprised you about the role of communication? What was the outcome of the case? Which communication/social media platforms do you encounter most often? A for a complete interview protocol for defense attorneys can be found in Appendix A and a complete interview protocol for investigators in Appendix B.

Analysis. After the interviews were professionally transcribed, I carefully reviewed them for accuracy, making corrections as necessary. To make sense of the interview data, I used a two-step coding approach (initial coding followed by focused coding) similar to the grounded theory method used to analyze the fieldnotes. I read the interview transcripts with an iterative approach. Iterative analyses alternate between emergent themes and existing theories and literatures (Tracy, 2013). Like grounded theory, the iterative approach consists of two phases of coding. In the initial coding phase I immersing myself in the data by conducting a first round of descriptive codes. This involved going through the transcripts line by line and labeling what was being said using descriptive language. This part of the analysis was about capturing the essence of the interviews (Tracy, 2013). During the process, I remained open to the data, taking in nuances and new themes as they emerged. I applied this approach to 10 (50%) of the interviews. At the end of the first round of coding, I had a tentative list of codes. As with the analysis of my fieldnotes, after completing the first round of coding, I met with my advisor to assess the validity of the preliminary codes. This discussion helped me formulate my codes into interpretive concepts. As with the fieldnotes, I organized the different codes I identified around the phases of the life cycle, noting when themes such as “information overload” or “humanizing of clients” appeared in relation to the different phases of the life cycle.

In the second, focused coding phase, I critically examined all 20 interviews using the codes identified in the first round. The function of the second round of coding was to “explain, theorize, and synthesize” the entirety of the data using the improved, interpretive codes (Tracy, 2013, p. 194). As part of this process, I also turned to existing disciplinary concepts and theories to see if my data intersected with them. This helped identify which theories and concepts engaged with my findings. Revised codes were recorded in Excel along with page numbers to relevant examples. This Excel sheet was separate from the Excel sheet in which I recorded the fieldnote codes from my lab and courtroom observations, and followed its own coding scheme. Here too, I noted to which phase of the life cycle certain codes pertained so that I would be able to trace digital evidence and its implications through different moments of case processing. Lastly, as with the analysis of my fieldnotes, I only used pseudonyms in my write-up. When necessary I also changed case details or location information to protect the identity of the defendants whose stories the attorneys shared during interviews.

Chapter 4: The Acquisition Phase

The acquisition phase is the first stage in the life cycle approach. During this phase, public defenders at the Northeastern Defender Association worked closely with two intermediary, role specialists, digital forensic analysts, and investigators to acquire digital evidence that could be beneficial to a defendant's case. Digital forensic analysts are professionals trained in the recovery of information from computers and other electronic devices, whereas investigators specialize in the gathering of on-the-ground evidence and questioning witnesses. At the Northeastern Defender Association, the public defenders have a unique, in-house, digital support system, in which these different areas of expertise come together in a collaborative effort to secure digital evidence for indigent defendants, thus restructuring attorney-client interactions around a larger pool of judicial actors who are part of a defense "team." Other public defender offices typically outsource to offsite experts their requests for digital evidence assistance. The key goal of this stage is to acquire digital evidence that might exculpate or otherwise help clients and place public defenders in a stronger position to articulate an alternative theory of the case that counters or complicates the prosecution's narrative. This stage is about the defense's efforts to acquire evidence of its own. Later, in the analysis phase, I will discuss how public defenders deal with information received as part of discovery – the process by which the prosecution shares the evidence it has collected about the defendant - and how they assess it alongside the evidence they have collected in the acquisition phase.

In the digital turn, I argue that digital evidence becomes a story-telling tool used by both sides to create competing narratives about poor defendants and their alleged crimes. The acquisition phase of the life cycle also marks the beginning of public defenders as storytellers (Delgado & Stefancic, 2012). This is where they collect important building blocks for the narrative they will create about their client and the circumstances of the crime. In the digital turn, I find that the process of acquiring such evidence brings judicial actors into contact with increasingly personal parts of defendants' lives. This occurs in terms of sensitive types of personal data and outreach to family members and others who are close to the defendant to aid in the acquisition process. My findings show that although this initial data acquisition process is laden with challenges, from clients who are reluctant to turn over devices to the inability to recover deleted content, the acquisition phase also presents new opportunities for defendants who are cooperative and proactive about evidence preservation to help shape the legal arguments made on their behalf.

This chapter is divided into three thematic parts. In the first part, I describe my first day in the field and how the efforts of the public defenders and analysts in the acquisition phase have implications for later phases of the life cycle. The second part briefly introduces the main types of forensic examinations the analysts performed. I then examine two, core, acquisition challenges: a) getting devices to the lab when clients are incarcerated or otherwise unable to come to the lab, and b) dealing with hesitant, fearful, and angry clients who are reluctant to turn over their personal devices. The last part examines how people's use of technology, for better or worse, shapes what can be recovered as evidence during the recovery process. I close the chapter with a critical analysis of my findings in the context of critical race theory and legal storytelling.

Learning about Public Defense Work

Midafternoon in early August 2017, I was sitting at a desk in the digital forensics lab of the Northeastern Defender Association, excited to begin fieldwork for my ethnographic study of the role of digital evidence in public criminal defense work. My morning had been filled with introductions, meetings, and office tours, but, at approximately 2 p.m. things seemed to be slowing down for the day, and I finally unpacked my lunch. I had hardly taken a bite of my sandwich when the office phone rang. I looked to my right to see whose desk phone was lighting up and noticed that Kelly had picked up the receiver, "Digital forensics, this is Kelly," she said. I put down my food and watched as Kelly cradled the phone in the crook of her shoulder to free up her hands for typing. She pulled up her work email. Although I was able to catch only small bits of the conversation, I heard enough to deduce that Kelly was speaking with one of the defense attorneys from the office. I observed her as she opened a file and switched back and forth between her email and the new document. Every now and then, Sarah, who was sitting to my right, glanced over at Kelly as if waiting for instructions. After a few minutes, the phone call was over, and Kelly turned around to share the details of the attorney's request.

"It's an assault case," she said. I learned that the incident had taken place in Brooklyn on March 26th, and that the client had been charged with physically assaulting his girlfriend. "The client claims he didn't do it; that he was in Atlantic City at the time of the assault," Kelly said. The attorney in charge of the case had already obtained the client's call detail records (CDRs) from AT&T, and now Kelly's job was to use these data to verify the client's claim. To do so, Kelly planned to create a map that traced the defendant's movements based on his cell phone activity between 11 a.m. and 4 p.m. on March 26th. There was a certain steadiness in the tone of Kelly's voice that told me she had done this before. As she launched a program on her computer, Kelly turned to Sarah and instructed her to go ahead and prepare a map too. "That way we can compare layouts," she said. Sarah was the newest analyst on board, having joined the digital forensics lab only the previous month. The digital forensics lab of the Northeastern Defender Association was a small, intimate team that consisted of four analysts and one staff attorney. As a new hire, Sarah was still undergoing training. Working on this mapping project would be a good exercise for her, Kelly explained. I moved my chair closer to Kelly’s to have a better view of her computer screen. For the next forty-five minutes, I watched as the two analysts prepare their respective maps using Google Earth Pro, a geospatial application software that supports the analysis and capture of geographical data. Using the location of the cell towers listed on the CDRs, Kelly and Sarah plotted a path of the client’s phone calls, carefully marking each call with a separate pin.

It didn’t take Kelly long to realize that the client had not been in Atlantic City during the timeframe of the assault, but had, in fact, been in Brooklyn and in close proximity to the location of the incident. “He was in Atlantic City the *previous* day,” she said pointing to the map. Slowly with her finger, she traced the path of red dots moving north from Atlantic City towards New York. Although she had initially planned to mark only calls that had taken place around the time of the incident, Kelly had mapped almost two days’ worth of calls to create a visual timeline of where the client had been, based on his cell-phone communications. “Each cell tower has three antennas, and the call detail records list which antenna picked up the signal,” Kelly said. She paused and looked at me while I wrote all of this down in my notebook, then turned her eyes back to the map on her computer screen. “This reduces the potential radius to an angle of 120 degrees and allows us to map the direction of the call,” she explained. I nodded. Adding the directionality allowed Kelly to show that the client had not only left Atlantic City on March 25th, but that he had moved towards Brooklyn and then lingered in that area for the rest of the day on March 26th. A little later, Sarah finished her map and confirmed Kelly’s findings. Both analysts agreed that the client had lied to the attorney about his whereabouts. There was some truth to the Atlantic City statement, he had been there, but according to the CDRs, he was not there on the day of the incident.

Just as Kelly and Sarah finished, the door to the lab opened and George, the lab's supervisor, walked in. As the lead staff attorney, George's job was to oversee the work of the analysts and provide legal and technical advice on the cases coming through the lab. Noticing that I'd been immersed in a conversation with Kelly and Sarah, he asked us what we'd been up to. Kelly brought him up to speed on the maps she and Sarah had prepared. Before she could finish, George asked whether they had found something that helped or hurt the client. "It's not good for the case," Kelly said. She went on to explain that the evidence showed the client had lied about his whereabouts. George let out a sigh, "When will they learn?" he asked. I could tell from his tone that this was not the first time a client had been untruthful. George and Kelly followed-up on other ongoing cases, and I took this time to finish my lunch.

Later in the afternoon, I asked Kelly what her findings from earlier meant for the assault case. It seemed to me that the work she and Sarah had completed using the CDRs data was not going to be helpful for the client. What were they going to do with the maps? Kelly leaned back and turned her chair around to face me. She explained that even though this evidence did not support the client's claim – it showed the client had lied about his whereabouts – generally, attorneys were glad to know the evidence, no matter what it showed. "They use it to get the story straight, to push for a plea, or even to confront their clients about the truth," she said. She planned to send the map she'd prepared, along with a brief report describing her work, to the attorney on the case, so the map could be analyzed alongside other evidence in the case.

Although I didn't fully comprehend it at the time, Kelly was telling me that more often than not, in criminal defense, they deal with digital evidence that hurts a client's case. Yes, there was the occasional case of mistaken identity or wrongful arrest, for which digital evidence helped secure dismissals or acquittals, but those were exceptions. Public defenders relied on digital evidence to better understand the circumstances around an alleged crime and, in cases such as the one I had just observed, to confront clients about the facts of the case. Although the Atlantic City case was fairly straight forward in tying the defendant to the location of the crime, Kelly explained that she often recovered digital evidence that was more open to interpretation and that allowed defenders to create nuanced narratives around the circumstances of a crime to help the defendant's case. This process of crafting legal narratives began in the acquisition phase and continued throughout the various stages of the life cycle. Once digital evidence had been acquired, public defenders began to evaluate its place within the larger story of the crime. Sometimes digital evidence persuasively confirmed the defendant's involvement in the alleged crime. In such instances, the legal storytelling of public defenders was limited. But digital evidence could also show that there were multiple sides to each story and evoke sympathy for the often-difficult lives of indigent defendants. Such types of digital evidence were an asset during plea negotiations, where they could help secure a probationary sentence over jail time or limit a client's period of incarceration. Even digital evidence that tied clients to the crime was useful for the story-telling work of public defenders, because it allowed them to prepare against the prosecution's narrative of the events. Furthermore, whether helpful or harmful, digital evidence was a valuable asset during attorney-client meetings, because it gave public defenders something tangible to point to when discussing possible case outcomes and whether to consider a plea offer. Digital evidence was key to how the attorneys came to understand and defend their clients in the digital turn.

That neither George nor Kelly seemed surprised that the client had lied about his whereabouts and given a false alibi foreshadowed the various everyday challenges of public criminal defense that I would observe in the coming months. Many of the indigent defendants serviced by the Northeastern Defender Association had had past negative experiences with the criminal justice system and were distrustful of attorneys on both sides (Wice, 2005). They also faced hardships that made it difficult to cooperate fully, even when they wanted to work with their attorneys. It was not uncommon for clients to miss appointments, lie to their attorneys, or be reluctant to turn over personal devices for forensic examination. All these elements came into play throughout the life cycle of digital evidence in criminal case processing.

How Digital Evidence Finds its Way to the Lab

In the acquisition phase, the public defenders at the Northeastern Defender Association worked closely with digital forensic analysts who specialized in the recovery, preservation, and examination of digital evidence. Common forensic jobs that the analysts performed in the lab were: 1) mobile forensics, 2) social media preservation, and 3) cell site analysis. Mobile forensics was by far the most popular type of digital evidence recovery method and involved recovering various contents from cell phones. In my field observations I noted thirty-nine different cases in which the analysts performed phone extractions; I also learned of a dozen more in my interviews with the various public defenders in the office. Social media preservation came in second in popularity with twelve separate cases observed. Here, the analysts worked to save Facebook, Instagram, and other social media pages, often using the login information of clients. An additional piece of digital evidence acquired during the acquisition stage were Call Detail Records (CDRs), which the analysts used for the construction of maps showing the location of a client's phone, based on cell tower information. In my time in the lab, I observed the analysts work on ten such cell site analysis maps. In Appendix C, I provide a detailed technical review of how the analysts acquired data using these three forensic methods.

Although the analysts liked to say that video evidence was only a small aspect of their work, I observed seventeen instances of them working with surveillance footage. The analysts actually fielded more requests for help with surveillance videos than they did for social media content. I also observed or learned about the analysts' work on a series of other forms of digital evidence, including three cases that involved audio files, two cases that required preservation of content from Craigslist and dating websites, two laptop extractions, two iCloud back-up requests, and one case about accessing data from an Xbox gaming console. The variety of these types of digital evidence gives a sense of the reach and breadth of the different technologies that people use and find their way into criminal defense during the digital turn.

I have described the types of digital forensic work the analysts provided and now turn my attention to the challenges public defenders experienced to get the evidence - generally content from smartphones, which held potentially valuable evidence - to the office so the analysts could preserve the data. Acquiring devices in the socio-legal context of public defense work wasn't easy. The process brought judicial actors into contact with the personal lives of defendants, many of whom were wary of legal actors and faced socio-economic hardships that made cooperation difficult. The acquisition efforts involved working with the family members of incarcerated clients to bring the devices to the lab, and reassuring hesitant clients that turning over their phones was in the best interest of their cases.

One key acquisition challenge for the defense was acquiring devices that belonged to clients who were incarcerated. My findings show that the consequences of incarceration reverberate beyond the individual in prison, and that family members, especially women (girlfriends and mothers), played a crucial role in helping public defenders secure digital evidence. Christian et al. (2015) note that defendants are part of a broader social network, and that the people in that network also experience consequences related to incarceration. I found that the clients of the public defender office were at the mercy of family members, who were often struggling themselves, to coordinate drop-offs with the digital forensics lab. These hidden victims of the criminal justice system faced new demands on their time and resources as a result of their loved one’s arrest. I noted numerous instances of family members arriving late, rescheduling appointments, or organizing an off-site drop-off with an investigator. Early in the life cycle of digital evidence, it was clear that the clients serviced by the Northeastern Defender Association were at a disadvantage. Whereas a well-off person, working with a private attorney and personal investigator, would likely not have struggled to deliver a phone for forensic examination, this simple process could be quite difficult for poor defendants. Indigent defendants were unable to pay for any additional assistance they required and were wholly dependent on their personal network and court-appointed attorney for case-related support (Wice, 2005). In the next pages, I discuss the often-convoluted process through which digital evidence found its way to the lab, emphasizing the creative strategies public defenders devised to acquire the needed digital evidence. I also review instances when clients did not keep their appointments and in which the process of attempting to acquire digital evidence eventually had to be abandoned.

At the digital forensics lab of the Northeastern Defender Association, the ideal scenario for a phone drop-off proceeded like this: a defendant worked with his attorney to arrange a date and time to bring the device to the lab. Once the device was in the possession of the analysts, they worked to complete the phone extraction within the next hour or two. While the analysts worked upstairs, the client waited in the lobby or stepped out to grab a bite to eat. Then, when the analysts had completed the extraction, they returned the device to the client, who, at that point, had completed his part of the process. The acquisition of social media content did not typically involve a physical trip to the office, because usernames and passwords could easily be shared via email or over the phone. The analysts would simply use the client's credentials to log in, preserve the relevant evidence, and then pass it on to the attorney.

Benevolent girlfriends. In the time I spent observing the work of the analysts, approximately half of the drop-offs followed the ideal scenario. The other half of the devices that came through the lab were delivered either by investigators or a person close to the client, such as a girlfriend or mother. These other drop-offs were necessary, because clients found themselves in situations which made it difficult, if not impossible, for them to deliver the device personally. Some were incarcerated, others lacked transportation, and others worked odd hours, which meant that they were unavailable during regular business. Because of these circumstances, intermediaries were needed, and it was not uncommon for digital evidence to be passed between multiple people before it finally landed in the lab with the analysts.

On one of my field days in September 2017, I returned to the lab from a brief stop in the break room to find Andrew hooking a phone up to the Cellebrite machine, ready to start an extraction. "You just missed the investigator who dropped off the phone," he said. I learned that the attorney on the case had been trying for weeks to find a way to get her client's phone to the lab. The client was incarcerated, so the attorney had been in touch with his girlfriend about arranging a drop-off time. The plan that they eventually worked out, Andrew explained, was for the client's girlfriend to grab the phone at her place after work and bring it to the courthouse where an investigator would be waiting to receive the device. The investigator would then deliver the phone and its pass code to the lab. As I reflected on this multi-step, drop-off scenario, I realized that working with incarcerated clients required flexibility and some level of creativity too. Kelly who had watched my interaction with Andrew, jumped into the conversation. "You know, our clients often have complicated and difficult lives, but many have women who are really responsible, come to court, and stand by their side through it all," she said, a hint of something between surprise and disbelief in her voice. Andrew nodded quietly, like he'd heard that story before, the one where the woman stands by her man, no matter how bad the situation. In the acquisition phase of digital evidence, these girlfriends showed resilience in the face of hardship and fit their new obligations to their incarcerated partner into their lives, even at their own inconvenience (Christian et al., 2015; Comfort, 2008). I had witnessed other such circumstances of what are sometimes called, "ride or die" girlfriends, women who continue to support their boyfriends or husbands, expressing solidarity in the face of incarceration (Phillips, Reddick-Morgan, & Stephens, 2005).

Two weeks later, George and the analysts ran into another drop-off dilemma. This time the challenge involved finding a way to get a piece of video evidence to the lab for an incarcerated client whose family members struggled with odd working hours and couldn't make it to the lab for a physical drop-off. At 12:40, an attorney knocked on the door of the lab. He looked tired, irritated, and, as soon as he was inside the lab, he started rambling on about issues he was having with the digital evidence aspect of one of his cases. I had a hard time following what he was saying. George suggested he take a seat, and Ben offered to take on the case. The attorney started over, slowly this time. There was a video that was valuable to his client's case, but he was having a hard time obtaining the evidence. Ben asked him what the case was about. I learned that the client had been charged with resisting arrest and obstructing governmental administration. "And the video?" asked Ben, forcing the attorney to focus back on the digital evidence aspect of the case. The attorney went on to explain that, as his client was walking home with his girlfriend, he had been tackled by a group of police officers, and the incident had turned forceful. “Now, the officers had a parole warrant for him,” the attorney said, “but they didn’t clearly identify themselves, and, because he thought he was being jumped by a random group of men, my client resisted and fought back.” At some point during all this, the girlfriend had taken out her phone and begun filming, the attorney explained. This was the video he was trying to bring into the case. After the incident, the girlfriend had forwarded the video to the client’s mother. Technically, there were now two possible ways to retrieve the video, said the attorney, but both women had odd work schedules and could not come to the office without risking losing their jobs. The girlfriend appeared most responsive and willing to help, the attorney said. “The issue here, however, is that her work doesn’t permit her to drop off the device during the day, and she doesn’t want to give it to an investigator because it’s her only phone and she needs it, obviously,” he said. Ben listened carefully, nodding every now and then to signal he was still following along. The attorney went on to explain that the girlfriend tried to email him the video, but, because of the size of the file, her email couldn’t be sent. When he heard that, something seemed to click with Ben. He had suddenly thought of a workaround. “Ok. We can work with this,” he said excitedly. The attorney looked relieved. Ben explained that he would guide the girlfriend through how to upload the video on Google Drive or Drop Box. That way, she could share the file without any concerns about size. Ben prepared an email for the attorney with his contact information and told him to forward it to the girlfriend. Ben said he had described the steps in the email, but that he would also be happy to talk the girlfriend through it all on the phone. They were going to get that video, he reassured the attorney. In the end, things worked out, and they were able to bring the video into the case.

It’s important to note that once again, the defense team worked with a close relative of the defendant (another supportive girlfriend) to acquire the evidence. Due to the demands of her work schedule, she was not able to come to the office personally, but the analysts devised a creative solution around that problem, and the girlfriend fulfilled her part in ensuring the evidence landed in the lab. The client himself was markedly absent from the whole ordeal. The entire arrangement happened without his involvement and highlights the extent to which incarceration draws family members into judicial happenings, impacting their lives as well. The girlfriend in the above-mentioned case was faced with competing obligations: going to work (which was crucial to their financial security) and helping her incarcerated boyfriend (who was dependent on her to get the video to the digital forensics lab). Her persistence throughout the data acquisition process illustrates women's dedication to their incarcerated men and the difficulties they face in responding to this demand while also sustaining their own lives on the outside (Christian & Kennedy, 2011; Christian et al., 2015).

When clients don't show. In the preceding subsection, I noted that getting the devices of incarcerated clients into the hands of the analysts could be a challenging task. However, even when defendants were not incarcerated, the drop-off process was not without problems. I noted many instances when defendants rescheduled their missed appointments and then came to the new drop-off time, but I also witnessed scenarios in which defendants did not come to their scheduled appointment and no efforts were made to setup a new time. In June 2018, there had been so many no-shows that it had become a running joke in the office that clients no longer came to their appointments. "I *might* have a client coming in today," Sarah said when I asked her what was on the schedule for the day. When I pushed her on her decision to emphasize the word "might," she simply shrugged and responded with, "He's scheduled for 11:30 a.m., but you never know." The previous week, I had found a grumpy Andrew hunched over his keyboard, when I walked into the lab. When I asked him what the matter was, he barely made eye contact.

Eventually, he took a deep breath and sighed. "It's nothing. There's just nothing going on," he said. "No cases. They all fell through." He explained that the two clients who had been scheduled to drop off phones for an extraction had not come to their appointments. They hadn't even bothered to cancel or call the lab to reschedule, Andrew said.

As I waited to see whether Sarah's client would keep his appointment, I asked her what she'd been doing during the previous week. She had worked primarily on video editing. Cropping, zooming in, the usual requests, she said. Not much had happened in the lab all morning. At noon, Kelly pulled away from her screen to look over to where I was sitting with Sarah. "You know, I was expecting a client at 10:30 a.m., but he hasn't shown yet," she said. Sarah let out a low chuckle in response. "I guess we are 0 for 2 for the day," said Kelly. They laughed and, soon after, the analysts broke for lunch. The rest of the day went by with no scheduled clients coming to their appointments, and neither Kelly nor Sarah learned why. "Maybe they forgot, maybe something urgent came up, who knows?," Kelly said. When I followed up with the analysts on my next visit, the clients still had not rescheduled, and Kelly noted that sometimes attorneys just gave up. If their clients didn't show for their scheduled appointments, there wasn't much attorneys could, she explained. Wice (2005) notes that some defendants, believing that their public defender will push them to accept a plea no matter what, see no point in putting effort into their case. Without knowing the motivations of the Northeastern Defender Association's clients for missing their appointment, it is difficult to speculate, but it is possible that the clients felt that bringing their phone to the lab would make little difference in the larger context of the case. The no-shows were a stark reminder that the public defenders relied on the voluntary surrender of their client's devices to recover potentially helpful evidence. From my interactions with the attorneys and analysts in the office, I had the impression that clients typically realized it was in their best interest to cooperate with their court-appointed attorney. But, occasionally I heard about no-shows or attorneys who, after inquiring about digital evidence assistance, did not follow through with setting up an appointment for their client. These moments of uncertainty were rarely clarified. Not knowing why a client had failed to show up for an appointment or why an attorney had decided to not use the lab's assistance after all, was part of the everyday reality of public criminal defense work.

But… it's my phone!

Up to this point I have discussed the challenges attorneys encountered in getting smartphones to the public defender office, but this was not the only hurdle in the acquisition phase. Digital forensic analysts and public defenders encountered clients who, once physically present in the office, became reluctant, anxious, sometimes even angry, when asked to hand in their device for forensic examination. Ling (2012) defines cell phones as technologies of social mediation. Communicating through mediated communication, he argues, has become part of social organization, and people rely on phones for social, personal, and professional interactions. The everyday presence of phones in people's lives has led to these devices becoming not just tools for communication, but living archives of habits, preferences, and personal data (Forgays et al., 2014; Ramirez Jr et al., 2008). In turn, people have developed emotional attachments to their phones, both for the way these devices allow them to be tethered to the world, and because of the highly personal nature of the content they hold (Holte & Ferraro, 2018; Konok et al., 2016). I believe this sense of attachment played a role in why defendants hesitated to hand over their devices to the digital forensic analysts. The situation was compounded by the socio-legal context of criminal defense work and the reality that many indigent clients were distrustful and doubted the loyalties of their public defenders (Davis, 2007; Wice, 2005). The analysts were strangers to the defendants, even though they knew that these were specialists working with the defender's office. Handing over the phone was an act of blind trust that granted another person access to highly personal information. For poor defendants, this was a big request and demanded that they trust legal agents, when the criminal justice system has continuously discriminated against marginalized people (Alexander, 2012). In the next pages, I show how defendants manifested hesitancy during drop-offs and how analysts resolved these uncomfortable encounters.

On the surface, the process of passing the phone over to the analysts sounded simple enough: sign the chain of custody form, write down your pass code, hand over your phone, then wait in the lobby for an hour while the analysts work on preserving digital evidence for your case. Many of the clients who came through the office followed this process without hesitation, and they were in and out within a couple of hours. Some hardly exchanged words with the analysts. When reflecting on the range of interactions she had experienced, Kelly noted that she had once had a client who, when asked what his pass code was, simply pointed to the tattoo on his face. 1998, it read. It was the year of his birth and the code to unlock his phone. "We didn't really speak much," Kelly said. She had just moved on with her job and performed the extraction. The level of disinterest Kelly experienced from this client was unusual. Instead, what I observed more often were defendants who showed signs of uncertainty or uneasiness. When it was time to sign the paperwork, they became silent, clutched their phone, or looked at the floor. I use the story of Amir, a young, first-time offender, to illustrate the challenges analysts faced in convincing clients to release their phones.

Reluctant clients. I met Amir during a day of fieldwork in May 2018. That morning, Kelly had followed the usual routine of catching me up on the week's happenings. She then shared that she was expecting a client for a phone extraction at 11:00 a.m. "It's for a misdemeanor," she said, "criminal mischief." We talked about the background of the case, and I learned that Amir, the client, had allegedly struck the side mirror of his Uber ride (car-sharing service) and gotten into an argument with the driver of the car. Kelly noted that it was his first arrest, and that he was young, having recently turned nineteen. Kelly's job was to perform an extraction and recover videos, photos, and the Uber receipt. At exactly11:00 a.m., Kelly's phone rang. It was the receptionist; Amir was waiting downstairs. Kelly grabbed the usual: a chain of custody form, a clip board, and a pen. She headed downstairs, and I followed closely behind.

In the lobby, I picked out Amir right away. He was the youngest person in the room. Light brown skin, dark hair, neatly trimmed beard; he was sitting quietly hunched over his phone. Kelly introduced us and explained that she was here to take possession of his phone so they could perform an extraction and get the relevant digital evidence to his attorney. After she had finished speaking, Amir shifted in his seat. He seemed nervous, uncomfortable. Clutching his phone, he turned to Kelly and asked what her job was called. The question surprised me, but Kelly didn't flinch, "I'm a digital forensic analyst," she said. "What is that?" Amir asked. Kelly explained the basics of the job, but Amir had more questions. He wanted to know what forensics meant and what other devices Kelly had examined. Eventually the questions stopped, and I thought Amir would just hand over the device, but I was wrong. Still holding his phone, he again turned to Kelly. "How long will it take?" "Around an hour," said Kelly. Amir's eyes went wide "Do you really need my phone for this?" he asked. Calmly, Kelly explained that, yes, she needed to take his phone to perform the extraction and preserve the content. "Let me show you," Amir said, as he pulled up several videos on his phone. "I'll favorite them." Each time he clicked on the little heart icon to identify a video, Kelly briefly borrowed the phone to also write down the date and time at which the picture had been taken. Favoriting the videos was a nice gesture on

Amir’s part, but I knew it was not going to show up on the extraction. Kelly needed another way to identify the videos.

When they had finished going through the various videos and photos, Amir showed Kelly his Uber receipt. At this time, I figured we were finished. Kelly extended her hand for Amir to pass her the phone, but he held onto it and proceeded to start typing a message. A moment passed. Amir looked at Kelly, “What’s the address here?” Kelly gave him the building number and street name. Amir’s phone lit up as he sent another text message, probably to let someone know where he was, I reasoned. “I’ll also need your pass code,” Kelly said, reaching out for the phone once more. Amir looked down, pensive, then handed it over along with his 4-digit, unlock code. Kelly confirmed that Amir had shown her everything he wanted the attorney to have. “I’ll be back shortly,” she said, and we finally headed back up to the lab.

Once alone with Kelly, I commented that it had taken longer than usual to get the phone from the client. Kelly admitted that it had been odd to receive so many questions, but mostly she just sensed that Amir had been scared and uncomfortable. “This was his first arrest,” she said. “This must be overwhelming for him.” In the lab, Kelly started the extraction right away. As she connected the phone to her computer, she nudged me and pointed to Amir’s screen. There was a privacy filter on the phone which made it difficult to read the screen unless you looked at it dead on. “Goes with why he was so weird about handing over his phone,” she said and then proceeded to continue with the extraction. The privacy filter on the phone suggested that Amir was not only attached to his phone, but that he was someone who cared about maintaining privacy. This provided additional context for the demeanor I’d observed in the lobby. His story highlights the dilemmas that arise when the judicial context calls on defendants to give up personal information for the needs of the cases. Amir’s questions to Kelly and his overall behavior indicated that he struggled with having to give up his phone, a device to which he was highly attached, for the chance to share to his side of the incident through the digital evidence he had preserved. By answering his questions and remaining calm throughout the process, Kelly had reassured Amir and shown that she was on his side.

Kelly wasn’t the only analyst to face hesitant clients. In October 2017, Andrew described a recent difficult encounter he had had with a client. When he explained to the client that to preserve the recordings needed for the case, he would need to have a backup of the entire phone, the client had become distressed and then outright angry. He had asked Andrew to extract only the few recordings the attorney needed and nothing else. “But that wasn’t an option,” Andrew said. Their equipment did not allow for that kind of targeted extraction. The situation escalated, and the client turned from angry to paranoid. Andrew believed that the client’s outrage was most likely related to something personal he had on his phone. “So what? Maybe he has nudes on his phone, maybe he has porn. Who cares?” Andrew said. He explained that he didn’t snoop around, and that even if he had found evidence of criminal behavior, he would not have called the police. “The only thing we are obligated to report,” he said, “is child pornography.” And Andrew didn’t believe that was the issue with this client.

Eventually, Andrew had called the attorney on the case and she had succeeded in calming down the client. Andrew took possession of the phone and performed the extraction. The hesitancy that Andrew’s client had exhibited and the earlier confrontation with Amir show that although the analysts were part of the public defender office and thus legally on the clients’ side, that did not make clients readily trust them with their personal information. Amir’s story and Andrew’s interactions with this client are indicative of the fear and distrust that often shape the relationship between public defenders and their clients (Davis, 2007; Wice, 2005). In the digital turn, cooperation meant giving up some level of privacy; it meant turning over devices that hold highly personal data so that certain pieces of evidence could potentially be used later in the case. For indigent clients this was a difficult process, both because of the personal attachment they exhibited towards their devices. and because they were asked to trust judicial agents in a system that all too often did not treat them fairly.

Digital Evidence Acquisition Challenges

Previously, I noted that digital technologies have become embedded in people's everyday lives (Hampton, 2016; Ling, 2012). Smartphones and social media applications are now key tools for relational maintenance. For couples especially, these technologies play a key role in staying in touch throughout the day (Laliker & Lannutti, 2014). As part of this everyday use of technology, people adopt habits and make decisions about how, when, with whom, and under what circumstances they communicate (Baruh, Secinti, & Cemalcilar, 2017; Child, Haridakis, & Petronio, 2012). In this context, communication scholars have found that people use preemptive strategies to protect information or limit its audience ahead of time, and after-the-fact strategies, which are actions taken to reclaim privacy of already shared information (Child et al., 2012; Häkkilä & Chatfield, 2005; Lang & Barton, 2015).

In this section, I examine how the choices people make regarding their use of technology, including the use of certain preemptive and after-the-fact strategies, affect what kind of evidence can be recovered during the acquisition phase. I illustrate how these choices have consequences for digital evidence acquisition by taking a close look at a domestic violence case between a twenty-one-year-old defendant named Alex and his nineteen-year-old girlfriend, Krista. I found that the uses of technology that presented the greatest challenges for analysts included the deletion of content, the use of ephemeral communication channels, and identity concealment.

Deletion. The communication practice most likely to lead to evidence acquisition challenges was deletion. Whenever defendants shared that they had deleted text messages that might be valuable to the case, the analysts responded with reservation. I heard the doubt in their voices as they described to attorneys, investigators, and clients the recovery chances for deleted content. Although the analysts had various forensic machines and tools at their disposal, recovering deleted content was always a gamble because of the many variables that affected the recovery process. On more than one occasion, Ben had explained that whether a deleted text or image could be recovered depended on two basic things: 1) how long ago the content had been deleted from the device, and 2) whether the owner of the phone was a light or heavy user. When content is deleted from a phone, it goes to unallocated space where it waits to be overwritten with new data. Ben explained that the chances of successfully recovering data were lower when someone was a heavy user, because there was a high chance that the deleted content had already been overwritten with new data. However, if the owner were a light user and didn't use his phone much, then there was a chance the information had not yet been overwritten and was therefore still recoverable. It was also possible for only some of the deleted messages to be recovered or even just parts of a message. The recovery process was filled with uncertainty and the analysts could therefore not make any guarantees to the attorneys about whether they would be able to retrieve deleted content. Both device specifications and how a person used the technology shaped what could be forensically recovered.

In late August 2017, Stephanie, one of the attorneys in the office, contacted Kelly for help with a phone extraction on a domestic violence case. Stephanie's client, Alex, and his girlfriend, Krista, had had a tumultuous relationship filled with arguments. The CDRs Stephanie received from the prosecutor's office showed more than one thousand calls and text messages between the couple, most of which were incoming from Krista to Alex, but she did not know *what* was in those messages. The CDRs listed the time and length of the calls and the two parties in the communication, but they did not include the contents of any text messages. Alex claimed that although it was true that he had physically assaulted Krista, she had been attacking him with repeated calls and messages, and that his actions had happened in the context of those disagreements. Unfortunately, it was difficult for Stephanie to verify this claim, because Alex had deleted most of his conversations with Krista to hide them from his wife, Valentina. Stephanie had hoped that an extraction on Alex's phone might recover some of these messages.

Soon thereafter, Stephanie first contacted the lab for assistance. Kelly had Alex's phone in her possession and performed a logical extraction. She extracted 12GB of data in less than ten minutes and then copied the extraction output to her hard drive. Alex was a heavy user; Kelly was not very optimistic that she would be able to recover any messages. Luckily, the extraction recovered a handful of exchanges between Alex and Krista. I noticed a red "x" next to them. Kelly explained that the "x" was the system's way of indicating their status as recovered information. No text messages between Krista and Alex were found for the night of the assault, but the text messages Kelly had recovered showed that there had been tensions in their relationship. She also recovered several images, which were screenshots of additional text message exchanges between Krista and Alex, including a few from the night of the assault, as well as a few voicemails from Krista to Alex.

Working with defense attorneys meant representing clients who had committed terrible crimes and assisting the attorneys in providing the best representation possible (Hara, 2009; Weiss, 2005). Kelly did not think any text message conversation could justify Alex hitting his girlfriend, but she still believed in helping attorneys understand the circumstances of such difficult cases. Sometimes she sympathized with the plight of defendants. “Clients think they’re being slick by deleting their texts and calls, but those could have been helpful, especially in a case like this where it looks like she was baiting him with all these calls,” Kelly noted. Alex may have thought that deleting his messages with Krista was a way to keep his affair hidden from his wife, but now their absence made it more difficult for Alex’s attorney to situate the assault within the circumstances of their tumultuous relationship. The use of deletion had led to the recovery of only a handful of messages and left behind an incomplete record of Alex’s and Krista’s communication history.

Ephemeral communication. I just described the extraction Kelly had performed on Alex’s smartphone, which had resulted in only a handful of recovered text messages. Kelly knew Alex had deleted his conversations with Krista to hide them from his wife, but, upon closer examination of the extraction results, she learned that there was another explanation for the absence of text messages. Kelly realized that the multimedia messaging application, Snapchat, known for deleting content after it has been viewed, had been installed on Alex’s phone. After a call to Alex’s attorney, Kelly confirmed that Alex and Krista had indeed used Snapchat for many of their conversations. Messages, photos, and videos shared through Snapchat are automatically deleted after the recipient has viewed them. The ephemerality of Snapchat distinguishes this application from other social media applications and represents a real challenge for digital evidence acquisition, because there are simply no data to be recovered. The contents of all the conversations Alex and Krista had had over Snapchat were simply unrecoverable. For someone examining the evidence, the only indication that Alex and Krista had perhaps communicated through this ephemeral, communication channel was that the application had been installed on both of their phones.

Identity concealment. An additional communication practice that sometimes led to challenges during the acquisition phase was identity concealment. Over the course of my observations in the lab, I learned that defendants and complaining witnesses alike sometimes attempted to disguise their identity during communications. One such practice was to dial *67 before calls to prevent the display of caller identification on the receiver's phone. When Stephanie received a copy of the CDRs for the case with Alex and Krista, she realized that approximately one-quarter of Krista's calls to Alex had been dialed with *67. Because *67 had been added in front of Krista's, ten-digit, phone number on the CDRs, Stephanie first thought the calls had simply come from a different phone number; it was only upon closer examination that she realized the calls had actually come from Krista, but in disguised form. As the case progressed, Stephanie learned that Krista had resorted to this practice, because Alex had stopped answering her calls; concealing her caller identification was the only way to not reveal herself when calling. The challenge of this particular communication practice was that it could become overlooked in the maze of other entries on a CDR. Unless defense attorneys were trained to look for such possibilities, it was easy to mistake the use of *67 for a merely a phone number with a unique extension.

During my interview with Stephanie in December 2017, I learned that the various uses of technology that had presented challenges for the digital forensic analysts had been motivated by Alex's personal life circumstances. Communicating via Snapchat was something he and Krista had agreed upon to hide their relationship from his wife, and Alex's decision to delete his communications was part of that same cover-up. Krista's use of *67 was driven by the fact that Alex had stopped answering her calls after their many arguments, and also after the eventual assault. The digital evidence alone, however, did not tell this more nuanced story of how people fit technology around the complex circumstances of their lives. One could opine that the act of deletion had made Alex look even guiltier, despite the fact that, according to Stephanie, the deletion had not been motivated by the assault. Defending people who had committed disturbing crimes was part of being a criminal defense attorney (Hara, 2009; Weiss, 2005). Like most defendants who came through the office, Alex was guilty of the charges brought against him. His case went to trial, and he was ultimately convicted on several misdemeanor assault charges. Although no amount of angry text messages from Krista could have excused Alex's behavior, I sympathized with Stephanie's struggle to provide a more nuanced narrative around the circumstances of the assault. When digital evidence is missing or only partially recovered, it can be difficult for defense attorneys to bring the complexities of human relationships to bear on a case; their storytelling capacity is constrained by the available evidence.

Why Would You Delete This?

I've stated previously that the majority of the clients represented by the Northeastern Defender Association were guilty of the charges brought against them. It was not surprising then, that some of the defendants who deleted text messages and other communications from their phones did so intentionally, to hide their tracks and make it appear that they had not been involved in the crime. These actions reflected decisions by defendants to purposely limit what judicial actors would be able to see. Sometimes, their efforts were successful, and the prosecution was unable to recover deleted content to tie them to the crime, and sometimes their efforts were unsuccessful, and the prosecution was able to use their communications against them. Most surprising however, were the instances in which defendants who were innocent had deleted potentially exculpatory content. These defendants were often young men who had acted out of fear that a personal lie or misdemeanor offense would come to the surface if someone were to examine their phone forensically. Child et al. (2012) note that deleting unwanted communications is the most common, after-the-fact strategy for managing disclosures. They cite many motives for such behaviors, including impression management, fear of retribution, and managing conflict with others. In the criminal justice context, the act of deleting communications had the effect of making even innocent clients look guilty, and without the content of the communications, it was challenging for the defense attorneys to build strong, defense strategies. Below, I illustrate the challenge of working with clients who had deleted helpful information by looking closely at a case handled by Esme, one of the attorneys in the office.

In February 2018, Esme came into the lab to consult with George about the digital evidence components of a current case. Esme's client had been charged with acting as an accessory to a robbery that had taken place at the fast food restaurant where he worked. Although there was surveillance footage in which the defendant could be seen working in the kitchen at the time of the robbery, the prosecution had decided to move forward with the case, because the client's phone records and the extraction they had performed on his smartphone tied him through calls and text messages to one of the co-defendants. The CDRs indicated the client had called one of the co-defendants the day of the robbery, and the extraction report showed he had deleted several of their text message conversations. George noted that the surveillance video was very solid evidence in the defendant's favor. The video showed the client wearing earplugs and mouthing something as if he were singing along to music while preparing food in the kitchen. Deletion of communications, however, always made defendants look bad, he said. Even if there were reasonable motivations for doing so, deleting text messages gave the impression that the client had something to hide, and, in the eyes of the prosecution, that suggested guilt, George said. Esme explained that the prosecution was planning to argue that her client had acted as the lookout for the robbery, drawing on his communications with the co-defendants to show they had had prior contact and could have coordinated the robbery via text message. George offered to hear Esme out and look at the CDRs and the extraction report she had received from the prosecutor's office.

In the coming weeks, I learned more details about the case from George. Before he was formally charged and arrested, Esme's client had spoken with the police about the robbery. During the exchange, the officers had taunted him; when they noticed his phone, they told him the device would prove that he had been part of the robbery. The client did, in fact, know the co-defendants, not because he had helped them rob the fast food place, but because he had been buying marijuana from one of them. Nervous that the police would find out about his drug use, which was documented in text messages, Esme's client had deleted all the texts and call logs that tied him to the co-defendants. When he was later arrested and the police took his phone to perform an extraction, the forensic analysis revealed that he had been in communication with the co-defendant, but no message content could be recovered. This made things look bad for the client, George said. The case went to trial, and, thanks largely to the surveillance video, Esme's client was ultimately acquitted. The decision to delete his communication however, had had a major impact on the defendant's life. He was charged with a criminal offence and had to go through the tribulations of a trial, all because he had been scared that his drug use would surface. As in Alex's story, the absence of communication records had complicated the defense attorney's work. Unlike Alex however, Esme's client was innocent of the charges brought against him, and, if it had not been for surveillance footage of him in the kitchen, there was a real possibility that Esme would have lost the trial. How people manage their uses of technology and the various preemptive and after-the-fact strategies they rely on as part of this process can have severe consequences in the criminal justice system. The inability to recover communications during the acquisition phase reverberates through the rest of the life cycle, shaping the ultimate outcome of a case.

Opportunities for Digital Evidence Acquisition

I explained that the decisions defendants made about their use of technology, such as opting to talk via ephemeral communication channels or deleting text messages after-the-fact, had a negative impact on the ability of the digital forensic analysts to retrieve evidence that might be valuable to the defendant's case. To consider indigent defendants as self-sabotaging individuals who hurt their own chances at a better deal, or stupid criminals who get caught for simple mistakes, however, would be to do them an injustice. Poor defendants are often simultaneously guilty of the crime they have committed and victims of a system that operates on prejudice and intimidation. Decades of research have pointed to systemic inequalities in the criminal justice system in the treatment of marginalized individuals compared to white people. For instance, black people are subjected to higher arrests rates and face harsher sentencing than their white counterparts (Alexander, 2012). And, in the context of the digital turn, it has been pointed out that digital evidence has been used disproportionately to make moral judgements about young, black defendants through evidence that is more prejudicial than probative (Lane et al., 2018). This suggests that digital evidence helps repeat existing biases and inequalities that permeate the criminal justice system. Such injustices have led poor defendants to be distrustful of law enforcement and provide context for why someone like Esme's client might delete his communications for fear of facing drug-related charges.

During my fieldwork, I noticed many instances of digital evidence hurting clients. However, I also saw pockets of opportunities and moments when poor defendants capitalized on the chance to fight against the same system that was at the core of their subjugation. Over the course of my observations, I counted seven separate instances in which defendants took active measures, both preemptive and after-the-fact, to secure digital evidence that helped their case. These pieces of evidence came in the form of video recordings of police brutality, audio recordings of arguments, and screenshots of threatening text messages, among other things. The arguments by Stuart et al. (2015) to look beyond marginalized people's victim status and recognize their efforts of active resistance repeatedly came to mind as I watched these cases unfold. In the life cycle of digital evidence, the decisions to start recording an arrest or to preserve conversations through a screenshot represented strategies by indigent defendants to fight back against the enduring biases of the criminal justice system and make their own narratives heard. Yet, as helpful as these strategies were, they were also problematic because they put the onus on victims to be prepared and have their cameras ready if they wanted to have a better chance at justice. This leaves the door open for blaming victims who fail to record their arrest, and risks creating unrealistic expectations about defendants submitting proof of their victimization. In the next pages, I review these opportunities in the context of defendants who came to the Northeastern Defender Association, knowing what evidence they wanted the digital forensic analysts to retrieve for their case.

Fighting the system. When I arrived at the office in late August 2017, Sarah invited me to watch as she and Kelly worked on a new assignment. The defendant in the case, a young, black man in his mid-twenties, claimed to have been violently tackled to the ground by a group of police officers during what was supposed to be a routine stop for suspicion of drunk driving. Typically, the only digital evidence available in such cases is the dashboard camera footage from the officer's car. This time, however, Kelly noted, the client also had video proof of the incident.

His girlfriend, who was with him in the car at the time of the arrest, had captured most of the arrest with her phone camera. The girlfriend texted the evidence to the defense attorney who then stopped by the lab so the video could be transferred from her phone. I also learned that the client was an ex-marine who suffered from PTSD, and that he had been hurt during the altercation. The video that Kelly and Sarah had on their computer screens was the video recorded by the girlfriend. "I'll play it from the beginning so you can see what happened," Sarah offered. She noted that their task was to try to obtain the police officers' badge numbers off the video so they could match them to the badge numbers and names on the police report. Kelly clarified that, although the report listed who had been involved in the incident, it didn't specify which officer had done what, and the defense attorney wanted to know which officers had tackled her client to the ground.

As the video played, I could see a black man in handcuffs standing next to a police car. The car's lights were on. Sarah stopped the video and turned towards me. "You'll notice that although the client was stopped for suspicion of drunk driving, no breathalyzer test was given at any point in the video," she said. I nodded and Sarah resumed playing the video. Soon more police vehicles could be seen arriving at the scene. Several officers grabbed the client by the arms, then pushed him towards one of the open police cars. The client stumbled and fell, but the officers kept pulling at him. A few seconds later, the client fell to the ground. I presumed this was the moment when he was injured. Next, the camera panned to the side and more police officers arrived. Kelly and Sarah counted a total of twelve police officers. Eventually, the officers succeed in pushing the man into the car and closed the door.

I watched in silence as Sarah and Kelly replayed the video several times, pausing and zooming in to see if the badge numbers were visible. Shannon and Lisa were each able to pull one badge number from stills they took of the video, thereby associating two officers with certain actions during the arrest, including one who was heavily involved in pushing the client. From the smiles on their faces, I could tell the two analysts were excited to have been able to get this information, but I also noticed a hint of surprise in Sarah's expression. I nudged her on the matter. "Sometimes transferring videos hurts the quality of the file," she explained. When she heard the attorney had been given the video by text message, she was worried about the quality, but the video had been taken with a newer smartphone and the quality was exceptionally high. The video as a whole wasn't only of good quality; it was also valuable, Sarah said. The video's usefulness was tied to the different angles of the arrest it offered, and its revelation that the client had indeed been heavily outnumbered and pushed around harshly by the police officers. I later learned from George that the case had been dismissed; the attorney never even got to present the video evidence at trial. Officially, the case was dismissed under one of the state's time limitation laws, but George said it was not uncommon for the prosecution to let cases it realized couldn't be won expire like that. After the dismissal, the client hired a civil attorney to file a lawsuit against the NYPD and planned to use the video in the lawsuit.

Other defendants also recorded events or communications as a proactive measure. As I observed these cases unfold in the digital forensics lab, I was repeatedly reminded of the power of individual-level agency in helping attorneys re-shape narratives. In April 2018, Kelly shared that she'd been working with a client who had not yet formally been charged on preserving digital evidence for a possible upcoming case. The client was an electrician who had done unlicensed work in a building, which had soon after suffered fire damage. He was worried about being charged with a crime in connection with the fire. On several occasions, the superintendent of the building had told him to lie if ever questioned about his electric work in the building, and that had worried the client. He did not believe his work was the cause of the fire and wanted to get ahead of any possible charges. When he met with Kelly, he showed her pictures he'd taken of his work and which, according to him, showed everything was up to code. Using a phone recorder application, he had also recorded some of the conversations in which the superintendent had told him to lie if ever confronted about his work. Kelly performed an extraction and preserved the data in case formal charges were brought forth. When we debriefed afterwards, Kelly commented on how surprised she was to see someone so proactive about preserving digital evidence. Her encounters were usually about trying to recover information after-the fact, yet this man had realized the value of digital evidence and had acted on his instinct to save information against a possible future charge. When I exited the field in the summer of 2018, the man with whom Kelly had worked had not yet been charged.

Digital evidence and domestic violence. All other instances in which I observed defendants proactively preserve digital evidence involved domestic violence or harassment cases. In those cases, the defendants operated with the recognition that they were guilty of the charges brought against them, but they had saved text messages or voicemails from their ex-girlfriend in an attempt to show their side of the events and demonstrate that the situation wasn't cut and dry. These techniques revealed that the defendants had, to some extent, come to terms with the charges they faced and had moved on to focus on playing a role in the legal arguments that would be developed about them in the criminal justice system. The digital forensic analysts helped with the preservation of the content and then forwarded the data to the attorneys who then applied the evidence in the client's case to create more nuanced narratives of the events surrounding the alleged crime. I will write in more depth about the value of creating nuanced narratives to influence case outcomes in the chapter dedicated to the application phase of the life cycle.

The Acquisition Phase: Discussion

My findings show that the acquisition phase of the life cycle is laden with challenges. Public defenders need to devise often-convoluted workarounds to acquire devices from clients who are incarcerated, the analysts face clients who are reluctant to turn over their devices for forensic examination, and the consequences of defendants' technology use, such as deleting messages, often have negative implications for the ability of the defense attorney to create nuanced narratives about the circumstances of a crime. Yet this initial data acquisition process is not without opportunities. I also found that when defendants are cooperative, and especially when they are proactive about evidence preservation, there is an opportunity for them to contribute to the shaping of their story in the criminal justice system. I now situate these findings about the opportunities and challenges of the acquisition phase in more detail in the context of socio-legal studies and critical race theory.

Critical race theorists propose that storytelling can be an opening to a deeper understanding of how race and inequality operate in society. Delgado and Stefancic (2012) argue that "well-told stories describing the reality of black and brown lives can help readers to bridge the gap between their worlds and those of others" (pp. 47-48). They believe that stories can help create empathy for others and make visible differences in the way the world is lived by people of color. The storytelling emphasis of critical race theory shares with the practice of ethnography an interest in understanding people's everyday experiences and describing those observed realities for others to read (Emerson et al., 2011). Both offer a lens through which to expose mechanisms of inequality and social divisions.

My ethnographic study of the digital turn in criminal case processing was motivated by an interest in understanding how public defenders and their indigent defendants navigate a criminal justice system that relies increasingly on evidence from digital technologies and personal communications. Most of the defendants who came through the public defender office were guilty of the charges they faced. For the defense attorneys, this meant that the acquisition phase focused on securing evidence that would later permit the telling of nuanced narratives around the circumstances of a crime to help secure a better deal during plea negotiations. Public defenders were storytellers. In the context of the digital turn, they looked to digital evidence to show that there were multiple sides to each story and they tried to humanize their clients against a system that had repeatedly treated poor defendants with loathing and discrimination. Although none of the attorneys I observed or interviewed stated directly that they used critical race theory as part of their defense strategies, the theory's storytelling techniques permeated their work efforts. It was a natural fit for the defensive posture that public defenders adopted when representing their clients. Both the defense and the prosecution worked around assumptions of guilt and created diverging narratives about indigent defendants and their alleged crimes.

The acquisition phase of the life cycle signals the beginning of the storytelling work of public defenders in the digital turn. It is the stage at which they acquire the building blocks for the narrative they will be presenting about their client's case. By providing the digital evidence they have in their possession, clients also help start the narratives of their cases in these early moments of the life cycle. I argue that in the digital turn, the process of acquiring evidence brings judicial actors (defense attorneys and intermediary role specialists) in contact with increasingly personal parts of defendants' lives – both in terms of the demand the process places on the family members of defendants to aid in the gathering of evidence and in terms of the types of data, personal communications, photos and videos that are acquired. These early stage confrontations between the personal and the judicial require defendants to expose parts of their lives to combat their criminal charges. In its search for better, more persuasive evidence, law enforcement has expanded its scope to digital technologies, such as social media and smartphones (Dean, 2013; Fontecilla, 2013; Trottier, 2012). To respond to charges that draw on such evidence, public defenders too, turn to digital evidence as a storytelling tool. This can lead to a double exposure for defendants, where both the prosecution and the defense rely on evidence from personal communications to build their respective narratives. Defendants face an initial loss of privacy when confronted with the charges brought forth by the prosecution, and then a second loss of privacy when they are asked to cooperate with public defenders and digital forensic analysts in the acquisition of digital evidence that may help their case.

The first hurdle that public defenders had to overcome was getting the device that held potentially valuable information or the actual piece of evidence itself to the digital forensics. Here, I found that girlfriends played crucial roles by acting as intermediates in securing digital evidence from defendants who were incarcerated. By helping get evidence that was be beneficial to their loved one’s case to the lab, these women ensured that the narrative that has been set in motion would include elements of the defendant’s story. Lane (2018) writes that young women of color often feel obligated to the men in their lives, that they experience a combination of natural caring and pressured loyalty by virtue of coming from the same place and having faced similar struggles. The dedication shown by the girlfriends of clients who were incarcerated reflects loyalty in the face of adversity and care about ensuring that their partner’s voice is heard in the criminal justice system (Christian et al., 2015). Their willingness to stand by the defendant’s side and cooperate with judicial actors contrasts with the “no-shows,” or clients who failed to come to their appointment and did not attempt to reschedule. They fought for the inclusion of digital evidence, whereas the "no-shows" gave up on having this aspect of their story included in the case. Socio-legal scholars have pointed out that the consequences of incarceration reverberate beyond the person in prison and affect family members and loved ones (Christian & Kennedy, 2011; Comfort, 2008). This still hold true in the digital turn. My findings show that defendants are at the mercy of girlfriends and other close contacts to arrange digital evidence drop-offs, and that these individuals face difficulties to incorporate these new demands into their existing responsibilities. In the digital turn, public defenders call on their participation and that of intermediary role specialists, such as investigators, to assist in the acquisition of digital evidence.

The hesitancy of defendants to turn over phones showed that telling one's story in the digital turn was not always easy. It suggests that there is a cost to having one's voice heard through digital evidence - the relinquishing of personal information to judicial actors. I noted earlier that people feel attached to their phones because of the information contained in them and because they represent a connection to society (Holte & Ferraro, 2018; Turner & Turner, 2013; Vincent, 2006). Cell phones are highly personal devices. They have become living archives of people's lives – they hold photos, videos, messages, and other personal artifacts (Konok et al., 2016). This notion of cell phones as devices rich in personal data and to which individuals are attached matters for the acquisition phase because it provides context for why some defendants were hesitant, fearful, or even angry when asked to hand over their devices. Turning over a phone was not like turning over any other piece of evidence; it meant trusting someone with access to one's most intimate information and hoping he/she would not violate that trust. This contact between client's personal lives and the judicial was further strained because the digital analysts were strangers to the defendants. Unlike attorneys who were present throughout a defendant's case, the analysts appeared only when there was a need for assistance with digital evidence. This meant analysts had little time to build rapport with clients. They encountered them only briefly, as an intermediary specialist, and typically did not see clients again after the acquisition phase. Client hesitation may also have come from doubts about whether the defense was truly on their side. Research has shown that defendants find it difficult to trust attorneys to whom they do not personally pay for their services, and who are burdened with high caseloads (Davis, 2007; Weiss, 2005; Wice, 2005). Turning over a personal device to which defendants were personally attached was not easy in the first place but turning it over to someone they didn't fully trust further complicated the drop-off situation.

Later parts of the chapter looked at the relationship between people's uses of the technology and evidence retrieval. I found that how defendants managed their communications, for better or worse, shaped what digital evidence could be recovered. Through the story of Alex and Krista, I illustrated how what seemed like appropriate communication choices within the context of a relationship turned out to have dire consequences for the ability of Alex's attorney to engage in nuanced storytelling. Alex's decisions to delete most of his exchanges with Krista and to interact with her over the ephemeral messaging application, Snapchat, greatly reduced the amount of evidence that could be recovered. In turn, Alex's ability to tell his story was hampered. Although ultimately acquitted of the charges brought against him, Esme's client also faced serious backlash and went through the whole process of a trial as a consequence of his decision to delete communications from his phone.

But defendants weren't only victims of their own communications. I found that the digital turn also opened the door for individual-level agency and defendant-driven fighting back strategies (Stuart et al., 2015). Lane (2018) argues that police and prosecutors use mediated interactions, sometimes going deep into personal relationships and histories, to criminalize defendants. I find that poor, black defendants respond to such applications of technology by repurposing those same tools to formulate counternarratives. The proactive preservation of digital evidence I observed during my fieldwork, such as the story of the ex-marine whose girlfriend filmed his arrest, are attempts by defendants to take control of storytelling. Such proactive measures allow defendants to shape the narrative that will be told about them in the criminal justice system and to expose instances of racial discrimination and police brutality. They are narratives that raise awareness about the realities of what black men experience at the hands of law enforcement in a criminal justice system that is prejudiced against marginalized populations (Delgado & Stefancic, 2012). Yet, as noted in the chapter, counting on defendants to have video evidence of their victimization is problematic, because it places the burden of proving one's discrimination on the victims themselves. It leaves open the door to argue for personal responsibility in the face of structural problems, rather than pushing for change at the system level (Marwick et al., 2017). Such efforts should be a last resort and not the norm to fight discrimination and brutality at the hands of law enforcement; or else this risks creating unrealistic expectations about victim-preparedness in the face of potential acts of violence and discrimination.

The acquisition phase of the life cycle was the starting point of the different narratives that are told about defendants and their crimes. This chapter illustrated the challenges public defenders faced in acquiring digital evidence, including having to devise workarounds for clients who couldn't drop off their device at the office, and working with clients who were reluctant to turn over devices. I found that the process of acquiring digital evidence brought judicial actors into contact with personal parts of defendants' lives in terms of sensitive types of personal data and outreach to family members of the defendant to aid in the acquisition process. This chapter also showed how defendants' uses of technology greatly affected what evidence could be recovered and the role such evidence played in establishing the building blocks of nuanced and sometimes even counternarrative storytelling.

Chapter 5: The Analysis Phase

The analysis phase is the second phase of the lifecycle. During this phase, public defenders make sense of the digital evidence in the case. They examine extensive records from smartphones, social media accounts, computers, video surveillance systems, and other sources (Nelson & Simek, 2014; Sholl, 2013), and assess how this evidence might factor in the case. It is important to note that digital evidence enters this phase of case processing through two channels: the prosecution and the defense. In the adversarial criminal justice system of the United States, the burden of proof lies with the prosecution; as such, digital evidence in support of the charges brought against the defendant comes from the prosecutor's office. By law, the prosecution is also obligated to share any exculpatory evidence it finds as part of the search process. Defense attorneys, on the other hand, focus on obtaining evidence which may exculpate or otherwise help their clients. This defense-oriented acquisition process was described in the previous chapter.

In the analysis phase, defense attorneys assume a defensive posture. They evaluate how evidence helps or hurts the case and prepare a legal narrative that benefits their client. Attorneys work primarily alone and dedicate most of their time to assessing the incriminating digital evidence that comes from the prosecution's side. The digital forensic analysts are less involved in this stage of the life cycle; their assistance tends to be focused on helping attorneys interpret technical matters related to digital evidence. If the acquisition phase was about collecting building blocks, then the analysis phase is about sorting and re-organizing these blocks into a coherent, defense narrative. I find that this process of examination brings attorneys into further contact with the personal aspects of defendants' lives, intensifying the coming together of the personal and the judicial that characterizes the digital turn in criminal case processing. In this phase, attorneys work both independently and with their clients to create nuanced narratives of the alleged crime. My findings show that the digital turn adds new burdens to already overworked public defenders by presenting them with large amounts of digital evidence to analyze. Not all attorneys are equally adept at managing this data deluge. Technology literacy among public defenders varies greatly. Whereas some successfully and persuasively use the objective properties of digital evidence to reason with clients and discuss defense approaches, others feel overwhelmed by the technological demands of the digital turn. I also find that public defenders experience shifting professional boundaries when digital evidence from personal communications becomes part of attorney-client interactions. Some attorneys experience discomfort from the access to intimate photos and private, non-crime-related family exchanges of clients, whereas others see such digital evidence as a valuable lens into their clients' lives that helps humanize defendants in a system that all too often treats them like casefile numbers.

This chapter examines two intertwined aspects of the analysis phase as they relate to the digital turn: information overload and attorney-client interactions. The first half of this chapter discusses how public defenders manage information overload in terms of their individual work practices. Here, I look at the triage systems that public defenders developed to sift through large amounts of data and how they've dealt with the often-difficult learning curve of working with digital evidence. The second half of this chapter looks at how digital evidence has shaped attorney-client interactions in both intimidating and rewarding ways. I discuss the opportunities digital evidence has brought for attorneys and clients to work together on sense-making and data interpretation. I also look at how defenders use digital evidence to reason with their clients about the realities of the case and note the varying reactions to the clients' confrontation with digital evidence. I then examine how the overload of personal information in the digital turn (although it leads to moments of discomfort for both attorneys and clients) also has the potential to help foster honest, trusting relationships between public defenders and clients. I close this chapter with a critical discussion of the implications of my findings for the work practices of public defenders and attorney-client interactions in the digital turn.

Information Overload

When reflecting on how the growth of digital evidence had affected their day-to-day work, the attorneys at the Northeastern Defender Association noted that the biggest change was the amount of information they now had to go through as part of case handling. Since cell phones and social media accounts have become sources of evidence, the attorneys worried about and examined unprecedent amounts of data. But just how much is “more information” in this context? Vicky worked on a gang-related case, in which the DA’s office turned over 95,000 pages worth of Facebook data about her 14-year-old client. Erin had a drug case, in which the prosecution shared an iCloud backup that covered multiple years of communications and personal data, and both Linda and Stephanie worked on cases, in which they were given the entire contents of a person’s smartphone, from text messages to pictures saved on Pinterest. This came on top of other digital evidence, such as surveillance footage and recordings of prison phone calls, as well as traditional evidence, such as physical or testimonial evidence.

I qualify this data deluge as information overload: the experience of being confronted with more data than human attention can effectively cope with and process (Liang & Fu, 2017; Qihao, Sypher, & Ha, 2014). The evidence turned over to the defense by the prosecution during discovery was the primary source of this information overload. Discovery refers to the process whereby the defense receives the evidence the prosecution has gathered about the defendant’s case during its equivalent to the defense’s acquisition phase (Weiss, 2005; Wice, 2005). Most of the content given to the public defenders as part of discovery was not relevant to the case; that is the cause of the information overload for public defenders.

The reason for the information overload (of mostly irrelevant content) can be traced back to two problems with digital evidence in criminal case processing: First, the search warrants that judges issued for digital evidence were commonly overbroad, which means they authorized the seizure of all possible evidence on a device or social media account, with no scope limitations (Denney, 2018; Gershowitz, 2016). As a result, the prosecution was often granted full access to hard drives, Facebook accounts, and smartphones. This led to the prosecution having an extensive case on the defendant, filled with all sorts of digital evidence. Second, prosecutors shared discovery before they had decided what part of the mountain of data they had collected they would formally introduce as evidence at trial. In the end, the prosecution may decide to formally introduce only a couple of Facebook photos as evidence, but, at the time they shared discovery with the defense, they had not yet made that determination. This resulted in thousands of documents and metadata files being handed over to the defense with no clear indication about what was relevant to the case. Despite complaining about being swarmed with data, most defenders I spoke with believed the early sharing of discovery was a good faith effort on the part of the prosecution, because discovery laws in the state allowed prosecutors to withhold such information until shortly before trial (Lieberman & Kirshner, 2019; Schwartzapfel, 2019).

However, this action flooded the already overworked public defenders at the Northeastern Defender Association with a deluge of miscellaneous data. Because discovery was about evidence the prosecution proposed to use against the defendant, even if only a small subset of the evidence was eventually selected for presentation at trial, once discovery was in their possession, defense attorneys felt compelled to at least skim the evidence. Waiting until the DA’s office had narrowed down the evidence was perceived by defense attorneys as too risky a move, especially if the case involved serious charges with a potentially long jail sentence. Consequently, the defenders ended up scouring endless pages of Facebook content or listening to extensive, prison phone conversations just to get a head start and begin building their defense strategy around what the prosecution *might* introduce as evidence down the road. It is important to keep the labor conditions of public criminal defense attorneys in mind here; public defenders possess few resources and are already burdened with high caseloads (Weiss, 2005). The information overload they experienced in relation to digital evidence was stacked on top of these existing struggles of public service work.

Reflecting on the painstaking task of listening to hours and hours of prison phone conversations, Mark noted, “So much of the time it’s […] irrelevant to the case, and you have to slog through […] hours of conversations that are mind numbing and have nothing to do with the case. But you gotta listen because if the DA wants to use them [you have to know].” Stephen, another defense attorney shared this attitude. He felt that it was his responsibility to know what was in the files shared during discovery by the prosecution. When possible, Stephen pressed the DA’s office on what they planned to use, so that he could focus the task, but, in the end, there was often no alternative to simply going through the files. “Even if it takes you 70 hours. [You]’ll get through all of it. Because you cannot have a moment in the trial where they pull page 998 and you have an ‘oh shoot moment,’ ‘cause then that’s your fault. You had that -- you had that document and you didn’t find it,” he said. Despite being overwhelmed by the amount of information and the irrelevance of most of it to the case, defense attorneys felt compelled to examine the data to give their clients the best possible representation. Many believed that pushing through hundreds or even thousands of pages of digital evidence was part of a strong defense and the best way to avoid an upset later in the case.

Triage. To manage this information overload, the attorneys at the Northeastern Defender Association developed triage systems. Individual work practices included: looking first for evidence that might help, doing keyword searches for possible admissions or other anticipated pieces of damning evidence, and prioritizing data from near the time of the incident. In the next paragraphs I review these triage systems in more detail.

Mark was an experienced trial attorney and admired by many of his colleagues. His process for sifting through large amounts of data was to first look through the evidence for anything that could help the case. Information that placed his client away from the crime scene and occupied with an activity, preferably one witnessed by other people, would be a good start, he explained. Then, once he had exhausted that path, he started searching for evidence that could hurt the case. This process involved critically examining the information by asking himself how the prosecution might use it to support the charges against his client. “You’re playing defense,” he said, “you’re looking for what’s out there that could hurt the case.” To that end, Mark would skim the documents for possible admissions and damaging interactions. In the gang cases he handled, that meant looking for conversations about drug or firearm dealings. Any statement in which his client acknowledged the crime, whether it was bragging about a shooting on Twitter or arranging the sale of a firearm via Facebook messenger, would be considered an admission. Then, depending on how damning the overall evidence was, Mark started preparing for either a trial or a plea hearing.

Other attorneys in the office took a similar approach. When I met with Erin, she said that starting the skimming process by looking for things that might help was a good tactic.

Sometimes however, there was a unique concern to a case, and, in those instances, Erin investigated that issue first. For example, in a recent drug case with ample social media and text message evidence, Erin was particularly worried about mentions of Oxycodone, the drug her client was charged with selling illegally. “So, I got a list online of all the street names and slang terms for Oxy, and I control F’d the document for that first,” she said. Her initial search process focused on evaluating how much the DA knew about her client’s drug dealings based on the digital evidence recovered. For Erin, written admissions, such as text messages about arranging drug sales, would be highly damning. Before making defense strategy plans, she needed to get a sense of how much hurtful information the prosecution had acquired. After locating multiple social media and text message admissions, she realized she’d be preparing for a plea hearing rather than a trial. There was just too much damning evidence in the documents she’d received. The triage process had allowed Erin to make an informed decision about how to move forward with the case. At this point, her strategy shifted to examining the context around the admissions to see if there was a way to “spin” the narrative in her client’s favor.

Linda had an approach similar to Erin’s in that she also prioritized searching for information related to the crime. Because an entire phone’s worth of communications was an enormous amount of data, Linda typically started by looking at what happened near the time of the incident and then turned her attention to any communications between her client and the other parties involved in the alleged crime. However, Linda recognized that she couldn’t merely stop there. “That’s the easy first step,” she said. “We still need to [know] if there is something terrible from way before. The DA may still find it and use it, so we need to know and be prepared as well.” Although the timeframe of the incident was short and therefore more manageable from a data analysis perspective, defenders found it too risky to look only at interactions from that period. Instead, they operated on the timeline of the device or social media account they were given, which covered a much wider timespan. To help with such preparations, attorneys solicited assistance from others in the office. Another attorney, Stephanie, noted that, as part of the triage process, she handed over pages to law student interns so they could sort through the data, separate the good from the bad, and highlight content that could be valuable to the case. This team effort allowed defense attorneys to share the burden of sifting through large amounts of data and gave them another set of eyes on the case.

If the evidence came from the public defender's side, defense attorneys at the Northeastern Defender Association could rely on their digital forensics lab to narrow the data, by, for example, including in the final report only text messages from a particular timeframe. But, when the evidence came from the prosecution, skimming through all of it was often the only option. Thinking back to how her work habits have changed since the rise of digital evidence, Rebecca said, "The job has become much more difficult because we'll just get thousands… and the phone pictures, I mean our client's music, everything. All their social media. Every website they've looked up." It was tiring and overwhelming. In response to the growth of digital evidence in criminal case processing, the attorneys at the Northeastern Defender Association developed triage strategies. Prioritizing data from around the time of the incident, looking for evidence that might help, and searching for possible admissions or other anticipated pieces of damning evidence were some of the ways attorneys sorted through the heaps of data they received from the prosecutor's office. These approaches were not entirely novel; public criminal defenders have always been short on time because of stacked caseloads (Farole & Langton, 2010; Wice, 2005). To manage, they prioritize cases in highest need of attention, typically, those in which clients face potentially long prison sentences. Mark's, Erin's, Stephanie's, and Linda's stories illustrate, however, that in the digital turn there is a triage within triage. To deal with information overload, attorneys were not only prioritizing one case over another, they were also making decisions about what to prioritize at the individual case level – focusing first, for example, on information from near the time of the incident to make the data deluge manageable.

This new level of triage raises questions about the role of technology literacy in public criminal case processing, and whether attorneys who are less adept at filtering reports and other digital files might be at a disadvantage when it comes to preparing defense strategies. Erin's decision to search for mentions of Oxycodone was a creative way to quickly assess the damage-level of the evidence file she'd received, but not all attorneys at the Northeastern Defense Association felt comfortable enough to handle digital evidence on their own. Skimming through large amounts of data to get ahead works only if the attorneys are capable of making sense of the evidence in the first place. In the next section, I discuss the varying levels of technology literacy I observed at the office and how defense attorneys approached seeking help with the digital components of their cases.

Learning curve. As I talked with defense attorneys about how they approached digital evidence in their cases, I realized that the technology literacy of public defenders varied greatly. Older attorneys admitted that they struggled more than their younger counterparts. Attorneys who felt comfortable with their triage techniques typically worked independently, whereas those who struggled were dependent on the support of the digital forensics lab. When defenders felt unprepared, the analysts acted as mediators between the attorneys and the digital evidence and helped attorneys learn how to navigate and interpret such pieces of evidence as cell phone extraction reports of maps of cell site analyses. A common theme among all defenders, both those who were skilled in technology literacy and those who were not, was a sense that their schooling had not prepared them for the realities of working with digital evidence. Many had successfully picked up the needed skills on-the-job, but others still felt inadequate.

Some attorneys at the Northeastern Defender Association were very proactive about learning basic, digital evidence, preservation techniques; I met approximately a dozen who were capable of downloading a copy of someone's Facebook information or who knew how to save a video that had been posted online. When I was sitting in the lab with the analysts, I occasionally observed that attorneys walked in for a brief check-in, because they wanted to make sure they had downloaded a Facebook video correctly. Other attorneys however, relied heavily on the digital forensic analysts for support with all aspects of their case, from making sense of phone extraction reports to reading call detail records (CDRs). Cell site analysis was especially tricky for attorneys to understand. During my fieldwork, I noted at least two separate instances in which the analysts guided an attorney through the interpretation of the cell site locations map they had created for the case. "If you have digital evidence that could be exculpatory, you better hope your lawyer knows how to use it or how to get the right people on the case," Kelly said to me, exasperated, after she had just spent the better part of an hour trying to teach an attorney how to read a cell site analysis map over the phone. Working with digital evidence was a challenging, confusing task for many defense attorneys in the office.

Even attorneys in their late twenties and early thirties, who had grown up with smartphones and social media, needed help interpreting the format of certain, digital files. When Erin started working on the drug case for which she had an entire iCloud's worth of data, she quickly realized she needed the lab's assistance. "They helped me understand how to read the giant, massive amount of data that came from iCloud; it was really useful. Because it's not that obvious how everything is organized and like, when you're reading a text message backed up on iCloud, like… Who's it from? And who's it to? [Was] it deleted? And when it was deleted? And all of that," she said. The analysts helped her sort through the data and narrow down communications that seemed relevant to the case. Erin had received the file from the prosecutor's office with no instructions. The analysts therefore also assisted Erin in understanding how to navigate the iCloud copy and what to make of the different menus and subcategories. Had she not had this support available from the Northeastern Defender Association, Erin would not have been as well prepared, and she might have missed evidence that would have helped her client or provided valuable context for the alleged crime.

It is important to remember that the lab was a novelty inside the office, having been created only recently in 2013. In the digital turn, it was altogether quite exceptional for public defenders to have access to this kind of in-house assistance. The vast majority of public defender offices must outsource such services, often at great cost, which means only the highest priority cases receive digital evidence support. Whenever I interviewed attorneys from the Northeastern Defender Association, many expressed their gratitude for finally having in-house support for the digital evidence needs of their cases. Even experienced attorneys who had been in the office for some time still felt overwhelmed and unsure about digital evidence and were thankful for the services the lab provided. Linda noted that learning to work cases with social media, location data, and other new media aspects had taken time. "It's a big learning curve," she said. "I don't use a lot of these things in my own life. I'm not someone who has like a great knack for it. It's time consuming and it's foreign to me to do, and no one teaches you in law school about sorting through digital evidence or thinking of creative ways to use it or fight it." Other public defenders also mentioned not learning about digital evidence in their schooling. Often it was something they had to pick up on the job or through Continuing Legal Education (CLE) programs, which were professional development courses specifically designed for attorneys. Given the prevalence of digital evidence in their cases, the lack of formal training in that area upset many public defenders. Reflecting on having to work with digital evidence, Linda noted, “It is something at this point that is absolutely a necessary part of our job, but it’s not the part of your job that anyone trains you on or prepares you for, so that’s a real challenge.” There was a gap between what attorneys had been trained to do in law school and the realities of being a public defender in the digital turn. The creation of the digital forensics lab inside the Northeastern Defender Association was meant to help remedy this problem, and in the analysis phase of the life cycle, the analysts played a crucial role in assisting attorneys who struggled with digital evidence.

The digital forensics lab helped defense attorneys learn how to use and fight against such data in their cases. Furthermore, once attorneys had used the digital forensics lab for assistance, they tended to come back for help whenever they received a new case with a digital evidence component. During my observations, I noticed that some attorneys had become habitual users of the lab. This showed that early intervention was important in getting attorneys to realize that their office provided support for such matters. In my time in the lab, the names of a handful of attorneys came up repeatedly in conversations with the analysts, because they had become frequent users of the lab’s services. A few attorneys had even developed close relationships with one analyst in particular and reached out to that person directly for advice on cases. I was therefore surprised when, during my interviews, some public defenders were hesitant to ask for assistance. During our interview, Heather said that there were times when she had been reluctant to turn to the lab. “I think maybe what's holding me back is knowing that there are only so many of them and […] so many of us,” she said, noting that there were only four digital forensic analysts and George to assist the various Northeastern Defender Association offices across the city. When Heather put it in those terms, I sympathized with her reasoning. She knew first-hand what it felt like to be overworked and didn't want to impose more work on others. George and the analysts, however, were determined to have more public defenders seek support from the lab. If needed, they would expand the lab, George said. To raise awareness about the types of assistance they provided, George and the analysts had begun doing monthly "road shows," travelling from office to office to inform attorneys about the capabilities of the lab and encourage them to reach out for help.

Digital Evidence and Attorney-Client Interactions

The analysis phase of the lifecycle did not stop with public defenders searching through countless pages of digital records or seeking support from the digital forensics lab. Attorney-client interactions also informed the process and shaped the analysis of digital evidence. In the second half of this chapter I examine how digital evidence factors into meetings between public defenders and their clients. But, before I delve into the details of attorney-client interactions during this stage of the lifecycle, I briefly describe the often-antagonistic context in which public defenders and their indigent clients interact.

Mistrust, fear, and doubt are feelings that have long characterized the relationship between public defenders and their indigent clients (Hara, 2009; Abbe Smith, 1995). Research shows that indigent defendants are concerned about the loyalties of their public defenders because, unlike private attorneys, court-appointed attorneys are not paid directly by their clients (Wice, 2005). Surveys of defendants served by public defenders found that only 20% felt their attorneys were on their side (Casper, 1972; Weiss, 2005). The worry that public defenders may be working with the prosecution and arranging unfair plea bargains to bring cases to a close more quickly is among the concerns that clients experience (Wice, 2005). In his study of a Chicago, public defender office, Davis (2007) explains that clients would insult public defenders by demanding “real lawyers,” or calling them “PDs,” which stands not just for public defenders, but also penitentiary dispatchers, and signals the idea that public defenders are conspiring together with the prosecution to send defendants to prison. There is also a general perception among defendants that public defenders easily give up on cases, and that they consider their clients as little more than another casefile on their desk. Davis (2007) argues that some critics of public defenders even maintain that “the job of the public defender is not to defend, but to sort through their defendants, categorize them according to the nature of their charges, and help the court dispose of the cases in a businesslike manner as quickly as possible” (p. 84). However, just as poor defendants are prejudiced against their attorneys, Weiss (2005) finds that public defenders also judge their clients; they moralize them and look down on their behavior as dangerous and self-destructive. This backdrop must be considered in the context of attorney-client interactions in the digital turn, where attorneys come into contact with increasingly personal information about their clients’ lives.

To examine how attorneys and clients interact during the analysis phase, I first look at how public defenders enlisted their clients’ help to better understand what certain pieces of digital evidence meant and where they fit in the larger context of the case. Second, I examine the use of digital evidence to confront clients about the facts of the case and highlight diverging defendant reactions to seeing such evidence. Lastly, I close the section by describing how the overload of data, most of which is highly personal and irrelevant to the case, can make attorneys uncomfortable and humanize clients at the same time.

Working together. Sometimes digital evidence, especially social media content created by youth, represented an interpretive challenge. The attorneys could look at the time stamp and the names of the correspondents to get a sense of when and with whom their client had been in communication, but they did not always understand the meaning of these communications. Mark, an attorney who had handled several, youth gang cases, recollected one instance in which he had desperately turned to his client for help in deciphering the language of various Facebook posts, "I was going to Rikers with 100s of pages and […] working through it like what did you mean here? What'd you do here? And sometimes it's like […] he's like an ambassador – an emissary from a completely different world explaining forms and different rights and different phrases and slogans and slang." Mark's client was a young, black man charged in a shooting incident, and the prosecution was planning to use social media evidence at trial. To prepare a defense strategy for the upcoming court date, Mark felt that sitting down with his client and assessing the evidence together was the best option. Although previous studies have shown that the relationship between attorneys and clients can be strained by the fact that both often come from different social spheres and use different idioms and cultural references (Kunen, 1983; Weiss, 2005), Mark did not let these differences hurt his relationship with his client. On the contrary, Mark recognized that he needed to be educated by his young, black client. He didn't rush to judgement or moralize. As he brought his client in as a cross-cultural consultant, they worked together to assess the evidence, its meaning, and its implications in the context of the case.

When I interviewed Stephanie in December 2017, she had recently wrapped up a domestic violence case that involved a lot of digital evidence from text messages and social media posts. Going through the data had been strenuous, and, even with the additional support of interns, Stephanie had not been able make sense of all that was happening in the conversations between her client and his former girlfriend - the complaining witness in the case. Like Mark, she too decided to ask her client for help in interpreting the communications. Discussing evidence with clients was a common aspect of case processing, Stephanie noted, but going over personal communications was much more intimate than sitting down together to watch a surveillance video. In the context of domestic violence cases, it required openly talking about the darkest moments in a person's life, including verbal arguments and threats of violence towards his/her partner. At first, Stephanie's client did not want to talk about the digital evidence of the case. He was distant and reluctant. Stephanie sensed he didn't feel comfortable confiding in her about his behavior towards his girlfriend. She had to pull out printed copies of the communications and nudge him. "I needed more from him. [I needed] to get a better sense of where this fit in with like a broader picture of what was going on with their relationship at that point and what she was saying to him." The text messages and social media posts were the digital traces of her client's interactions with his girlfriend, but a lot more had transpired between the two than could be deduced from the evidence alone. Convincing her client to be more forthcoming turned out to be an exercise in trust-building and interpersonal communication skills. She succeeding in getting him to disclose more details about the circumstances around the assault, but their attorney-client meetings were strained.

Working on this case opened Stephanie's eyes to the importance of having an honest, open relationship with clients. Digital evidence from text messages and social media posts, more than any other type of evidence, exposed attorneys to a client's most personal interactions. By communicating through mediated channels, Stephanie's client and his girlfriend had created a record of all their fights and disagreements, and those interactions were now at the heart of the case. To provide effective counsel in this context, public defenders had to re-consider their trust-building techniques and help clients recognize the mutual benefits of having honest conversations about personal, hurtful pieces of digital evidence. This was a task, which Stephanie found daunting. One of the realities of criminal defense work is that most defendants have committed the crime(s) with which they were charged (Feige, 2001; Weiss, 2005). Feige (2001) suggests that rather than address a client's participation in the event, public defenders should work first on getting to know their clients by building rapport with them. This can be accomplished by taking an interest in who clients are, learning about their families, living circumstances, and life struggles. Because digital evidence is so rich in personal information, it can give the false impression that this step can be skipped. Yet, as Stephanie's story shows, to critically talk about the facts of a case, attorneys have to gain their clients' trust to develop this type of cooperative effort.

Discussing digital evidence. The clients who came through the public defender office were rarely truthful, and many were uncooperative. Clients who are defensive towards or even doubtful about their court-appointed attorney are a longstanding issue in public criminal defense (Abbe Smith, 1995; Wice, 2005). In my fieldwork, I noticed public defenders who turned to digital evidence to back up their arguments to clients in a more convincing way to avoid being seen as pushing a client towards a deal for no good reason. They relied on digital evidence to confront their clients about the factual matters of the case and show that their reason for nudging them towards a plea was justified. Just like DNA testing was perceived as an objective scientific method, certain properties of digital evidence, such as time stamps and geolocation data were often seen as irrefutable (Casey, 2011; Pendleton, 2013). Public defenders relied on those qualities during attorney-client meetings to get defendants to recognize that denying the charges or pushing for a trial wasn't the best approach. Time stamps on a photograph, cell tower information from CDRs, video footage, etc., are examples of the pieces of evidence attorneys used to move the case along persuasively. For example, in all her DWI cases, Heather made it a point to bring her clients to the office for a formal sit down so they could watch the footage of the client taking the breathalyzer test and doing the physical coordination assessments. Often the video showed the client clearly intoxicated, belligerent, and shouting at the police officers. According to Heather, watching the video together was more persuasive than any verbal argument she could have made on her own. In reference to one client, she said, “After he saw the video, he was like, ‘I think we’ll probably have to take a plea.’” There was something about the objectivity of the video that made clients realize the severity of the charge, she explained. Other attorneys also used this method to help clients have more realistic expectations about trial chances or plea-bargaining options.

In May 2018, I was talking with Erin about her encounters with digital evidence, when the conversation turned to how she made use of such data during client meetings. Recently, she had worked on a drug case with a great deal of digital evidence. Eventually, the amount of hurtful evidence became so overwhelming that she no longer believed in a successful trial outcome. She had to sit down with her client and have a heart-to-heart conversation about how to proceed. To help plead her case, Erin brought the digital evidence to the meeting, “Listen, there’s all this stuff in here. I don’t think we can win this trial,” she said to her client. Luckily, he agreed, and Erin was able to move the conversation away from trial preparations and towards plea options. The revealing of the digital evidence is what tipped the scale in favor of the plea, she thought. Like Heather, Erin believed that when clients saw the evidence firsthand, something “clicked,” and they became more attuned to the realities of their predicament.

Not all attorneys at the Northeastern Defender Association however, had positive experiences when using digital evidence in client meetings. Some defendants, no matter how convincing the evidence, refused to consider plea agreements, and still others became angry when confronted with evidence that tied them to the crime. Despite attempts at honest, upfront discussions, there were times when public defenders found themselves unable to use the persuasive appeal of digital evidence to reason with their clients.

On an early morning in November 2017, I was sitting in the digital forensics lab with Kelly and George, when Maggie walked into the office. She was scheduled to meet with a client later and needed the lab's help in preparing still shots from a surveillance video which showed her client walking around midtown with a meat cleaver and then attacking the off-duty police officer who tackled him to the ground. "He keeps denying the attack on the officer," she said. Her client kept repeating that he had dropped the knife, but the surveillance video showed him with the meat cleaver in hand. Maggie believed that if she brought screenshots to the meeting, she would be in a better position to reason with her client. Her hope was that once he saw the video and screenshots, he would be more cooperative, but her efforts proved fruitless. The case ended up going to trial, and Maggie's client was convicted on all counts brought against him. He was sentenced to twenty years in prison.

In a harassment case, after receiving a CD-ROM full of emails which confirmed her client had sent naked pictures of his girlfriend to her employer, Heather encouraged the defendant to consider a plea deal using the damning evidence to support her argument. "I confronted him with that, and I said, this is what they're going to use against you at trial and this is what a jury is going to see. […] And I believe that, given today's political climate, if we went to trial, I think we would lose," she said. Heather felt the evidence against her client was convincing and that the odds of winning at trial were slim. The emails identified her client by name, context, and language style. There was no doubt in Heather's mind that he had sent the email to his girlfriend's employer. Furthermore, the deal offered by the DA was fair, she explained, because it would have left her client without a record. Her client however, refused to compromise and even hung up on Heather during one of their phone calls. By the time I exited the field, Heather's client still hadn't taken a deal, and the plan was to move forward with a trial.

Yet another attorney, Stephen, noted that when clients were confronted with their social media content, many became defensive. Seeing their personal pictures, posts, and messages come into contact with the criminal justice system made them feel violated and exposed. To understand why defendants were angry at seeing their personal histories laid bare in the criminal justice system, one needs to view this exposure in the context of other violations poor people experience. For example, to get access to government services and welfare programs, poor defendants have to submit themselves to various, privacy violations, from unannounced home visits to the tracking of their spending habits (Alexander, 2012; Wacquant, 2001). Having prosecutors and defense attorneys dig into their social media pages and smartphones adds yet another level of violation. In the digital turn, even personal communications aren't excused from the prying eyes of the government.

Openly discussing these instances of the judicial system entering defendants' personal lives led to uncomfortable meetings. If the contents were relevant to the crime itself (messages showing the sale of a firearm, for example), Stephen was generally able to get his clients to recognize the risks of going to trial with such damning evidence in the hands of the prosecution. However, if the digital evidence were only peripheral to the case and made a moral claim about the defendant's lifestyle or online self-presentation, clients became upset. "If it's just an insinuation, almost every time the person gets defensive," he said. Stephen explained that his clients felt the prosecution was purposefully trying to make them look violent or dangerous by selecting pictures of them throwing hand gestures or posing with friends in the streets. And generally, Stephen agreed that the prosecution was moralizing and being highly discriminatory. Stephen said that his clients attempted to contextualize the evidence by saying, “Come on, it’s just me and my friends, right? Those aren’t gang signs […] I grew up with these guys.” I sensed that Stephen sympathized with his clients’ struggles to defend their online images. He brought up the social media evidence not to personally judge his clients, but to make them aware that the prosecution had this information too, and that, from a defense perspective, they needed to be prepared for it to come up during trial. It was part of Stephen’s process of working on the case, of preparing a counternarrative to what the prosecution would say about the client. Yet, this act of sharing what the prosecution knew often resulted in his clients feeling anger towards him as well. For Stephen, having these conversations with his poor, black clients was a difficult process. It required talking about the criminal justice system’s reliance on stereotyping black defendants as dangerous criminals and acknowledging his own limitations as a defense attorney to fight back against such prejudicial evidence.

Shifting professional boundaries. Previously, I established that the digital turn in criminal case processing was characterized by information overload. Approximately one-third of the attorneys I interviewed expressed feeling uneasy not only about the amount of digital evidence they received, but also the highly personal nature of the evidence. For some attorneys, this discomfort came from the general access to all the information on a person’s phone, for others, the discomfort was tied to a particular type of content such as explicit photos of their clients or written arguments between a couple. Here, I found that attorneys often engaged in moralizing. Without outright condemning their clients for having nude pictures on their phone or attacking their girlfriend in text messages, they acknowledged that such behaviors were of poor taste and had a negative impact on how they viewed their clients.

Stephanie, who worked on domestic violence cases, recalled feeling uncomfortable when reading through social media arguments between couples. The text messages male defendants sent to their girlfriends could be "really awful," she said, and it took a conscious effort on her end to not judge her clients based on the harsh things she had read. Ann, too, experienced discomfort when examining certain pieces of digital evidence and compared the act of looking at the details of a phone extraction report to voyeurism. "You could piece together somebody's entire life minute-to-minute once you have their phone […] It feels like a real intrusion on somebody's privacy to have that much access to their life," she said. Another attorney, Linda, noted that to limit her discomfort, she tried not to dwell on personal information and to only skim over content that was unlikely to have any bearing on the case. "The communication an individual has with their mom, unless it's criminal in any way and related to the case, I'd rather not be a part of it and not have it be part of my relationship with my client," she said. The ease with which social media content and text messages could be acquired meant that attorneys were now often confronted with the private lives of their clients. Sometimes, taking a deep dive into a client's life was necessary for making sense of the circumstances of a case. This was certainly true for domestic violence and harassment cases, in which understanding the history between the two parties was crucial to situating the incident within the context of a previous relationship. At other times, however, the presence of personal information felt like an unnecessary intrusion by the judicial system. Public defenders spoke of having to redraw professional boundaries to keep irrelevant details about their clients' lives out of their minds and out of the case.

Of all the personal content to which attorneys were exposed, one stood out as particularly uncomfortable: explicit nude pictures and videos. This issue was brought up by female attorneys in connection with male clients. Three of the female attorneys I interviewed described sexual content as the main thing they wish they didn't have to see as part of their work. Linda said, "We get cases where a lot of images of a client's genitals are turned over to us, and you're like, 'Dude, they're from the DA, and I had to look through them, and, by the way, do that less." Linda had been with the Northeastern Defender Association for almost a decade when I met her, and although she found such pictures uncomfortable, she had learned to brush them aside. Occasionally, she had to bring up the pictures during attorney-client meetings; in those situations, Linda's process was to keep the conversation focused on the case and to discuss explicit content only as it related to the charges brought against her client.

Not all defense attorneys, however, were able to distance themselves so easily from the sexually explicit images of their clients. Reflecting on the challenge of dealing with such content, Erin noted, "I really like him, and he's a really nice kid, but I've literally seen him having anal sex. […] It certainly impacts my view of him that I know he cheats on his girlfriend all the time, you know what I mean, it's hard not to, does it matter? Not really, I'm not like his teacher or his friend, I'm his lawyer, but yeah, I think it does." Conversations with clients after having seen such personal photos and videos were awkward, because there were certain things that Erin could simply not disassociate from her client. She seemed aware that she was moralizing and judging her client because of what the digital evidence had revealed. Though she tried to not let it affect her work, she recognized that there had been a shift in how she perceived her client.

Being confronted with a client's personal information could also have the opposite effect and actually bring defenders and clients closer together. Heather too, had worked on cases where she had seen very explicit images of her clients. When I spoke with her in September 2018, she had recently wrapped up a case involving a BDSM community where her client had been part of consensual sex parties that included sexual practices like asphyxiation and bondage. Working on that case had involved going through a lot of explicit material. “That was my first sex case […] beyond like a butt grab on the subway,” she said. Heather explained this case taught her a lot about how to deal with her own discomfort and how to maintain professional boundaries with clients. Surprisingly, in the end, even though the content she examined had been disturbing, she felt it brought her closer to her client. “He knew what I was getting access to,” she said. “I think in a lot of ways, you know, it made for a trusting relationship where he knew that I had everything under control, that it was nicely organized.” In fact, Heather’s professionalism and kindness on the case had struck her client so much, that when he was arrested again a month later on different charges, Heather was the first person he called from prison. There was something about the intimacy of the case, she said, which, although uncomfortable, also helped her establish a very honest relationship with her client.

Heather wasn’t the only attorney to feel there were benefits to the added information to which defense attorneys had access in the digital turn. Jack, who specialized in child custody cases and worked in one of the satellite offices, noted that he now saw facets of his clients’ lives he had never before seen, including happy moments when his clients posed with friends and family members. As a public defender whose work often involved guiding young, struggling fathers through the challenges of custody visitation, seeing their social media posts helped him see another side to his clients. “The social media posts will have pictures of your client with a child. […] You’re sort of always hearing about this child, but you don’t know what they look like because they don’t come into court, and you don’t really know what your client’s relationship is like with them, so sometimes it’s interesting to see pictures of them with their children. […] You get definitely more of a window into your client that way.” Child custody and visitation cases also included other evidence, such as reports from case supervisors, but Jack noted that in recent years, his clients had increasingly volunteered their social media posts as additional documentation. The vast majority of custody visitation cases are settled outside of court, and digital evidence played a role in negotiations. Sharing social media content was his clients’ way of proving that they were, in fact, involved in the lives of their children.

Jack also noted that seeing this personal side of his clients’ lives motivated his work as a defense attorney, “I tend to think I’m a zealous advocate regardless of whether I saw a picture of my client with their child but certainly it humanizes [them], and I think it’s powerful to see your client being affectionate with their child; it definitely makes it more personal.” The presence of digital evidence helped public defenders look beyond the charges and see a different, more human side of their clients. For Jack, it meant an opportunity to see defendants as loving, caring fathers. In the United States, public defenders are notoriously overworked; they handle multiple cases simultaneously and rarely have time for long sit down with individual clients (Weiss, 2005). Such work conditions don’t give public defenders many opportunities to get to know their clients on a more personal level. The experiences of Heather and Jack suggest that social media evidence may have the potential to intervene in the current system by humanizing clients in the eyes of public defenders and, in turn, make their relationship more amicable.

The Analysis Phase: Discussion

In this chapter, I examined two intertwined aspects of the analysis phase of the lifecycle: information overload and attorney-client interactions. I found that the analysis stage brings attorneys into further contact with the personal aspects of defendants’ lives, intensifying the coming together of the personal and the judicial that characterizes the digital turn in criminal case processing. This increased access to defendants' lives and personal information in the judicial system happens in two ways in the analysis phase: 1) during the individual work practices of attorneys as they sift through vast amounts of digital evidence to make sense of the case, and 2) during attorney-client interactions, when defense attorneys discuss personal communications, photos, and other pieces of digital evidence in meetings with clients.

When discussing the implications of the digital turn for the individual work practices of public defenders, it is important to consider the labor conditions of such attorneys. Unlike private defense attorneys, public defenders have few resources and carry high caseloads (Weiss, 2005). The information overload experienced by the attorneys at the Northeastern Defender Association was stacked on top of these existing public service struggles. Devising triage mechanisms to make data more manageable was not a new concept for the defense attorneys. They have always been prioritizing cases in highest need of attention (Wice, 2005). What stood out about the triage practices of the digital turn, however, is that they involved a type of triage within triage. Attorneys were not only prioritizing one case over another, they were making decisions about what to prioritize at the case level. They were focusing, for example, on information from the time of the incident and sidelining the rest to keep the amount of data manageable. Attorneys recognized that it wasn't humanly feasible to examine thoroughly the entirety of the evidence (Liang & Fu, 2017; Qihao et al., 2014). Engaging in such triage methods required technology literacy and creativity, and I found that not all attorneys were equally prepared for this task.

Again, the context of public defense matters for these work-related challenges and their implications for the representation of indigent defendants. One of the flaws of the adversarial process of the American justice system is that it assumes the prosecution and defense operate on level playing fields, when, in reality, the prosecution has numerous advantages over public defenders (Farole & Langton, 2010; Wice, 2005). Prosecutors, Wice (2005) argues, tend to be better paid, more experienced, and backed by a more extensive support staff. They also have the discretionary power to choose which cases they want to pursue, which means they can decide to discard cases that would be difficult to win. On the other hand, public defenders "must defend any indigent client the prosecution attempts to convict" (Wice, 2005, p. xi). The public defenders at the Northeastern Defender Association benefited from a unique in-house support to which most public defenders do not have access. The digital forensics lab provided crucial support and helped struggling attorneys make sense of digital evidence. But many defenders still felt unprepared to handle cases with digital evidence. This uncertainty attorneys experienced concerning digital evidence raises questions about their ability effectively to use and argue against such evidence as part of their defense. The analysis phase is the stage at which defense attorneys assemble the building blocks of the story they'll tell about their client and the circumstances of the alleged crime. If public defenders aren't able to make sense of digital evidence or develop triage mechanisms to manage the discovery they receive from prosecutors, then their storytelling capacities in the digital turn are hampered. They risk missing out on opportunities to create more nuanced narratives for their clients.

I found that technology literacy varied greatly among defenders and that there was a gap between what attorneys were taught in law school and the realities of being a defense attorney in the digital turn. Attorneys felt they hadn't been prepared for how to examine and use digital evidence as part of processing a case. Of their own volition, some attorneys sought help from the digital forensics lab and worked towards improving their technology literacy. I also noticed that once attorneys had used the lab, they were more likely to seek assistance on future cases. This suggests that early intervention and in-house support are key to leveling the playing field between prosecutors and public defenders. Digital evidence analysis is a demanding activity that calls for better resources, both in terms of staff support and available educational opportunities. State or local learning programs could be implemented to bridge this gap. The Northeastern Defender Association recognized the benefits of having its own digital forensics lab. In fact, the lab at the main office had proven so valuable that, when I exited the field in late 2018, there were talks of opening a second lab in one of the other offices. During the writing of this manuscript, I learned from George that a new lab would open at the northern satellite office in July 2019 to accommodate the growing needs for assistance with digital evidence.

Primarily, I found the attorneys of the Northeastern Defender Association to be fervent defenders who cared about giving their clients the best representation possible. The digital turn brought interpretive and sense-making challenges, yet rather than rush to judgement in the face of social media posts and text messages that they did not fully understand, attorneys involved their clients in the analysis process by asking them for input on meaning and context. Defenders and defendants became collaborators who teased out nuances and discussed their implications in relation to the case. Such efforts ran counter to the stereotype of public defenders who easily give up on a case and push clients to take any deal the prosecution puts on the table (Davis, 2007). Meeting with clients to engage in collaborative efforts was time-consuming and often required a trip to corrections facilities. But the defenders felt the input they received from their clients was worth the trouble, because it helped them get a stronger grasp of the evidence and prepare what they believed was a more effective defense. In some ways, although these meetings were driven by a personal necessity on the part of the attorneys to better understand the circumstances of the case, these interactions were also a chance for defendants to set the record straight and reclaim ownership of their narrative. In other words, working together during the analysis phase was a way for attorneys to give their client's voice a chance to be heard and included in the defense of the case (Fajans & Falk, 2009).

My findings also show that the easiest pieces of evidence for attorneys to discuss with clients were the ones that seemed self-evident and persuasively tied the defendant to a crime. In those instances, attorneys counted on the evidence speaking for itself. Heather's practice of sitting down with clients to watch their DWI arrest video comes to mind as one such example. By inviting defendants to watch the video, Heather put them in a detached, outsider's perspective. In a way, defendants were forced to look at the evidence objectively and evaluate what conclusions an average viewer might draw. This technique was also a way for attorneys to legitimize their recommendations to take a plea. Through digital evidence, attorneys brought clients into their perspective of the defense narrative and suggested that, logically, the building blocks of the story could be assembled only one way. In the context of the often-strained attorney-client interactions, this represented an opportunity for defenders to demonstrate that they weren't just trying to bring the case to a close or send the client to prison (Wice, 2005). Pointing to the evidence as the reason for taking a plea humanized defense attorneys; they had merely followed the evidence, just like the defendant was now invited to do.

On the flip side, digital evidence from social media and personal communications that was more nuanced and open to interpretation tended to put a bigger strain on attorney/client interactions. Such pieces of evidence often made defendants realize just how much information their attorneys had in the digital turn. This realization led to feelings of discomfort and sometimes even anger, which seeped through during meetings. Here the antagonism towards public defenders didn't come from the belief that they wouldn't fight for them (Davis, 2007;

Hara, 2009), but from a broader frustration at having one's personal life exposed in the judicial context and having that information re-interpreted into the context of the crime.

Clients weren't the only ones who experienced dissatisfaction at seeing personal information enter the judicial system on such a level. Attorneys found themselves overwhelmed with data that were irrelevant to the case, yet highly sensitive and personal. This led to feelings of discomfort and unease. Like doctors and nurses who have to redraw professional boundaries after the sharing of unpromoted information by patients, I found that defense attorneys had to focus on putting aside moralizing judgements after seeing explicit pictures or violent conversations (Petronio & Sargent, 2011). However, not all access to personal information led necessarily to discomfort for either clients or attorneys. Instead, I found that certain types of personal information humanized defendants in the eyes of attorneys. Seeing family pictures, for instance, was an opportunity see a client as a father or boyfriend instead of as a suspected criminal. Such personal data gave attorneys insights into the everyday lives of their clients, which they would otherwise not see. Various public defender organizations across the country have been advocating for more personal approaches to the processing of cases using the argument that, "fostering a personal relationship was integral to humanizing and restoring dignity to clients in a system that constantly dehumanizes them" (Luo, 2019). Perhaps digital evidence should be included in these discussions, as one possible avenue through which attorneys can foster a deeper relationship with their clients. Social media evidence could be a starting point for in-person conversations that allow public defenders to build a trusting rapport with their clients. This "humanizing" process could also go the other way. After realizing that attorneys have a genuine interest in their lives, defendants, in return, also learn to see the human side of the public defender and not merely the person paid by the state to represent them.

The analysis phase of the life cycle was about sorting and re-organizing pieces of evidence into a coherent, defense narrative. This chapter illustrated the information overload and technology literacy challenges public defenders faced in the digital turn. It also showed how digital evidence could be used to different effects during attorney-client meetings, from confronting clients about the facts of a case to working with them to make sense of the evidence. Lastly, this chapter showed that public defenders experienced shifting professional boundaries due to the increasing personal content of digital evidence. In some instances, access to personal information led to more intimate, humanizing moments, and in others, it led to discomfort and strained interactions.

Chapter 6: The Application Phase

The application phase is the last phase of the life cycle. In this stage, the defense applies the pieces of digital evidence acquired and analyzed in the previous phases toward a legal development in the case, such as during hearings, negotiations, or trials. This is also the stage at which the defense responds to or challenges the application of digital evidence by the prosecution. Defense attorneys work mostly independently in this phase. Intermediary role specialists, such as digital forensic analysts or investigators, occasionally come into play at trial when asked to testify about their assistance in procuring or examining digital evidence.

At this stage of the life cycle, public defenders and prosecutors present their competing narratives of the alleged crime by drawing on digital evidence, which comes increasingly from defendants' personal communications and social media interactions. I find that, although there were certain objective, damning types of digital evidence that were recognized as such by both the prosecution and the defense, most of the time, defenders and prosecutors worked with gray digital evidence that was open to different interpretations. Here, both sides formulated opposing moral arguments about the defendant: the prosecution drew on preexisting stereotypes of criminals, and the defense challenged those assumptions by pointing to socially desirable behaviors in the defendant, such as good school attendance.

I have divided this chapter into two thematic sections. The first half of the chapter examines how the prosecution uses digital evidence against defendants. This section first looks at how objective types of digital evidence are used to place defendants at the location of the crime, to identify a defendant visually as the person committing the crime, and to infer admissions of criminal activity. Then I examine the ways gray digital evidence is used to make damaging moral arguments about defendants to help bring down a case. I close this first half of the chapter by looking at how public defenders have fought back against such damning applications of digital evidence. The second half of the chapter looks at how public defenders have successfully used digital evidence to help their clients. I break down this second half according to case outcomes, examining how public defenders have used digital evidence to have cases dismissed, to win acquittals in the courtroom, and to negotiate better deals during hearings. Finally, I conclude the chapter by situating my findings within larger concerns about social inequality and discrimination in the criminal justice system.

The Many Ways Digital Evidence Kills Cases

When I explained to public defenders in the office that I was there to study digital evidence, the initial reaction of many was a long sigh, followed quickly by a comment about how digital evidence "killed" their cases. To understand why digital evidence was seen by many attorneys as a damning force, it is important to understand the circumstances around which such incriminating evidence appeared in cases. The clients who came through the Northeastern Defender Association would claim that they hadn't committed a crime - they were innocent of the charges brought against them. Experienced public defenders tended to be more skeptical of such claims than those who had been on the job for only a year or two; but in both instances, once a case was theirs, public defenders worked to prepare what they considered the best possible defense for their clients based on the currently available facts.

Later, as part of discovery – the process by which the prosecution shared what it had collected on the defendant – defense attorneys received a copy of a phone extraction report, a Facebook photo, or some other piece of digital evidence that linked their clients directly to the charges. The implications of the reveal were clear: the client had lied about being wrongfully charged, the digital evidence supported his/her involvement in the crime, and there was little defense attorneys could do to mitigate the situation. In those instances, the introduction of digital evidence was described by defense attorneys as “killing their cases,” because it signified the end of whatever leverage they had over the prosecution’s case. “It went from a case that we had a very good chance at winning at trial to ‘He needs to take a plea,’” said public defender, Erin, after the prosecution announced it planned to use an entire iCloud back-up worth of evidence that showed her client’s participation in illicit drug sales. For Erin, being faced with such damning evidence had signaled a finality; the case was no longer winnable. I found that evidence that “killed” cases was recognized by both the defense and the prosecution as objective, persuasive evidence. This type of evidence often included time stamps and metadata, which tied the defendant to the alleged crime (Brunty, 2016). This separated it from more nuanced digital evidence, such as records of a verbal argument, which were open to interpretation and lent themselves to divergent legal narratives. I noticed that when defense attorneys spoke about digital evidence as “killing” their cases, this “death” happened three ways: 1) by placing the defendant at the location of the crime; 2) by visually identifying the defendant as the person who had committed the crime; and 3) by offering an admission on the part of the defendant that confirmed his involvement in the crime. In the next paragraphs, I will describe each one of these three themes by taking a closer look at some of the cases that came through the Northeastern Defender Association’s office.

Location. In April 2018, I interviewed Linda, one of the public defenders in the office, about the different ways in which the prosecution used digital evidence against defendants. Linda noted that she had seen an increase in cases that use location-based data to show that a defendant was at the location of the crime. Recently, Linda had defended a client involved in a home robbery in which this had been the main piece of digital evidence. To demonstrate her client’s guilt, the prosecution used cell tower information that placed him at the location of the robbery. But, to argue that he was planning to sell the stolen goods, and to finish the "kill," they also used the defendant's smartphone Internet browsing history to show that he had searched for pawnshops in the area shortly after the robbery. That he had searched for pawnshops, the prosecution argued, further supported their argument about the defendant's involvement in the robbery. "That was significant evidence against him both because it place[d] him in the area, and also because it would be quite a coincidence if he just happened to be searching for a pawnshop right after this robbery occurred," Linda said. The evidence was convincing, and Linda felt there wasn't much she could do for her client. If her client had been regularly searching for pawnshops, then perhaps she could have made the argument that this behavior wasn't unusual for him, that it was part of a pattern, but that wasn't true in this case. There was no way for her to flip the narrative in her client's favor, she explained.

As part of her work on the case, Linda had looked at the report of her client's phone extractions text message exchanges. She had deduced that he was struggling with a drug problem. "There was nothing there that was going to help us, […] except [that] it also showed he was sort of a sad, drug-addicted kid. He wasn't like some master robber. Most of the communications were about needing drugs or needing money for drugs," she said. At best, Linda explained that she might be able to bring in the messages to argue for leniency at sentencing, but the digital evidence against her client was strong, and it was persuasive. Together, the location-based data and the browsing history had "killed" the case. Because of the nature of the evidence used against her client, Linda did not think this case lent itself to nuanced storytelling.

Visual identification. Another way in which digital evidence "killed cases" was by providing visual confirmation that the defendant was the person involved in the crime. Often this evidence came in the form of surveillance footage in which the defendant could visibly be identified. I observed numerous instances of public defenders asking the digital forensics lab to create stills from video surveillance footage in which their client could be seen shooting someone or fleeing from the scene of the crime. When showing the video to the analysts, attorneys often pointed out “their guy” and explained his involvement in the incident.

When surveillance footage was of poor quality, the prosecution attempted to cross reference it with another piece of evidence, such as a social media photograph, to make the case that the defendant was indeed the person seen in the surveillance footage. Julie, one of the public defenders in the office, experienced such a situation in one of her cases. The prosecution claimed that her client was the young man seen exiting the building on the surveillance video in an assault case. According to Julie, the video was taken from far away, and one could not clearly make out anyone’s face. However, Julie agreed that one could tell the person in the video was wearing a Yankees cap and khaki pants. The person also had the same build and height as her client. On his Facebook profile picture, Julie’s client could be seen wearing a Yankees cap like the one in the surveillance video. The prosecution, Julie explained, ended up issuing a search warrant for her client’s Facebook account to access additional photographs. Using the additional photos, which showed him wearing the Yankees hat and khaki pants, the prosecution was able to make the case that Julie’s client was, in fact, the man in the surveillance footage, and that was the moment Julie realized the case had become unwinnable. The social media pictures confirmed what was shown on the surveillance footage and together, these two pieces of evidence identified her client as the man involved in the assault. Social media content in this instance provided a new verification opportunity that prosecutors did not have before the digital turn (Brunty & Helenek, 2013), and showcases how defendants’ personal, everyday social media use finds its way into aspects of criminal case processing (Hoffmeister, 2014; Trottier, 2012). It is worth noting that in NYC, Yankee caps have a reputation for being worn by criminals (Fernandez, 2010). In using the Yankee cap connection, the prosecution relied on the stereotype of the "usual suspect" to justify the search of the defendant's Facebook account. Although the connection ended up being true in this case, relying on people's online self-presentations to infer criminal behavior is problematic as research has shown that young, black men, especially, tend to portray tougher personas on social media for purposes of posturing, without actually being involved in violent behavior offline (Lane, 2018; Patton et al., 2013).

Admissions. A third way in which digital evidence "killed cases" was through records that both defenders and prosecutors recognized as admissions of guilt. In September 2018, during my interview with Rebecca, another defense attorney in the office, the conversation turned to how drug cases are often difficult to defend because of text-message admissions of guilt. She explained that a common prosecution tactic is to have undercover police officers befriend suspected drug dealers and then follow the cell phone interactions between the two until they showed an established dealer-client relationship. Rebecca said the texts between the defendant and the undercover police officer, which often lasted several weeks and sometimes months, damned cases, because they proved "that there really was this interaction with the undercover [officer]. Sometimes […], what the undercover cop will do is make a first sale, or make a first buy, and then ask for more drugs, and let's meet again, and then more and more, and it ends up being so much weight in terms of drugs that it gets to be a more and more serious case."

To tie the defendant to the charges, the prosecution often used records from both parties involved in the exchange - the undercover police officer and the defendant. The prosecution acquired the contents of the defendant’s phone by requesting a search warrant from a judge to search the defendant’s phone. Once the phone was in the prosecution’s possession, the digital forensics team performed an extraction to save the text messages. I was surprised to hear that drug dealers openly discussed the sale of illicit substances through text messages, and I pushed Rebecca on the issue. Sometimes, the clients Rebecca represented spoke in code, but she described their code as “often very bad and very obvious.” According to Rebecca, the coded language employed by the clients didn’t disguise the nature of the communication; to show just how clear it was that the exchange was about drugs, she gave me the example of clients who asked, “Do you have the green?” or “Do you have CD's.” The text messages “killed these cases,” because the content of the messages was the equivalent of an admission. The texts showed intent and thus linked the defendant to the act of selling the drugs, which was then further corroborated by testimony of the undercover officer. The presence of texts in the case made it impossible for a defense attorney to raise doubts about the defendant’s participation in the drug sales. There was no option for a “he-didn’t-do-it” defense, because the text messages demonstrated there had been communication.

In all three cases described above, the defense attorneys acknowledged the objective quality of the evidence introduced by the prosecution against their client. Although the evidence had “killed” their cases, the public defenders didn’t hold grudges against the other side. In fact, sometimes they would even tip their hat to the police and prosecutors, and comment that it was good law enforcement to get such persuasive information. What public defenders called “killing cases,” was actually prosecutors and police effectively using digital evidence to locate and convict people who had committed a crime (Browning, 2010; Brunty & Helenek, 2013).

Digital Evidence on the Periphery

I have just described instances in which defense attorneys experienced digital evidence as a damning force – as one of the, if not the key piece of evidence that led to a defeat at trial or forced them to advise their clients to take a plea. However, the concept of digital evidence "killing cases" was not the only way public defenders experienced such evidence being used against their clients. During my time in the field, I noticed digital evidence being used as a peripheral factor alongside other forms of evidence to bring down a case. By peripheral factor I mean that digital evidence played a role in the downfall of the case, but it didn't strike the killing blow. Instead, digital evidence, especially from social media, was used by the prosecution to make moral arguments that the defendant was dangerous or vile, and was introduced as supporting evidence in the larger context of the case. In making these moral arguments, prosecutors drew on stereotypes of what criminals looked and acted like to insinuate that the defendants were worthy of punishment. Unlike the evidence used to "kill cases," which was objective and recognized as such by both sides, the digital evidence used to make moral arguments tended to be gray and open to interpretation. In the next paragraphs, I review the role of digital evidence as a peripheral factor and discuss how public defenders responded to or challenged these applications during bail hearings, plea negotiations, and trials.

Bail hearings. First, I discuss the use of digital evidence as a peripheral factor during bail hearings. Bail hearings are court processes during which a judge decides whether a defendant will be allowed to post bail and await trial outside of prison or if the defendant will be remanded in custody. This is also the time at which the amount of the bail is set. When determining the bail amount, the judge considers a range of factors, including the nature and severity of the alleged crime, whether there is a flight risk, and the personal character of the defendant. Here, I found that prosecutors were able informally to introduce digital evidence to make moral arguments about the defendant and request a higher bail amount or remand, because the defendant seemed dangerous or appeared to have ties to criminals.

Julie, the attorney who worked on the case with the Yankees cap and whom I mentioned earlier in this chapter, described a digital evidence-related struggle she had faced during a bail hearing with another client. The defendant had been charged with criminal possession of a forged instrument for having a fake driver's license. That was the only charge, she explained. However, on social media, he had interacted with individuals who were suspected of being in terrorist groups. During his bail hearing, this information was raised by the prosecution to request a higher bail amount. "They weren't proceeding on any sort of terrorism charges," Julie said. The social media content, she argued, was brought in by the prosecution only "to try to make a bigger case out of something that they didn't have much of a case on." The higher bail amount however, meant Julie's client could no longer afford to pay his bail and had to stay in jail until a plea agreement was reached months later. Julie was frustrated by this decision, especially because the terrorism references were not related to the charges brought forth against her client. The social media content came in only during the bail hearing; it had no bearing on the eventual plea bargain.

Linda, to whom I'd previously talked about the use of location-based evidence in digital cases, also experienced several instances in which social media were introduced during bail hearings by the prosecution to request a higher bail amount. In one case, the introduction of social media pictures of her client holding a firearm led a judge to reevaluate an original bail agreement. Linda's client had been out on bail, she explained, but after the prosecution presented this new piece of evidence at a hearing, the judge decided to reevaluate his earlier decision. "The judge really changed his attitude towards the client," she said. The judge increased bail, and Linda's client had to go back to jail for a period of time until he was able to secure enough funds to make the new bail amount. Linda tried to argue against the increase, noting that her client had no prior record, that he had ties to his local community, but she was unsuccessful in her effort.

The stories shared by both Julie and Linda illustrate how, in the digital turn, personal social media content is reinterpreted in the judicial context to paint moral arguments about defendants as dangerous and therefore worthy of punishment. In the first instance, by alluding to a possible association with terrorists, and in the second, by suggesting the defendant had in the past yielded a gun. Each time, these peripheral uses of social media led to prison time for the defendants, a severe consequence, especially given that the evidence was never formally applied towards their charges. The defendants were made to answer for their choices of online associations and self-presentation through incarceration.

Plea hearings. Another example of the peripheral application of digital evidence was during plea hearings and informal talks between public defenders and the DAs. Plea hearings refer to the moments in case processing when both sides come together to agree on the terms and conditions of a guilty plea for the defendant. Rebecca, an attorney in the office, recalled facing a digital, evidence-related challenge during such a hearing. On the basis that a picture showed the client had engaged in dangerous behavior, the prosecution introduced a Facebook picture of her client holding what appeared to be a gun during the plea hearing to ask for a less advantageous deal. The defendant was a young woman, a first-time offender, who was facing charges for a low-level drug crime, a nonviolent offense. Rebecca felt that bringing in the Facebook picture was unfair to her client, because it made the young girl look like a threat in a way that was not proportionate to her actual crime. "It was informally used. I [was] asking for something from the judge. I [was] asking for a better offer, saying, ‘No record; non-violent; this isn't anything’, and [the prosecution] was saying, ‘Yeah, but beware of her. Look at this [picture]’,” Rebecca said. Guns imply participation in a violent crime, yet her client had been charged with only a low-level drug offense.

Rebecca argued that it was a fake gun, a BB gun, and that her client was not an actual threat. She added that the young girl was attending high school and playing basketball, and, outside of that one incident with the drugs, she was an upstanding, young woman. Eventually, Rebecca asked her client to speak directly to the judge. This was risky, she said, “I almost never do this, but I let her [speak] to the judge. She admitted she] was just posing in a dumb way with a fake gun that [belonged to] someone else.” This decision ended up playing in the client’s favor. According to Rebecca, she ultimately secured a good plea for her client, however, she couldn’t shake the feeling that things could have gone even better without the photo.

These examples showed how digital evidence adds layers of complication for defense attorneys and forces them to respond to the prejudicial narrative of the prosecution through moral arguments of their own. In the digital turn, defendants are made to answer for their online self-presentations and the friends they keep to the criminal justice system (Lane, 2018). In this instance, the young defendant literally had to speak up to defend herself against the photo introduced by the prosecution and justify her self-presentation in front of judicial actors.

At trial. The third way digital evidence entered cases tangentially was during trials. Stephen, a public defender from a neighboring office, who worked on many gang-related cases had several instances in which digital evidence unrelated to the case was successfully used to make prejudicial claims against his clients’ personality or lifestyle. Next, I will describe two of the stories Stephen shared with me about the use of peripheral, social media evidence.

Stephen, whom I met through his wife Erin, shared a story about how the introduction of a prejudicial photograph to identify his client negatively impacted the outcome of a recent trial. To make the identification, the prosecution selected a picture from the client's Instagram account in which the client looked particularly thuggish, Stephen explained. When describing the photo, Stephen said the Instagram picture showed his client "standing on the street corner with the baggy pants in a, you know, in a tank top with his hands sort of out there at his crotch, looking tough." What upset Stephen about the use of this kind of picture for identification purposes was that it was highly prejudical and implied the client was a gang member, when the case itself was not about gang violence. To make matters worse, Stephen noted that the prosecution could easily have chosen a different picture to make the identification. "Now, mind you, every third photo in his Instagram account is a picture of him holding his two-year-old daughter," Stephen said. The prosecution's argument for choosing the more thuggish-looking photograph was that it was a full body shot and made it easy to recognize the client's height in relation to other markers in the picture. Stephen did not believe this was a valid point, "Here's a full-body image of him holding his child. What gives you better sense and perception of how tall and big he is than that?" Stephen asked. I sensed his disappointment at what appeared to be a selection bias in the type of photographs chosen to identify his client. As we talked, Stephen noted that ultimately, there was other digital evidence that hurt his client, and that the result had not come down to this picture only. However, he felt the picture had painted his client as someone who looked intimidating, and that its introduction had added a layer of prejudice that had damned the client even further.

In a different case about a gang shooting, the prosecution played a video in court in which Stephen's client and several co-defendants could be seen dancing to loud rap music. In parts of the video, the men were touching their crotches and holding their hands out like guns; it certainly wasn’t a flattering video. However, there were no actual guns in the video. Stephen said that the video had established only that the men knew each other and listened to rap music. “Now, that came in as evidence. Tell me how that’s relevant other than to make my client look like he’s kind of a bad dude, right?” he asked. His client was charged with weapons possession and named as an accomplice in an assault homicide. According to Stephen, the video had not helped to support these charges against his client. The decision to allow the video was highly prejudicial. When I asked Stephen how he had fought back against this piece of evidence, he simply said he hadn’t. His only option would have been to put his client on the stand at trial and have him explain that the video showed a group of friends “out having a good time, playing music, drinking, and screwing around.” That, however, was too much of a risk for Stephen. He believed that providing context for the video would do little to help and only open his client to further scrutiny. As I’d learned from other attorneys, permitting defendants to testify is a gamble. Many defendants don’t come across as very likeable, and once they are on the stand, there is a risk that they might share information, which may further damage their case. Reflecting on the gamble of putting his client on the stand, Stephen said, “To me, it’s an incredible shifting of the burden when someone’s presumed to be innocent, to have to explain things like this that have so many explanations.” Stephen believed that his client should not have had to take the risk of defending his behavior in a video, which, according to Stephen, should not have been introduced as evidence in the first place. Of the various cases he has handled, Stephen noted that this one struck him as particularly harsh and unfair because of the way digital evidence was used to paint a negative picture of his client.

Challenging Prejudicial Content and Overbroad Search Warrants

In the informal setting of hearings, there were no legal standards to which the defense attorneys could turn to prevent the presentation of damaging, prejudicial, digital evidence. That is because the evidence wasn't being formally introduced in connection with the charges, but was presented informally instead, as part of a point the prosecution made during a hearing. In trial cases, however, defense attorneys had some legal recourses. "There are rules against presenting bad acts that are separate from the client's alleged incident," Rebecca explained. When the prosecution introduced what the defense perceived to be harmful evidence against their client, defense attorneys tried to fight back by arguing that the evidence was not relevant to the case or had no probative value. Vicky, who worked on many cases with youth who had gang ties, noted that she typically argued that the inclusion of peripheral information, such as social media pictures of her clients posing with weapons or throwing hand gestures, was "overly prejudicial, and that it had no probative value." Sometimes Vicky was able to have content that painted her clients in a negative light excluded, and sometimes she was unsuccessful.

Very few cases, however, went to trial, and so defense attorneys were not often able to use these arguments to fight back against harmful digital evidence. An alternative option was to attack the manner in which the prosecution had acquired the evidence. One such approach was to contest the validity of the search warrant issued for the evidence. As seen in the analysis phase, a issue common to search warrants for digital evidence was that they tend to be overbroad, which means that they grant access to the entire content of a phone or social media account, with no limitations by timeframe or type of data (Denney, 2018; Gershowitz, 2016). In the year I spent observing the work of the digital forensic analysts and talking to defense attorneys, Linda was the only attorney with whom I spoke who succeeded in controverting a search warrant and suppressing the social media content that had been recovered because of it. George, from the digital forensics lab, had helped her write the motions in the case and recommended that I speak with her to learn more about how she had tackled the search warrant issue.

I met with Linda in April 2018 at her office in the Northeastern Defender Association for an in-person interview. We talked about the background of the case. Linda, explained that her client, Rob, had stolen goods from a perfume store and had been stopped by law enforcement while attempting to drive away. The police officers searched the car and, during the search, recovered not just the proceeds from the larceny but also a gun stored in the glove box, and several electronic devices, including a phone and a GPS navigation system. The gun find was bad for Linda's client because Rob did not have the appropriate permit to have it in his vehicle in the state of New York. Thus, he was charged with an additional offense. Now that the various electronic devices were in the prosecution's possession, Linda explained that a "blanket search warrant for everything and anything that might possibly have any relationship to any criminality at any point from any of the devices with no limitations" was issued. Though she had seen broad search warrants before, she was shocked by the sweeping reach granted in this one. She turned to George for help in writing a motion to controvert the search warrant on the basis that the search could reasonably have been limited to communications with the other individuals in the car or to digital content related to the grand larceny charge. Linda said, "If those electronics were in the car and […] were with them while they were committing the crime," a reasonable search warrant, should have said, "Let me look for communication between these individuals as they made their plans or let me look if they were using some sort of mapping [service]," Linda explained.

As she waited to hear back from the judge about the motion, Linda learned that the prosecution planned to use digital evidence from the various devices recovered from the car in two core ways. First, they wanted to introduce Internet browsing histories that showed Rob had looked up specific fragrances and then searched for stores that carried those same fragrances. The perfumes he had searched for were the same ones recovered in the car. Linda admitted that that was a fair use of digital evidence against her client. Second, the prosecution planned to use a series of old Facebook messages, dating back several months, in which Rob and a friend had discussed using a gun in a potential confrontation with Rob's sister's boyfriend. Linda disagreed with this application. She believed the prosecution had no basis for searching Rob's social media for mentions of a gun. "It wasn't like they were alleging an ongoing criminal conspiracy that dated back months," she said. The gun wasn't used as part of the larceny; it was discovered as part of the vehicle search, Linda noted. With the help of George, she presented written arguments that challenged the scope of the warrant.

Ultimately, the judge decided in Linda's favor. He ruled that the search warrant was overbroad and that the Facebook messages about the gun could not be used. This was a great victory for the public defender office. Reflecting on the overbroad search warrant, Linda said, "They were just fishing. They got a search warrant […]. They looked at everything and they found something they liked. That's not how it's supposed to go." In the end, Rob took a plea instead of going to trial, but Linda still believed that challenging the search warrant had been crucial to Rob's case and to defender case law more broadly. By having the Facebook messages excluded, Linda was in a stronger position to argue for a favorable plea for Rob. She also hoped that, in the future, other public defenders would be able to look back on this case as an example of how to successfully challenge flawed, overbroad, search warrants.

The Few Times Digital Evidence Saves Cases

The more I talked with attorneys about the different ways in which digital evidence appeared in their cases, the more I realized that, although digital evidence was often harmful and difficult to combat, the situation wasn't quite as bleak as defense attorneys made it out to be. During my time in the field, I observed numerous instances in which digital evidence was a valuable resource for defense attorneys. Outright victories, such as a trial acquittal were rare, but digital evidence played a role in getting cases dismissed and securing better plea agreements for defendants.

Dismissals. In late 2018, I interviewed Maggie, a defense attorney whom I'd met during my observations in the digital forensics lab, to discuss how she approached cases with digital evidence. Like most of the attorneys with whom I spoke, Maggie stated that she typically encountered digital evidence as something that hurt her cases. The prosecution presented a phone extraction report or shared a Facebook printout, and, inevitably, an admission by her client tied him directly to the crime. "It can really hurt [your case]. If your client said something in these texts or on Facebook – you know, it can be strong evidence against you," she said. When I asked her if she thought it could go both ways, whether digital evidence could also be used to help her clients, she paused for a moment. "I guess," was her initial response. Sensing that there was more to this, I pressed her on the matter. Maggie then said that, surprisingly enough, she had recently used digital evidence to get a mistaken identity case dismissed. "I forgot about that one! That was an amazing case that helped my client," she said excitedly.

With a newfound enthusiasm, Maggie shared the details of the case. Her client, Jon, had been charged with assaulting a man outside of a bar. The DA's office had surveillance footage that showed a large, African American man in a blue shirt sucker punching another man outside of the bar. The video had been shot from far away, Maggie explained. She was able to tell that the men involved in the altercation were African American, but one couldn't see faces. Her client, Jon, was a black man, and he had admitted to being at the bar that night, but that was really all they had on him, Maggie noted. Although he admitted to being outside the bar when the fight happened, Jon was insistent that he was not in the video and that the prosecutors had mistaken his identity. A few days went by with no update on the case until Maggie received a message from Jon letting her know that one of his friends who was with him that night had taken a picture of them and posted it to Facebook. Jon forwarded the picture to Maggie. "It was dated, timed, everything. [It was] on Facebook; four guys, you know, hugging each other, and my guy was clearly wearing a [different] outfit," Maggie said. The man who threw the punch in the video was wearing a blue shirt, but in the picture, Jon could be clearly seen wearing a red shirt. Armed with this piece of digital evidence, Maggie reached out to the DA on the case. They rewatched the surveillance video together, and, this time, they were able to spot Jon in his red shirt in the background, far away from the fight. "They completely got the wrong guy," Maggie said. The DA apologized, and the case was dismissed right away.

Once they got the Facebook picture, everything happened very quickly, Maggie said. I could tell she was excited to have been able to help her client, and I wondered why this kind of success story wasn't at the forefront of her mind when she thought about digital evidence. Perhaps Maggie's point about how quickly everything was finished explains why this kind of use of digital evidence does not have the same staying power. Jon wasn't Maggie's client for very long. They had met a couple of times, and, as soon as she was able to get the charges against him thrown out, she moved on to the next case.

After hearing Jon's story, I asked what would have happened if Jon's friend hadn't remembered that he'd uploaded a picture of them on Facebook. Maggie hypothesized that she probably would have asked Jon and his friends to testify that the man in the video wasn't Jon. "We would have tried. [Jon] would have testified, maybe his friends would've come in and said that's not [Jon], he's over here in the video," she said. Having the Facebook picture, however, was a much safer bet. There was an objectivity to the time stamped, geotagged picture of Jon in a different shirt that could not as easily be replicated by having his friends testify. Jon's story showed that digital evidence can give credibility to a defendant's claims to be recognized as persuasive and valid by both the defense and the prosecution.

Courtroom acquittals. In this section I discuss the application of digital evidence during trials and show how a combination of objective and gray digital evidence was used to secure an acquittal for a defendant. In public criminal defense, cases hardly ever make it to trial, and acquittals are a rarity (Weiss, 2005; Wice, 2005). During my field work, I observed one trial acquittal and learned of a handful of others through my interactions with attorneys. In October 2017, when I heard that Kelly was scheduled to testify in court about the digital forensics work she had performed, and that the case in question had a decent chance of having a positive outcome for the defendant, I jumped at the chance to observe firsthand how digital evidence was handled in the courtroom. The case involved a young man named Daniel and his alleged participation in a drug-related crime. The prosecution's case against Daniel rested primarily on the statement of an undercover police officer who claimed to have seen Daniel participate in a drug transaction at a bodega in Manhattan's Lower East Side. When Daniel was arrested however, he had no money or drugs in his possession, and he was adamant that the police officer at the scene had confused him with someone else. It was true that Daniel had spent time in that neighborhood, including in the bodega, but he stood by his statement that he was not involved in any drug transaction.

At trial, the defense team turned to digital evidence in several key ways to raise doubts about the prosecution's argument that Daniel was the young man at the bodega. First, the defense used CDRs and phone extraction data to show that there had been no communications between Daniel and the other person allegedly involved in the drug transaction. Then, it used CDRs and cell tower information to suggest that Daniel was not in the Lower East Side at the time of the incident. And third, the defense used the content of text messages Daniel had sent and received around the time of the alleged incident to show that he was preoccupied with school and other personal happenings, and not, as one might expect of someone involved in the sale of illicit substances, finalizing the details of a drug transaction. In doing so, the defense combined object evidence, such as CDRs and location information, with gray evidence from text messages that made a moral argument about the client as a good, college-bound kid. In the next paragraphs, I take a closer look at Daniel's trial and the different ways in which the prosecution and the defense brought digital evidence to bear on their interpretation of the events.

When I entered the courtroom, the prosecution was presenting an exhibit to the jury. The presentation revolved around a map that highlighted six to eight locations where Daniel had been, according to his cell-phone activity on the day of the alleged drug sale. The pins on the map indicated the locations of the various cell towers to which Daniel's phone had connected to send and receive text messages. Based on the map, Daniel had spent parts of the day in Queens and then moved west to Midtown later in the afternoon. A text message Daniel received at roughly twenty minutes before the time of the incident placed him somewhere around 42nd street, a good forty blocks away from the location of the drug sale. The prosecution used the cell tower information to suggest that Daniel had been on a trajectory west and then south throughout the day, and that he could have reached the bodega on the Lower East Side in the twenty-minute time span between the last text message he had received and the time at which the drug transaction had taken place. The defense disagreed with this interpretation, and Kelly was called to testify on behalf of Daniel.

Kelly's witness testimony began with a review of her qualifications as a digital forensic analyst. After she had been declared an expert witness, she explained that the first task she performed for Daniel's case was a phone extraction. As part of that process, she had filtered the data up to the date of the alleged incident. Kelly found no communications on Daniel's phone during the time of the alleged drug sale, which took place around 4:10 p.m.; the last phone call on Daniel's device was an incoming call at 12:28 p.m., and the last message was an incoming text received at 3:47 p.m. He had sent and received other messages earlier in the afternoon, Kelly said. These messages, including the one he had received at 3:37 p.m., corresponded to the cell tower locations of the map shown earlier by the prosecution. The last cell tower to which Daniel's phone had connected placed him in Midtown, several miles from the bodega at which the drug transaction took place.

Next, the defense attorney handed Kelly a copy of Daniel's CDRs and asked her if there were any communications, whether in the form of text messages or calls, between Daniel and the other individuals allegedly involved in the drug exchange. Kelly had already examined these records as part of her digital forensics work on the case months ago; still, she took the time to look at the pages carefully. She said she found no occurrence of any activity between the defendant and the other phone number. The defense attorney then proceeded to ask if the phone extraction Kelly had performed on Daniel's phone showed whether he had saved that number as a contact. Kelly said that when she performed the extraction, she had found no evidence of Daniel having stored the number as a contact on his phone.

At that moment, the defense attorney switched gears and asked Kelly to share the person with whom Daniel was texting back and forth that afternoon, and to read the contents of the messages aloud for the jury to hear. Kelly said the messages were from an exchange with a contact saved in the phone as "mom." In the texts, Daniel and his mom discussed schoolwork and his acceptance to a local community college: "I'm accepted. Passed the test, 44 out of 50," read one of Daniel's texts to his mother. Although the prosecution had used the cell tower location data from these very same text messages to suggest Daniel had been traveling south in the direction of the bodega where the drug transaction had taken place, they had made no mention of their content. By including these conversations, the defense added a psychological layer to their defense. It was a moralizing argument designed to paint Daniel in a positive light. Not only did the timeline and location of his texts make it unlikely that Daniel could have made it to the bodega in time to partake in the exchange, but the contents of his communications suggested that he was mentally preoccupied with other, more uplifting, life pursuits. Reading the text messages aloud was a way for the defense to take control of the narrative and present the Daniel they wanted the jury to see -- an upstanding young man who talked about schoolwork and was excited to tell his mother he'd been accepted into college. All in all, the defense's trial case focused on guiding the jury through Daniel's physical and mental whereabouts to show that he was not the person presumed to have participated in the drug exchange.

After court closed, Kelly and I walked back to the office to debrief with George and the other analysts. When Sarah asked if George, who'd seen Kelly's testimony, thought they'd win the case, George said he didn't want to jinx their chances by saying something, but he had watched the jurors and thought one of them was very likely on their side. A week later, I learned that George's instincts had been correct. Daniel had been fully acquitted.

Daniel's story was one of the most memorable cases from my time in the lab. It stood out for several reasons. First, it was one of the few cases in the office to make it all the way to trial *and* to result in a full acquittal, a very rare outcome in public criminal defense (Wice, 2005). Second, Daniel's defense strategy had relied heavily on digital evidence. Text messages and cell tower location data played key roles in challenging the prosecution's argument about Daniel's alleged involvement in the drug transaction. Daniel's acquittal story illustrates that the appeal of digital evidence is not limited to finding incriminating information (Dean, 2013; Grimm, 2014). The stories our smartphones tell about where we were, what we were doing, and with whom we were conversing can also be relied upon to establish a defense.

Plea bargains. In this section I turn my attention to the gray areas of digital evidence in plea bargaining. Sometimes, digital evidence played a dual role – it simultaneously confirmed the defendant's involvement in a crime *and* showed that the circumstances around the offense were more complex than the prosecution had claimed. When faced with such cases, public defenders used digital evidence to engage in nuanced storytelling and humanize their clients during plea negotiations. They attempted to show that, although a client may have committed the offense, the complaining witness had behaved in ways that encouraged or provided important context for the actions of the defendant. These gray applications of digital evidence were possible only if there was considerable digital evidence to draw upon to create a more nuanced narrative of the circumstances. Therefore, these uses of digital evidence happened almost exclusively in cases in which the two parties knew each other, such as domestic violence, harassment, stalking, and other unwanted contact cases. This also meant that defense attorneys had to be shameless and bring up unflattering aspects of a victim's behavior. Defending their client without blaming the victim was a difficult line to walk at times. I sensed that attorneys sympathized with both their clients and the victims of the alleged crime. None of the attorneys I interviewed believed victim-blaming was an acceptable strategy. They called on the complaining witness's actions only when it was absolutely necessary to their client's defense.

When I asked defense attorneys if they had ever used digital evidence to help their clients during such plea negotiation, many responded that they had used text messages and social media content in domestic violence or harassment cases to counteract the often-damning portrayal of their client by the prosecution, but they were hesitant to say that the evidence had "helped." The reason for this hesitancy, I learned, was because most evidence in domestic violence or harassment cases was bad for the defendant. For instance, text messages and social media posts could be evidence that a defendant had violated a protection order or communicated with the victim, even though a no-contact order had been issued. At the same time, defense attorneys recognized that there was something of value in those communications. Although the communication may not have been authorized, it was often consensual and friendly. Rebecca, one of the attorneys in the office, noted that she had encountered instances in which the alleged victim had been the first to reach out and had even attempted to rekindle a romance via social media. Having this information was important for Rebecca, because it allowed her to show that the communication wasn't unwanted, or at the very least had not started out as such. Another attorney, Linda, said that the dual character of this type of digital evidence made her work as a defense attorney challenging, because she had to think about how to fit opposing viewpoints together to achieve the best possible outcome for her client. During our interview, she said, "Those interpersonal relationships that have a long history […] and are very complicated […]

yield a lot of things that are very bad for our clients. Often the existence of the communication itself is a crime. [At the same time] they are often very fruitful to us, [and allow] us to say, your victim, your complainant, is no angel here." Ultimately, using digital evidence showed the complexities of human relationships, that defending a client who had committed an offense by pointing to communication as a sign that the circumstances of the case were not cut and dried. I noticed two themes in the approach defense attorneys took in those instances: 1) they presented girlfriends/romantic partners as threatening the defendant, or 2) they presented the communication as welcoming, friendly, and initiated by the complaining witness.

Girlfriends and prison threats. Harassment and domestic violence cases are challenging not simply because there are two sides to each story, but because there is a lot of story to examine, which further complicates the task of deciphering the narrative. Linda noted that when she was working on such a case, she received a lot of data from the prosecution to suggest her client had repeatedly contacted the complaining witness to the point of harassment or intimidation. Call logs and social media exchanges were common examples, and, on the surface, this evidence painted the defendant as guilty and as a bad person. However, when she had met with her client to hear his side of the story and had had the digital forensics lab recover her client's communication records, Linda's understanding of the situation had shifted. Not only did these records show that there had been calls and messages from the complaining witness directed at the client, but, sometimes, the complaining witness had engaged in intimidation of her own. "Our client comes in with their phone and shows us that the other person, the person who's claiming to be stalked or harassed […], in fact, has been messaging every bit as often and […] saying, 'If you don't do what I want, I'm going to go to the police and say you're stalking me'" or saying, "I'm going to the police and I'm going to say you're doing this," Linda said. For a defense attorney, showing this other side of the relationship was a crucial part of painting a picture in shades of gray rather than black and white. The messages allowed Linda to argue that the complaining witness was prepared to use the criminal justice system to punish the defendant, and that her client was not the only one who was engaging in improper behavior. Although the communication history had harmed Linda's client because it had revealed that he had been contacting the complaining witness, it had also been helpful because it had shown that the complaining witness was holding this violation over the defendant's head and threatening to use it against him in the criminal justice system. Heather, another attorney, referred to the process as "filling in gaps." The prosecution presented one side of the issue, which wasn't entirely fair to the defendant, and defense attorneys worked on uncovering the rest of the story. Linda encountered so many instances of girlfriends or wives using the threat of the criminal justice system that she made it a rule to tell her clients to be forthcoming with any information that may help their case. "I tell my clients if you are getting communications directed at you from this person who is saying you are doing these things, you save them, you notify me, you come in, and we collect that information," she said.

It was mutual. In one of my visits to the digital forensics lab in December 2017, I observed while Kelly worked on a phone extraction. She explained that she had been asked by the attorney on the case to preserve a series of text messages between the defendant and the complaining witness. The defendant was a young, after-school program worker. He had been accused of sleeping with a fourteen-year-old girl who was a student at the center where he worked. Even if the relationship had been consensual, by law, the girl was unable to consent to the relationship. Kelly was more quiet than usual while working on the extraction, and I wondered if she was affected by the serious charge of rape in the case. Working as a digital forensic analyst in the public defender office meant assisting defense attorneys in the provision of the best defense possible for all clients, even those charged with raping fourteen-year-old girls.

Kelly found some flirtatious text messages between the two parties and put them into a report for the attorney. The text messages provided background information for the client's defense. They established that the defendant and the complaining witness had close, personal communications, and that they were mutually attracted to each other. Kelly later learned that it was the girl's sister who had reported the relationship to the police, not the girl herself. This too might help the client's case, she explained. Kelly assumed the plan was to argue that, although the relationship was not lawful, the communication wasn't unwanted or based in harassment.

The case Kelly worked on had the additional hurdle that it involved sex with a minor. But the idea that of the communication between the defendant and the complaining witness was friendly or even flirty was not uncommon. Rebecca had handled numerous domestic violence and harassment cases and noted that she often brings up a couple's communication history in her meetings with the prosecutor to show that the matter is not clear-cut, that her client isn't the monster that they made him out to be. She turns to call logs, social media posts, or other communication records to show that the complaining witness was not scared of the defendant, but, was contacting him/her repeatedly and sometimes trying to get back with him/her. Rebecca was very forthcoming that this type of evidence doesn't save her cases. Yet when she reflected on the work of public defenders in those situations, she said, "It makes it easier for us to negotiate." Although it does not excuse the fact that her client has violated a protection order or a no-contact order, having tangible proof of a friendly back-and-forth exchange between her client and the complaining witness can go far to help obtain a better deal.

The Application Phase: Discussion

In this chapter I examined how digital evidence was used in case outcomes. First, I looked at how the prosecution used digital evidence against defendants to either “kill” cases through objective, damning evidence or as a contributing factor in the downfall of a case through more subjective, gray evidence that made moral arguments to paint defendants as vile and dangerous. I also explored how defenders fought back against such applications by raising questions of relevance and prejudice and challenging the overbroad search warrants that had permitted the acquisition of the evidence in the first place. The second half of the chapter focused on how public defenders successfully applied both objective and gray forms of digital evidence to help secure trials and acquittals for their clients and to argue for better plea deals during negotiations with prosecutors.

The most interesting take-away from the application phase was the contrast between objective evidence and subjective or gray evidence. The defense and the prosecution both used digital evidence to these effects, but to different ends and with different consequences for defendants. In the face of damning evidence that tied the defendant to the alleged crime, defense attorneys spoke of digital evidence “killing” their cases. These applications of digital evidence tended to be self-evident and left little room for a nuanced interpretation of the facts. Location-based evidence that firmly put the client at the scene of the crime or video evidence that identified the defendant as the person who had committed the crime were examples of objective evidence. The decision to refer to digital evidence as “killing” their cases reflected the defeat that defense attorneys experienced at their inability to engage in legal storytelling in those instances (Delgado & Stefancic, 2012). To counter the digital evidence that “killed” cases was to use digital evidence to have cases dismissed. In such instances, defense attorneys were the ones who drew on the objective appeal of digital evidence to clear their clients of the charges brought against them. Although they never expressed it in such terms, dismissals were how the defense “killed” the prosecution’s case by using the same types of digital evidence that the prosecution used against them in another scenario. Dismissals didn’t require lengthy legal narratives. In fact, in the mistaken identity case I described in this chapter, Maggie had only to show the prosecution the Facebook picture of her client at the bar with his friends. What separated objective, digital evidence from its nuanced, gray counterpart was that both sides recognized and agreed about its persuasiveness. There was a mutual recognition that such evidence was powerful and convincing, and that the side on the receiving end of the digital evidence did not stand much of a chance.

It is in the presentation of gray forms of digital evidence that it became obvious that the prosecution and defense engaged in radically different, legal storytelling. Both sides formulated opposing moral arguments about the defendant: the prosecution drew on preexisting ideas of what criminals look like, and the defense challenged those assumptions by pointing to socially desirable behaviors in the defendant, such as community involvement or school attendance. These were also the applications of digital evidence that relied most heavily on information about the personal lives of defendants. This was where the prosecution brought in social media images and personal communications as supplementary evidence to help bring down a case through moral appeals about defendants as threatening, violent, or otherwise unsavory individuals. In the context of the life cycle, the application phase represented the culmination of judicial actors coming into contact with defendants’ personal information - a key aspect of the digital turn.

The peripheral applications of digital evidence by prosecutors indicated a continuation of racial stigmatization and punishment of marginalized people by the government (Alexander, 2012). By holding up photos of defendants with guns, the prosecution was effectively labeling them as criminals, before a verdict had been reached on the case. I found that the digital turn offered prosecutors a way to exercise preemptive judgement about defendants through a reinterpretation of mediated interactions in the context of trials and hearings. Because the photos and messages used for such purposes had been created by the defendant, the prosecution could claim the evidence was being endorsed by the defendant (Lane, 2018; Lane et al., 2018). In the context of young men accused of being gang members, Lane (2018) notes that photos were a powerful way for the prosecution to tie defendants to forms of self-presentation, which were widely associated with criminals and other deviants. In other words, showing such photos was a way to say nonverbally that the defendants appeared to be gang members.

The legal narrative about peripheral, digital evidence was overwhelmingly controlled by the prosecution who selectively chose which social media pictures to include and which ones to exclude, based on whether the content serviced their preferred legal narrative of the alleged crime. To make an identification at trial, the example of the prosecution selecting a picture of the defendant looking thuggish rather than picking one of the many of him holding his daughter illustrates how the prosecution controlled the narrative presented about a defendant in troubling, prejudicial ways. Lane (2018) refers to this curated selection of digital evidence by the prosecution as "editorial control," and argues that putting forth a preemptive interpretation of the defendant as someone who fits a stereotypical description of a criminal allows the prosecution to get a head start on the story told in court. Defense attorneys attempt to keep such evidence out of courtrooms by challenging its probative value or calling it out for being overly prejudicial. However, more often than not, defenders are unsuccessful.

Although the tools of oppression were expanding to include new types of evidence, I found that the criminal justice system continued the same subjugation and discrimination of marginalized groups that has been rampant since the war on drugs started in the 1970s (Alexander, 2012; Stevenson, 2014). Personal communications, from texts to social media photos, represented a shift in how moral arguments about poor, black defendants were being made. But the stereotypes remained the same; the prosecution continued to paint indigent defendants as dangerous and therefore worthy of punishment (Delgado & Stefancic, 2012; Dickinson, 2012). The peripheral use of digital evidence had severe consequences for defendants. At trial, such pieces of evidence criminalized defendants and helped secure guilty verdicts. During plea bargains, they were used to request higher bail amounts or the remand of defendants to custody. Clients who couldn't make the new bail amount or were remanded faced jail time. This often resulted in a temporary loss of income, if not the loss of one's employment all together, and put a strain on a defendant's loved ones (Blankenship, del Rio Gonzalez, Keene, Groves, & Rosenberg, 2018; Christian et al., 2015). My findings show that the use of digital evidence in bail hearings is adding to an existing cycle of poverty among the poorest in society. The Prison Policy Initiative estimates that 70% of the 646,000 people being held in local jails are there pre-trial, which means that they have not yet been charged. Most of those individuals make less than $15,109 a year (Rabuy & Kopf, 2016). Although they have not yet been convicted, those individuals suffer the same consequences as those who are incarcerated post-trial.

Peripheral use of digital evidence was not a tool that was exclusive to the prosecution. I found that defense attorneys used digital evidence to make moral arguments of their own, to challenge the prosecution's depiction of the defendant, and to help their clients get better deals during plea negotiations. The use of such storytelling techniques was a way to raise awareness about the plight of poor defendants and point to systemic issues of prejudice and racism in the criminal justice system (Delgado & Stefancic, 2012; Fajans & Falk, 2009). But not all narratives were about exposing discrimination. In the stories they told, public defenders also had to humanize and evoke sympathy for defendants who had been charged with heinous crimes, such as domestic violence, harassment, and assault case. During my time in the field, I never met a defense attorneys who relished attacking victims of domestic violence or who discounted their suffering. On the contrary, Stephanie, an attorney who handled numerous such cases noted that at a recent trial, she had been hesitant to go after the alleged victim because the young woman had appeared to be a very sympathetic witness. "I was worried about the appearance of ganging up on her or, you know, being too aggressive with her." Being a public defender meant having to represent men who hit their girlfriends and putting one's personal feelings about such actions aside to build a defense strategy in the client's favor (Davis, 2007). Defending clients against such charges required a level of shamelessness, and sometimes their defense called for challenging alleged victims. Mostly however, when constructing a narrative in favor of their client, I found that the attorneys emphasized the complexities of the relationship between their client and the alleged victim to create nuances around the circumstances of the incident.

In addition to plea bargains and dismissals, I described one rare instance in which defenders were able to use digital evidence to secure an acquittal for a client. Through the story of Daniel, I showed how defenders used a combination of objective and gray digital evidence to suggest that not only was it unlikely that the defendant could have made it to the location of the crime, but his conversations with his mother painted him as a morally upright individual.

Although Daniel's story illustrates that digital evidence can exculpate and is not only a prosecutorial tool for incrimination, I am hesitant to suggest that taking cases to trial is the best way to confront injustices in the legal system. This hesitancy comes from two concerns. First, defense trials based on digital evidence call for special expert witnesses (such as a digital forensic analyst) and a defense attorney who is well-versed in technical matters. Technology literacy among public defenders varies widely. Public defender offices that don't have in-house, digital support face the additional cost of outsourcing requests for assistance. This suggests that not all public defenders are equally prepared to handle such high stakes cases. Second, trials are notoriously risky and unpredictable (Wice, 2005). It is hard to determine how the individual characteristics of jurors will influence their decisions or whether jurors will be able to understand the technical aspects of how digital evidence is acquired and analyzed (Goodison et al., 2015; Hans & Eisenberg, 2011). Asking defendants to trust in the exculpatory power of digital evidence at trial places an undue burden on them. It asks them to take a gamble on their future in a system that is unpredictable and has historically been biased against marginalized people.

Perhaps the best approach is to fight back at the source and push for legal changes regarding the overbroad search warrants through which personal information enters the judicial system. Various civil liberties organizations have challenged the legitimacy of overbroad search warrants by using the argument that they violate 4th amendment rights, such as the right to be protected from unreasonable searches (Denney, 2018; Gershowitz, 2016). In this chapter, I pointed to one instance of a public defender succeeding in having information excluded from the case by challenging the search warrant that had been used to obtain the evidence. Recent legal developments, such as the Carpenter v. United States ruling on the necessity of search warrants to acquire historical cellphone location records and the Riley v. California ruling on the unconstitutionality of warrantless searches of digital content during an arrest, show that there is a broader push to limit judicial access to personal information (Liptak, 2014; Matsaki, 2018). These movements as well as the attorney-level pushbacks I observed represent opportunities to intervene to protect the privacy of defendants and others whose data become swept up in the criminal justice system.

In the application phase of the life cycle public defenders and prosecutors presented their competing narratives about defendants and their alleged crimes during hearings, plea negotiations, and at trial. This chapter showed that, although there were certain objective, damning types of digital evidence that were recognized as such by both the prosecution and the defense, most of the time, defenders and prosecutors worked with gray digital evidence that was open to different interpretations. Here, both sides formulated opposing moral arguments about the defendant. I found that prosecutors used digital evidence to continue the same subjugation and discrimination of poor, black defendants by drawing on preexisting stereotypes of criminals when discussing the personal communications and photographs of defendants. However, I also found that access to personal information about their clients' lives allowed defenders to challenge those assumptions by pointing to socially desirable behaviors in the defendant, such as good school attendance, or creating nuanced narratives of the circumstances of a crime.

Chapter 7: Conclusion

Review of Findings

This dissertation studied the digital turn in public defense. I argued that the defining feature of the digital turn was the increased use of digital evidence by prosecutors and defenders throughout case processing. As part of handling cases, both sides came into contact with photos, conversation records, and location information, and used these pieces of digital evidence to understand the people, events, and circumstances involved in the alleged crimes. This raised questions about how such information entered the criminal justice system, the processes behind its analysis, and how it was interpreted to formulate competing narratives about poor defendants and the circumstances of their alleged crimes. I developed the "life cycle" approach to show, through an intuitive framework, how different moments in the life of a case unfolded in the digital turn. This life cycle approach was divided into three phases that focused on different elements of case processing: acquisition, analysis, and application. This framework makes an important contribution to socio-legal studies by presenting a process-oriented approach that allows scholars and legal practitioners to understand how the digital turn has shaped public defense. Below, I briefly review key findings for each phase in the life cycle approach.

Acquisition phase. This first stage in the life cycle focused on the acquisition of evidence from smartphones and social media, which could be helpful to a defendant's case. It involved public defenders working closely with digital forensic analysts and investigators to assemble the building blocks of the defense's narrative. I found that the process of acquiring digital evidence brought defenders, analysts, and investigators into contact with personal parts of defendants' lives, in terms of both sensitive, personal data and interactions with the family members and girlfriends of defendants. Although this initial data acquisition process was laden with challenges, such as the need to find workarounds for clients who couldn’t drop off their device at the office, clients who were reluctant to turn over devices, and the inability to recover deleted content, the acquisition phase also presented new opportunities for defendants who were proactive about evidence preservation to help shape the legal arguments made on their behalf.

Analysis phase. In this second phase, public defenders examined extensive records from social media, smartphones, and other sources to assess what kind of defense narrative they would be able to formulate. Digital forensic analysts sometimes assisted the defenders in interpreting technical aspects of digital evidence. My findings show that the information overload associated with the digital turn added new burdens to the already overworked public defenders. Technology literacy among public defenders varied greatly, and not all attorneys were equally adept at managing this data deluge. Whereas some successfully used the objective properties of digital evidence to reason with clients and discuss defense approaches, others felt overwhelmed by the technological demands of the digital turn. I also found that public defenders experienced shifting, professional boundaries when digital evidence from personal communications became part of attorney-client interactions. Some attorneys experienced discomfort from the access to personal information about their clients, whereas others saw it as a valuable lens into their clients’ lives that helped humanize defendants.

Application phase. In this last stage of the life cycle, either the prosecution or the defense applied digital evidence toward a legal theory of the case and strategy for the targeted outcome during hearings, negotiations, or trials. Defense attorneys worked primarily alone; digital forensic analysts and investigators came into play only during the rare event of a trial to testify about the assistance they had provided on the case. I found that, although there were certain objective, damning types of digital evidence that were recognized as such by both the prosecution and the defense, most of the time, defenders and prosecutors worked with gray digital evidence that was open to different interpretations. Here, both sides formulated opposing moral arguments about the defendant: the prosecution drew on preexisting stereotypes of criminals to paint defendants as dangerous or otherwise unsavory, and the defense challenged those assumptions by pointing to socially desirable behaviors in the defendant, such as good school attendance. Peripheral applications of gray digital evidence could have severe consequences for defendants, including more severe sentences and pre-trial incarceration. Yet, I also found that defenders were able to leverage gray evidence, such as photos and text messages, to secure better deals for their clients during plea negotiations.

Broader Implications

In the digital turn, the breadth and persistence of digital evidence brings judicial actors into contact with increasingly personal aspects of defendants' lives. This shift raises important questions about the relationship between digital evidence, the law, and the marginalized groups who are overrepresented in the court system. Technology optimists, who are proponents of the digital turn, see the access to large amounts of information as an opportunity to gather data for investigations, make police work faster and more effective, and strengthen the prosecution's case (Dean, 2013; Trottier, 2012). Proponents emphasize the system benefits of the digital turn, and see the abundance of information available from personal, digital media as a positive development in the criminal justice system. To them, the exposure of personal information to judicial actors is justified by the added benefits to law enforcement's investigative work. Findings from my research, however, lend further credence to the concerns raised by civil rights activists and scholars about the intrusiveness of digital evidence and the racial biases in the ways such evidence is used against indigent defendants (Joh, 2018; Mateescu et al., 2015). Although I found that public defenders were able to draw on digital evidence to engage in nuanced legal storytelling on behalf of their clients, sometimes even securing dismissals or courtroom acquittals, more often than not, defenders faced cases where digital evidence hurt their clients, either by “killing” cases or by being used to make harmful, moral arguments. In the latter scenario, the prosecution interpreted digital evidence to present defendants as morally bad. They engaged in moralizing, that is, they judged the decisions, actions, and self-presentation of defendants as being wrong and/or of poor taste based on subjective standards of right and wrong.

My research indicates that, in the digital turn, there is a growing emphasis on understanding people and events through their digital traces. Yet making sense of persons and alleged crimes based on these pieces of evidence can be highly problematic. Digital evidence, whether in the form of photos, conversation records, or even location information, only paints a partial picture of the circumstances, and when re-interpreted in the judicial context, loses important contextual meaning (Nissenbaum, 2010). My findings show that, as part of case processing, public defenders were confronted with gray forms of digital media which were used to make moral arguments about their clients as dangerous, threatening, or otherwise contemptible. The digital evidence used to make these arguments often came from social media. Compared to other forms of digital evidence, such as cell site location, for example, defenders found social media content to be much more ambiguous and open to interpretation. When presented outside of its original context, such evidence lent itself to moralizing. Pictures of poor, black defendants in baggy clothing, throwing up hand gestures, dancing to rap music, or holding what appeared to be a weapon were used to preemptively label them as criminals before a formal verdict had been reached in the case. Such prosecutorial understandings of indigent defendants draw on biased stereotypes about criminality and the cultural dynamics and community norms of poor, black urban neighborhoods (Lane, 2018; Stevens et al., 2017). This raises concerns about the ways in which the digital turn is perpetuating existing inequalities and racial biases through new tools of discrimination.

The prosecution's use of digital evidence to exercise preemptive judgements through moral arguments, indicates that the digital turn is furthering system-level discrimination against marginalized defendants. The balance of power in the applications of digital evidence tips heavily in favor of the DAs who selectively use defendants' online associations and self-presentations to control the legal narrative of the case and put forth an image of the defendant that fits their interpretation of the events. Public defenders attempt to combat these problematic applications of digital evidence with arguments about relevance and prejudice but are limited in their abilities to respond both, because they have fewer resources than the prosecutor's office, and because responding to moral arguments often risks exposing indigent clients to further scrutiny and privacy intrusions. The digital turn's perpetuation of inequality and bias is rooted in the fact that the adversarial criminal justice system does not operate on an equal playing field (Weiss, 2005; Wice, 2005). The prosecution's life cycle process benefits from better resources, more people, and more time than that of the defense. This structural difference also needs to be considered in discussions about different types of digital evidence. In my findings I note that some forms of digital evidence were recognized by both sides as objective and persuasive. Yet given their high caseloads and limited resources, it's possible that public defenders also folded more easily when faced with certain types of digital evidence. They may have been less willing to problematize face value objectivity or question possible technological limitations because of the resources and time investment needed for such efforts. This too is problematic, as research has shown (Garcia, 2016) that bias is now encoded in algorithms and software products, and that racism, sexism, and xenophobia permeate technology.

Limitations

In my ethnographic study of the digital turn in public defense, I observed the day-to-day work of attorneys, digital forensic analysts, and investigators. As part of these observations I was able to witness some interactions between indigent defendants and the staff of the Northeastern Defender Association, but I did not interview or otherwise directly seek out defendants. That is a limitation of this study. To reflect on how the digital turn has shaped the lives of the poor, black defendants represented by the public defenders, I had to rely on what attorneys and intermediary role specialists said about their clients. This has led to a bias in my study, because core moments in the life cycle of digital evidence, such as attorney-client meetings, are told exclusively from the perspective of attorneys. How attorneys spoke about their clients was tied to the moral judgments they had made about them and their personal data. Their accounts of the events and their clients' responses offer only one side of a two-person conversation. Future studies should consider asking defendants about their experiences with both objective and gray digital evidence during attorney-client interactions and inquire about how the presence of increasingly personal data is shaping their perception of public defenders. Since attorney-client privilege laws can make attorneys hesitant to discuss ongoing cases, future researchers might want to consider interviewing defendants after their cases have come to a close. A defendant-focused study would also be able to investigate more thoroughly the personal motivations behind defendants' uses of technologies, including decisions to delete or preserve content. This would provide insight into the psychological underpinnings of defendants' actions and help identify a potential feedback loop where defendants are reacting, through their own uses of technology, to how personal information is used as a tool of the criminal justice system.

By focusing on the life cycle of digital evidence in public defense, I also only examined one side of the criminal justice system. I did not look at how law enforcement and prosecutors gather and analyze digital evidence and what kinds of challenges and opportunities they face in the process. While much has been written about the appeal of digital evidence for prosecutors (Brunty & Helenek, 2013; Trottier, 2012), future studies might want to consider examining the processes behind digital evidence acquisition, analysis, and application on the prosecution's side.

Choosing the Northeastern Defender Association as my fieldsite was a mixed blessing. On the one hand, the newly created in-house digital forensics lab offered a unique opportunity to observe how public defenders and digital forensic analysts worked together to acquire, analyze, and apply digital evidence towards cases. On the other hand, the lab's uniqueness meant that the Northeastern Defender Association was not representative of other public defender offices in the United States. The vast majority of public defender offices don't have on-site help and must outsource their requests for assistance with digital evidence. This comes at an additional costs and might limit the extent to which other defenders are able to seek out digital evidence that could help their cases. Furthermore, other offices would also not benefit from the assistance provided by the lab during the analysis phase, when the digital forensic analysts play an important role in helping public defenders interpret technical aspects of digital evidence, such as cell site analysis or cell phone extraction reports. The acquisition, analysis, and application efforts I observed at the Northeastern Defender were likely a "best case scenario" situation, and this limits the generalizability of some of my findings.

Future Directions

One of the key findings of my dissertation is that the digital turn brings judicial actors into contact with increasingly personal parts of defendants' lives. Access to photos, text messages, and other personal content allows for the development of moral arguments which, more often than not, are harmful to the defendant's case and rely on unfair stereotypes of criminals. Although personal information enters cases through both the prosecution and the defense, most of the information overload of personal content from smartphones and social media comes from data given to the defense by the prosecution during discovery. In the discussion section of Chapter 6 about the application phase of the life cycle, I propose pushing back against the growing use of personal information by attacking the problem at the source, namely the overbroad search warrants through which such evidence is acquired. This is where my upcoming research efforts are headed.

I am currently collaborating with George, the supervisor of the digital forensics lab at the Northeastern Defender Association, on a project about overbroad search warrants. This new study has two goals: 1) to assess through a representative sample, how widespread overbroad search warrants are, and 2) to determine if there are any biases in the types of cases and technologies for which such overbroad requests are made. I have filed several requests under New York's Freedom of Information Law (FOIL) with the Manhattan's district attorney's (DA) office to compile a sampling frame of cases from which to request search warrant applications. In December 2018 I requested copies of all intake logs and chain of custody forms for digital devices either received by or analyzed by the DA's High Tech Analysis Unit/Computer Forensics Unit (the prosecution's digital forensics lab) between January 1, 2016 and July 31,

2016. In April 2019, I was granted access to 302 records. I am now in the process of reviewing these chain of custody forms to determine for which cases to request search warrant applications.

Although civil rights organizations, such as the ACLU, have challenged the legitimacy of overbroad search warrants under the argument that they violate 4th amendment rights, most notably, the right to be protected from unreasonable searches (Denney, 2018; Gershowitz, 2016), no study to date has examined how widespread this phenomenon really is or how overbroad searches might tie into existing biases and prejudices against marginalized people in the criminal justice system. Going beyond individual case studies and examining, via a representative sample, how privacy intrusions are linked to particular types of cases and certain technologies will provide additional insights into how mechanisms of inequality operate in the criminal justice system. In turn, this will better prepare public defenders to challenge future overbroad search warrants by helping them articulate why the warrants are unconstitutional.

A large-scale examination of search warrant applications may also yield new insights into technology literacy issues. It has been suggested that search warrants for digital evidence are overbroad, in part, because law enforcement does not know how to limit requests for digital content (Denney, 2018). The judges who sign off on these warrants may also not realize the extent of the access they are granting judicial actors. If the study reveals that search warrants are systematically overbroad and do not take into consideration technological capabilities to sort or limit digital data, then there is an argument to be made for digital literacy education in legal contexts to protect defendants and witnesses from unnecessary privacy intrusions.

Appendix A

Interview guide for attorneys

Thank you for spending time with me today. X suggested you as a research participant because of your recent case involving Z incident or client /your experience with cases that involve digital evidence. This is an open-ended interview. I have prepared a set of questions on the broad topic of digital evidence in criminal defense. Feel free to expand on any issues which you find particularly relevant.

1) X mentioned you recently had a case with a digital evidence component (refer to case/client/charge).
    - How did that case come to you and what was it about?
    - What role did technology-mediated communication play?
    - What surprised you about the role of mediated communication?
    - What was the outcome of the case?
2) Thinking back about other cases you worked on that included digital evidence, what communication platforms have you encountered in your cases? (Texting, Facebook, Instagram, Twitter, Snapchat, etc.).
    - Which ones do you encounter most often?
    - Why do you think this platform is popular/used often?
3) As part of my observations in the digital forensics lab, I’ve seen the analysts prepare reports about their findings. Often these reports include text messages, call logs, chats and other content pulled from a person’s communication history.
    - How do you interpret and evaluate these reports?

- What are some of the challenges you've encountered in making sense of these reports?
- What strategies do you use when communication is hard to interpret?

4) Thinking about digital evidence and your work as a defense attorney, how does content pulled from cell phones and social media help you understand your cases and your clients?
    - What unique insights do they provide?
    - How has digital evidence changed the way you work with clients/cases?
5) Thinking about digital evidence and cases that went to trial. How has digital evidence affected case outcomes?
    a. Do you have examples of digital evidence hurting your cases?
        i. How did you attempt to counteract the prosecution's use of digital evidence?
    b. Do you have examples of digital evidence helping your cases?
        i. What did digital evidence provide that helped your case?
6) Have you had any concerns/hesitations about using digital evidence in your cases?
7) What about concerns, if any, do you have about digital evidence being used against your cases (by the prosecution)?
8) In general, what do you see as the main opportunities and challenges of using digital evidence in criminal defense?

Demographic questions

1) How old you are?
2) How do you identify racially and/or ethnically?

Appendix B

Interview Guide for Investigators

Thank you for spending time with me today. X suggested you as a research participant because of your recent case involving Z incident or client /your experience with cases that involve digital evidence. This is an open-ended interview. I have prepared a set of questions on the broad topic of digital evidence in criminal defense. Feel free to expand on any issues which you find particularly relevant.

1) What are your work responsibilities as an investigator for defense attorneys?
2) X mentioned you recently had a case with a digital evidence component (refer to case/client/charge).
    - How did that case come to you and what was it about?
    - What role did technology-mediated communication play?
    - What surprised you about the role of technology-mediated communication?
    - What was the outcome of the case?
3) How do you use digital/mobile communication as part of your work?
    - What is the most common use?
    - How has digital/mediated communication changed the work you do as an investigator? (Helping? More difficult? Unique challenges?)
    - How much of your work happens in the field and how much happens online?
4) Can you guide me through an example of how you use digital/mobile communication to help an attorney (locate witness/find online video, etc.)?

5) Thinking back to other cases you worked on that included digital evidence, what communication platforms have you encountered? (Texting, Facebook, Instagram, Twitter, Snapchat, etc.).
    - Which ones do you encounter most often?
    - Why do you think this platform is popular/used often?
6) When you examine content from mobile/digital communication, how do you evaluate the communication/video?
    - What are some of the challenges you've encountered in making sense of digital/mobile communication?
    - What strategies do you use when communication is hard to interpret?
7) Have you had any concerns or hesitations about using social media/mobile communication as part of your investigative work?
8) In general, what do you see as the main opportunities and challenges of using digital evidence for investigative purposes?

Demographic questions

1) How old you are?
2) How do you identify racially and/or ethnically?

Appendix C

Cell Phone Extractions, Social Media Preservation, and Call Detail Records

Cell phone extractions. Smartphone extractions were the most common type of digital forensic work the analysts performed. Extractions could provide a wide range of data about a person's communications and habits, thanks to call logs, text messages, photos, videos, calendar events, chats, location information data, and sometimes also the contents of the applications installed on device (Sammons, 2014; Tassone, Martini, Choo, & Slay, 2013). As I observed the work of the analysts, I learned that there were different ways of extracting content from cell phones. The simplest way of acquiring content was through a manual extraction. This involved an analyst personally handling the phone and interacting with its buttons and applications to identify relevant content to be copied onto a separate device (Barmpatsalou, Damopoulos, Kambourakis, & Katos, 2013). Photographing the phone screen, either through a screenshot or with an external camera was one way to perform a manual extraction (Hannon, 2015). This extraction method, however, was prone to human error and time-consuming. I witnessed the analysts resorting to this technique only when the phones brought in were too old to be connected to either a computer or forensic extraction machine.

Most phone extractions were done using forensic tools and machines that communicated with the phone to extract relevant content. In the lab, analysts tended to conduct either logical or physical extractions using the Cellebrite Universal Forensic Extraction Device (UFED), which was a small portable machine that connected to cell phones via a USB cable. A logical extraction performed a bitwise copy of all files and directories and then output the extracted data in a readable format. It was named for its ability to make a copy of the logical storage objects of a cell phone (Tassone et al., 2013). This type of extraction was quite comprehensive but did not always succeed in recovering deleted files. Barmpatsalou et al. (2013) note that “information that is not practically deleted, but ‘disguised’ as available space for further overwriting within databases” may still be recovered with a logical extraction (p. 325). During my observations, I noted several instances when logical extractions recovered some deleted messages, especially on newer smartphones. Because of that, it was generally the go-to extraction method for the analysts.

If recovering deleted content were crucial, then a physical extraction was a better option. A physical extraction also created a bitwise copy, but with the added advantage of a higher likelihood of recovering deleted files and other data remnants (Barmpatsalou et al., 2013; Ogden, 2017). It made a copy of the entire physical storage of the phone (Ogden, 2017; Tassone et al., 2013). Beyond the need to access deleted content, the choice of extraction method was also influenced by the type of operating system, the presence of security mechanisms, and the condition of the device. When I was conducting my observations, the Cellebrite UFED machine did not yet allow ways to limit the extraction to content from only certain days. As such, the analysts typically copied the entirety of the phone and then, based on the case attorney’s guidelines, narrowed down the data to only certain types of files (e.g., messages) or only data from a certain time period (e.g., the day of the incident).

Social media preservation. Another core aspect of the lab’s digital forensic work revolved around preserving social media data. Typically, the social media content the analysts preserved belonged to the clients represented by attorneys in the office. However, on occasion, I also observed analysts preserve publicly available social media data that belonged to witnesses or co-defendants. That most of the social media preservation being done was for the defendants themselves greatly simplified the preservation process, because there were no legal barriers to obtaining the data. The analysts needed only the voluntary cooperation of the defendant. Most social media preservation efforts did not require clients to come into the lab; they could simply share their username and password via phone or email. Once the analysts were inside the client's account, they typically used site-supported, download tools to preserve the data or saved the content via screenshots. The most common, social media platform from which the analysts preserved content was Facebook, in particular Facebook videos and Facebook user pages. The process of downloading Facebook user pages was remarkably simple. Facebook has a built-in tool that allows any user to make a copy of his/her own page. I tried my hand at it, using my own account under Kelly's guidance. To save my Facebook user page, I followed these easy steps: select the drop down menu on the right, choose "settings," then "Your Facebook Information," and lastly, in the new menu, select the second item on the list called "Download a copy of your information to keep." At the time, Facebook gave the option of limiting the download by date range and offered various file formats.

It was difficult to obtain non-public, social media records from witnesses or others involved in a case. To get such data, the public defenders would typically have to subpoena the social media companies directly. However, under the Stored Communications Act, social media companies and Internet providers are not obligated to share what is considered content (e.g., written communications or photos) with non-government entities, even when served with a valid subpoena. This often limits public defenders to requesting non-content data, such as log-in times and IP addresses, which tend to be of lower value because they are less rich in information. During my fieldwork, I heard twice from public defenders who were unsuccessful in obtaining from social media companies content about witnesses or co-defendants.

Call detail records and cell site analysis. Outside of performing an extraction, an additional way to access data about a person's cell phone activities was to subpoena the call detail records (CDRs) from cell phone carriers, such as AT&T, Verizon Wireless, and T-Mobile (Sammons, 2014). At the Northeastern Defender Association, the attorneys in charge of the case subpoenaed the records and then passed them along to the digital forensics lab for assistance. CDRs included details about the date and time of incoming and outgoing calls as well as information about who made the call, who was called, and how long the call lasted. They provided the same information for text messages. In addition, CDRs included the coordinates of the originating and terminating cell site towers for each call and text message (Sammons, 2014). Cell site tower information could be used to map the location of calls, thereby providing an estimate of where a person was at a given time. The analysts used this information regularly to map the location of several calls or texts over a period of time to show a defendant's trajectory (Sammons, 2014). This practice was known as cellular historical data reconstruction or cell site mapping. It's the task I observed Kelly and Sarah perform on my first day in the field.

References

ACLU. (2010). Cell phone company data retention chart. *ACLU*. Retrieved from https://www.aclu.org/cell-phone-location-tracking-request-response-cell-phone-company-data-retention-chart

Alexander, M. (2012). *The new Jim Crow*. New York, NY: The New Press.

Barmpatsalou, K., Damopoulos, D., Kambourakis, G., & Katos, V. (2013). A critical review of 7 years of mobile device forensics. *Digital Investigation, 10*(4), 323-349. doi:10.1016/j.diin.2013.10.003

Baruh, L., Secinti, E., & Cemalcilar, Z. (2017). Online privacy concerns and privacy management: A meta-analytical review. *Journal of Communication, 67*(1), 26-53. doi:10.1111/jcom.12276

Baym, N. (2015). *Personal connections in the digital age* (Second ed.). Malden, MA: Polity.

Bever, L., & Phillips, K. (2017). Texting suicide sentencing provides no closure, but victim's mother declares: 'We want to move on'. *Washington Post*. Retrieved from https://www.washingtonpost.com/news/true-crime/wp/2017/08/03/michelle-carter-whose-texts-pushed-her-boyfriend-to-suicide-to-be-sentenced-in-his-death/?utm_term=.65d9aa6f0ccc

Blankenship, K. M., del Rio Gonzalez, A. M., Keene, D. E., Groves, A. K., & Rosenberg, A. P. (2018). Mass incarceration, race inequality, and health: Expanding concepts and assessing impacts on well-being. *Social Science & Medicine, 215*, 45-52. doi:https://doi.org/10.1016/j.socscimed.2018.08.042

Bloss, W. (2007). Escalating U.S. police surveillance after 9/11: An examination of causes and effects. *Surveillance and Society, 4*(3), 208-228.

Blumberg, S., & Luke, J. (2018). Wireless substitution: Early release of estimates from the national health interview survey. *National Center for Health Statistics,* pp. 1-13. Retrieved from https://www.cdc.gov/nchs/data/nhis/earlyrelease/wireless201712.pdf

boyd, d. (2010). Social network sites as networked publics: Affordances, dynamics, and implications. In Z. Papacharissi (Ed.), *The networked self: Identity, community, and culture on social network sites* (pp. 39-58). New Haven, CT: Yale University Press.

Brayne, S. (2014). Surveillance and system avoidance: Criminal justice contact and institutional attachment. *American Sociological Review, 79*(3), 367-391. doi:10.1177/0003122414530398

Brown, W. S., & Palvia, P. (2015). Are mobile devices threatening your work-life balance? *International Journal of Mobile Communications, 13*(3), 317-338. doi:10.1504/IJMC.2015.069128

Browning, J. G. (2010). Digging for the digital dirt: Discovery and use of evidence from social media sites. *SMU Science and Technology Law Review, 14*(3), 465-496.

Brunson, R. K., & Miller, J. (2006a). Gender, race, and urban policing: The experience of African American youths. *Gender & Society, 20*(4), 531-552. doi:10.1177/0891243206287727

Brunson, R. K., & Miller, J. (2006b). Young black men and urban policing in the United States. *The British Journal of Criminology, 46*(4), 613-640. doi:10.1093/bjc/azi093

Brunty, J. (2016). Mobile device forensics: Threats, challenges, and future trends. In *digital forensics*.

Brunty, J., & Helenek, K. (2013). *Social media investigation for law enforcement.* London, UK: Routledge.

Cagle, M. (2016). *Facebook, Instagram, and Twitter provided data access for a surveillance product marketed to target activists of color*. Retrieved from https://www.aclunc.org/blog/facebook-instagram-and-twitter-provided-data-access-surveillance-product-marketed-target

Carlson, S. (2015). When is a tweet not an admissible tweet: Closing the authentication gap in the federal rules of evidence *University of Pennsylvania Law Review, 164*(4), 1033-1065.

Casey, E. (2011). *Digital evidence and computer crime: Forensic science, computers, and the Internet.* (3rd ed.). Waltham, MA: Academic Press.

Casper, J. D. (1972). *American criminal justice: The defendant's perspective.* Englewood Cliffs, NJ: Prentice-Hall.

Charmaz, K. (2014). *Constructing grounded theory* (2nd ed.). Thousand Oaks, CA: Sage

Chernyshev, M., Zeadally, S., Baig, Z., & Woodward, A. (2017). Mobile forensics: Advances, challenges, and research opportunities. *IEEE Security & Privacy, 15*(6), 42-51. doi:10.1109/MSP.2017.4251107

Child, J. T., Haridakis, P. M., & Petronio, S. (2012). Blogging privacy rule orientations, privacy management, and content deletion practices: The variability of online privacy management activity at different stages of social media use. *Computers in Human Behavior, 28*, 1859-1872. doi:10.1016/j.chb.2012.05.004

Christian, J., & Kennedy, L. W. (2011). Secondary narratives in the aftermath of crime: Defining family members' relationships with prisoners. *Punishment & Society, 13*(4), 379-402. doi:10.1177/1462474511414781

Christian, J., Martinez, D., & Martinez, D. (2015). Beyond the shadows of the prison: Agency and resilience among prisoners' family members. In J. Arditti & T. l. Roux (Eds.), *And justice for all: Families and the criminal justice system* (pp. 59-84). Ann Arbor, MI: University of Michigan Press.

Clayton, R. B., Leshner, G., & Almond, A. (2015). The extended iSelf: The impact of iPhone separation on cognition, emotion, and physiology. *Journal of Computer-Mediated Communication, 20*, 119-135. doi:https://doi.org/10.1111/jcc4.12109

Comfort, M. (2008). *Doing time together: Love and family in the shadow of the prison*. Chicago, IL: University of Chicago Press.

Davis, K. (2007). *Defending the damned: Inside a dark corner of the criminal justice system*. New York, NY: Atria Books.

Dean, M. (2013). Authenticating social media in evidentiary proceedings *Criminal Justice, 28*(49), 1-4.

Delgado, R., & Stefancic, J. (2012). *Critical race theory* (2nd ed.). New York, NY: New York University Press.

Denney, A. (2018). Judge urges action to curb 'overbroad' digital search warrants. *New York Law Journal*. Retrieved from https://www.law.com/newyorklawjournal/sites/newyorklawjournal/2018/01/24/judge-urges-action-to-curb-overbroad-digital-search-warrants/

Desmond, M., Papachristos, A. V., & Kirk, D. S. (2016). Police violence and citizen crime reporting in the black community. *American Sociological Review, 81*(5), 857-876. doi:10.1177/0003122416663494

Dickinson, E. (2012). Addressing environmental racism through storytelling: Toward an environmental justice narrative framework. *Communication, Culture & Critique, 5*(1), 57-74. doi:10.1111/j.1753-9137.2012.01119.x

Dixon, T. L., Schell, T. L., Giles, H., & Drogos, K. L. (2008). The influence of race in police-civilian interactions: A content analysis of videotaped interactions taken during Cincinnati police traffic stops. *Journal of Communication, 58*(3), 530-549. doi:10.1111/j.1460-2466.2008.00398.x

Ellison, N. B., Gibbs, J. L., & Weber, M. S. (2015). The use of enterprise social network sites for knowledge sharing in distributed organizations: The role of organizational affordances. *American Behavioral Scientist, 59*(1), 103-123.

Elm, D. L., & Dellinger, R. S. (2013). Dismantling Gideon's legacy: Sequestration's impact on public defender services. *The Federal Lawyer, 60*(6), 11.

Emerson, R., Fretz, R., & Shaw, L. (2011). *Writing ethnographic fieldnotes* (2nd ed.). Chicago, IL: University of Chicago Press.

Fagan, J. (2008). Punishment, deterrence and social control: The paradox of punishment in minority communities. *Ohio State journal of criminal law, 6*, 173-229.

Fajans, E., & Falk, M. (2009). Untold stories: Restoring narrative to pleading practice. *The Journal of the Legal Writing Institute, 15*(3), 3-65.

Farole, D., & Langton, L. (2010). A national assessment of public defender office caseloads. *Judicature, 94*(2), 87-90.

Farrell, H. (2018, May 30). The FBI blunder on phone encryption, explained. *The Washington Post*. Retrieved from https://www.washingtonpost.com/news/monkey-cage/wp/2018/05/30/the-fbi-blunder-on-phone-encryption-explained/?noredirect=on&utm_term=.4de1bb9da566

Feige, D. (2001). How to defend someone you know is guilty. *The New York Times*. Retrieved from https://www.nytimes.com/2001/04/08/magazine/how-to-defend-someone-you-know-is-guilty.html

Fernandez, M. (2010). Crime blotter has a regular: Yankees caps. *New York Times*. Retrieved from https://www.nytimes.com/2010/09/16/nyregion/16caps.html

Fontecilla, A. (2013). Ascendance of social media as evidence. *Criminal Justice, 28*(1), 55-57.

Forgays, D. K., Hyman, I., & Schreiber, J. (2014). Texting everywhere for everything: Gender and age differences in cell phone etiquette and use. *Computers in Human Behavior, 31*, 314-321. doi:10.1016/j.chb.2013.10.053

Funtasz, J. (2012). Canadian middle manager experience with mobile email technologies. *Information, Communication & Society, 15*(8), 1217-1235. doi:10.1080/1369118X.2011.614627

Garcia, M. (2016). Racist in the machine: The disturbing implications of algorithmic bias. . *World Policy Journal, 33*(4), 111. doi:10.1215/07402775-3813015

Gershowitz, A. M. (2016). The post-Riley search warrant: Search protocols and particularity in cell phone searches. *Vanderbilt Law Review, 69*(3), 585-612.

Goodison, S., Davis, R., & Jackson, B. (2015). Digital evidence and the U.S. criminal justice system. *Rand Corporation*. Retrieved from https://www.rand.org/pubs/research_reports/RR890.html

Grimm, P. W. (2014). Authenticating digital evidence. *GPSolo, 31*(5), 47-49.

Grosdidier, P. (2016). Authenticating: Can Cellphone Text Messages Stand up in Court null [notes]. In (pp. 278).

Häkkilä, J., & Chatfield, C. (2005). *'It's like if you opened someone else's letter': User perceived privacy and social practices with SMS communication.* Paper presented at the 7th International Conference on Human Computer Interaction with Mobile Devices & Services, Salzburg, Austria.

Hampton, K. (2016). Persistent and pervasive community: New communication technologies and the future of community. *American Behavioral Scientist, 60*(1), 101-124. doi:10.1177/0002764215601714

Hampton, K., Goulet, L. S., & Albanesius, G. (2015). Change in the social life of urban public spaces: The rise of mobile phones and women, and the decline of aloneness over 30 years. *Urban Studies, 52*(8), 1489-1504. doi:http://usj.sagepub.com/content/by/year

Hannon, M. J. (2015). Evidence authentication in a digital world--Part I. *Computer & Internet Lawyer, 32*(10), 10-25.

Hans, V. P., & Eisenberg, T. (2011). The predictability of juries. *DePaul Law Review, 60*(2), 375-396.

Hara, N. (2009). *Communities of practice: Fostering peer-to-peer learning and informal knowledge sharing in the work place*. Berlin, Germany: Springer.

Hargittai, E., & Marwick, A. (2016). "What can I really do?" Explaining the privacy paradox with online apathy.(Report). *International journal of communication (Online)*, 3737.

Hermida, A., & Hernández-Santaolalla, V. (2018). Twitter and video activism as tools for counter-surveillance: the case of social protests in Spain. *Information, Communication & Society, 21*(3), 416-433. doi:10.1080/1369118X.2017.1284880

Hirst, M. (2011). Hearsay, confessions and mobile telephones. *Journal of Criminal Law, 75*(6), 482-502.

Hoffmeister, T. (2014). *Social media in the courtroom: A new era for criminal justice?* Santa Barbara, CA: Praeger.

Hofmann, M., Selbst, A., & Data & Society Research Institute. (2017). Brief of amici curiae in support of petitioner in Carpenter v. United States of America. *Data & Society,* pp. 1-39. Retrieved from https://www.scotusblog.com/wp-content/uploads/2017/08/16-402-tsac-data-.pdf

Holte, A., & Ferraro, F. (2018). Tethered to texting: Reliance on texting and emotional attachment to cell phones. *Current Psychology*, 1-8. doi:10.1007/s12144-018-0037-y

Humphreys, L., Von Pape, T., & Karnowski, V. (2013). Evolving Mobile Media: Uses and Conceptualizations of the Mobile Internet. *Journal of Computer-Mediated Communication, 18*(4), 491-507. doi:10.1111/jcc4.12019

Joh, E. E. (2016). The new surveillance discretion: automated suspicion, big data, and policing. *Harvard Law & Policy Review, 10*(1), 15-42.

Joh, E. E. (2018). Automated policing. *Ohio State journal of criminal law, 15*(2), 559-563.

Keenan, V. M., Diedrich, D., & Martin, B. (2013). Developing policy on using social media for intelligence and investigations. *The Police Chief, 80*(6), 28-30.

Kirk, D. S., & Matsuda, M. (2011). Legal cynicism, collective efficacy, and the ecology of arrest. *Criminology, 49*(2), 443. doi:10.1111/j.1745-9125.2011.00226.x

Kirk, D. S., & Papachristos, A. V. (2011). Cultural Mechanisms and the Persistence of Neighborhood Violence 1. *American Journal of Sociology, 116*(4), 1190-1233. doi:10.1086/655754

Konok, V., Gigler, D., Bereczky, B. M., & Miklósi, Á. (2016). Humans' attachment to their mobile phones and its relationship with interpersonal attachment style. *Computers in Human Behavior, 61*, 537-547. doi:10.1016/j.chb.2016.03.062

Krathwohl, D. (2009). *Methods of educational and social science research* (3rd ed.). Long Grove, IL: Waveland Press.

Kunen, J. S. (1983). *"How can you defend those people?" The making of a criminal lawyer.* New York, NY: McGraw-Hill.

Laliker, M. K., & Lannutti, P. J. (2014). Remapping the topography of couples' daily interactions: Electronic messages. *Communication Research Reports, 31*(3), 262-271. doi:10.1080/08824096.2014.924336

Lane, J. (2018). *The digital street*. New York, NY: Oxford University Press.

Lane, J., Ramirez, F. A., & Pearce, K. E. (2018). Guilty by visible association: Socially mediated visibility in gang prosecutions. *Journal of Computer-Mediated Communication, 23*(6), 354-369. doi:10.1093/jcmc/zmy019

Lang, C., & Barton, H. (2015). Just untag it: Exploring the management of undesirable Facebook photos. *Computers in Human Behavior, 43*, 147-155. doi:10.1016/j.chb.2014.10.051

LeBlanc, P. (2017). The text messages that led up to teen's suicide. *CNN*. Retrieved from https://www.cnn.com/2017/06/08/us/text-message-suicide-michelle-carter-conrad-roy/index.html

Liang, H., & Fu, K. w. (2017). Information overload, similarity, and redundancy: Unsubscribing information sources on twitter. *Journal of Computer-Mediated Communication, 22*(1), 1-17. doi:10.1111/jcc4.12178

Lieberman, D., & Kirshner, I. (2019). Take off the blindfold: Reform and NY discovery law. *ACLU*. Retrieved from https://www.nyclu.org/en/publications/take-blindfold-reform-ny-discovery-law-commentary

Ling, R. (2012). *Taken for grantedness: The embedding of mobile communication in society.* Cambridge, MA: MIT Press.

Liptak, A. (2014). Major ruling hields privacy of cellphones. *The New York Times*. Retrieved from https://www.nytimes.com/2014/06/26/us/supreme-court-cellphones-search-privacy.html

Lu, K. (2017). Growth in mobile news use driven by older adults. *Pew Research Center*. Retrieved from http://www.pewresearch.org/fact-tank/2017/06/12/growth-in-mobile-news-use-driven-by-older-adults/

Luo, J. (2019). Public defense and rebellious lawyering. *Confluence*. Retrieved from https://confluence.gallatin.nyu.edu/context/independent-project/public-defense-and-rebellious-lawyering

Marwick, A., Fontaine, C., & boyd, D. (2017). "Nobody sees it, nobody gets mad": Social media, privacy, and personal responsibility among low-SES youth. *Social Media + Society, 3*(2). doi:10.1177/2056305117710455

Mateescu, A., Brunton, D., Rosenblat, A., Patton, D., Gold, Z., & boyd, D. (2015). Social media surveillance and law enforcement. *Data & civil rights*. Retrieved from http://www.datacivilrights.org/pubs/2015-1027/Social_Media_Surveillance_and_Law_Enforcement.pdf

Matsaki, L. (2018). The Supreme Court just greatly strengthened digital privacy. *Wired*. Retrieved from https://www.wired.com/story/carpenter-v-united-states-supreme-court-digital-privacy/

Murphy, J. P., & Fontecilla, A. (2012). Social media evidence in government investigations and criminal proceedings: A frontier of new legal issues. *Richmond Journal of Law & Technology, 19*(3), 1-30.

Murray, J. (2005). The effects of imprisonmnet on families and children of prisoners. In A. Liebling & S. Maruna (Eds.), *The effects of imprisonment* (pp. 442-492). Cullompton, UK: Willan.

National Institute of Justice. (2016). Digital evidence and forensics. Retrieved from https://www.nij.gov/topics/forensics/evidence/digital/Pages/welcome.aspx

Nelson, S. D., & Simek, J. W. (2014). Preserving, harvesting, and authenticating social media evidence *Judges Journal, 53*(4), 26-29.

Nissenbaum, H. (2010). *Privacy in context : technology, policy, and the integrity of social life*

Standford, CA: Stanford University Press.

Ogden, D. (2017). *Mobile device forensics: Beyond call logs and text messages* Retrieved from U S Attorneys' Bulletin: Washington, DC: https://www.justice.gov/usao/page/file/931366/download

Oliver, M. (2003). African American men as "criminal and dangerous": Implications of media portrayals of crime on the "criminalization" of African American men. *Journal of African American Studies, 7*(2), 3-18. doi:10.1007/s12111-003-1006-5

Pager, D. (2007). *Marked: Race, crime, and finding work in an era of mass incarceration*. Chicago, IL: University of Chicago Press.

Park, N., Chung, J. E., & Lee, S. (2012). Explaining the use of text-based communication media: An examination of three theories of media use. *CyberPsychology, Behavior & Social Networking, 15*(7), 357-363. doi:10.1089/cyber.2012.0121

Park, N., Lee, S., & Chung, J. E. (2016). Uses of cellphone texting: An integration of motivations, usage patterns, and psychological outcomes. *Computers in Human Behavior, 62*, 712-719. doi:10.1016/j.chb.2016.04.041

Parker, C. E., & Swearingen, T. B. (2012). Tweet me your status: Social media in discovery and at trial. *The Federal Lawyer, January/February* 34-53.

Patton, D. U., Brunton, D.-W., Dixon, A., Miller, R. J., Leonard, P., & Hackman, R. (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), 1-10.

Patton, D. U., Eschmann, R. D., & Butler, D. A. (2013). Internet banging: New trends in social media, gang violence, masculinity and hip hop. *Computers in Human Behavior, 29*(5), A54-A59. doi:10.1016/j.chb.2012.12.035

Patton, D. U., Leonard, P., Cahill, L., Macbeth, J., Crosby, S., & Brunton, D. W. (2016). "Police took my homie I dedicate my life 2 his revenge": Twitter tensions between gang-involved youth and police in Chicago. *Journal of Human Behavior in the Social Environment, 26*(3-4), 310-324. doi:10.1080/10911359.2015.1127738

Patton, D. U., Leonard, P., Lane, J., Macbeth, J., & Smith Lee, J. R. (2016). Gang violence on the digital street: Case study of a South Side Chicago gang member's Twitter communication. *New Media and Society, 19*(7), 1000-1018. doi:10.1177/1461444815625949

Pendleton, A. (2013). Admissibility of electronic evidence: A new evidentiary frontier article. *Bench and Bar of Minnesota*. Retrieved from http://mnbenchbar.com/2013/10/admissibility-of-electronic-evidence/

Petronio, S., & Sargent, J. (2011). Disclosure predicaments arising during the course of patient care: Nurses' privacy management. *Health Communication, 26*(3), 255-266. doi:10.1080/10410236.2010.549812

Pew Research Center. (2018). Mobile fact sheet. *Pew Research Center*. Retrieved from http://www.pewinternet.org/fact-sheet/mobile/

Phillips, L., Reddick-Morgan, K., & Stephens, D. P. (2005). Oppositional consciousness within an oppositional realm: The case of feminism and womanism in Rap and Hip Hop, 1976-2004. *The Journal of African American History, 90*(3), 253-277. doi:10.1086/JAAHv90n3p253

Purcell, K., Entner, R., & Henderson, N. (2010). *The rise of apps culture*. Retrieved from http://www.pewinternet.org/2010/09/14/the-rise-of-apps-culture/

Qihao, J. I., Sypher, U., & Ha, L. (2014). The role of news media use and demographic characteristics in the prediction of information overload. *International Journal of Communication (19328036), 8*, 699-714.

Quick, D., & Choo, K.-K. R. (2017). Pervasive social networking forensics: Intelligence and evidence from mobile device extracts. *Journal of Network and Computer Applications, 86*, 24-33. doi:10.1016/j.jnca.2016.11.018

Rabuy, B., & Kopf, D. (2016). Detaining the Poor: How money bail perpetuates an endless cycle of poverty and jail time. *PrisonPolicy*. Retrieved from https://www.prisonpolicy.org/reports/incomejails.html

Rainie, L., & Perrin, A. (2017). 10 facts about smartphones as the iPhone turns 10. *Pew Research Center*. Retrieved from http://www.pewresearch.org/fact-tank/2017/06/28/10-facts-about-smartphones/

Ramirez Jr, A., Dimmick, J., Feaster, J., & Lin, S. F. (2008). Revisiting interpersonal media competition: The gratification niches of instant messaging, e-mail, and the telephone. *Communication Research, 35*(4), 529-547. doi:10.1177/0093650208315979

Renter, E. (2010). How the broken public defense system exarcebates racial disparities. *The Huffington Post*. Retrieved from https://www.huffingtonpost.com/elizabeth-renter/how-the-broken-public-def_b_738305.html

Rideout, C. (2015). Applied legal storytelling: A bibliography. *Legal Communication and Rhetoric, 12*, 247-264.

Sammons, J. (2014). *The basics of digital forensics: The primer for getting started in digital forensics*. Waltham, MA: Syngress.

Sanders, C. B., & Hannem, S. (2012). Policing 'the risky': Technology and surveillance in everyday patrol work. *Canadian Review of Sociology, 49*(4), 389-410. doi:10.1111/j.1755-618X.2012.01300.x

Schutt, R. (2012). *Investigating the social world*. Thousand Oaks, CA: Sage.

Schwartzapfel, B. (2019). 'Blindfold' off: New York state overhauls discovery laws. *American Bar Association Journal*. Retrieved from http://www.abajournal.com/news/article/new-york-overhauls-pretrial-evidence-rules

Seigfried-Spellar, K. C., & Leshney, S. C. (2016). The intersection between social media, crime, and digital forensics: #WhoDonIt? In J. Sammons (Ed.), *Digital forensics: Threatscape and best practices* (pp. 59-66). Boston, MA: Elsevier.

Sholl, E. W. (2013). Exhibit Facebook: The discoverability and admissibility of social media evidence. *Tulane Journal of Technology and Intellectual Property*, 207-230.

Silver, A., & Matthews, L. (2017). The use of Facebook for information seeking, decision support, and self-organization following a significant disaster. *Information, Communication & Society, 20*(11), 1680-1697. doi:10.1080/1369118X.2016.1253762

Smiley, C. (2015). From silence to propagation: Understanding the relationship between "Stop Snitchin" and "YOLO". . *Deviant Behavior, 36*(1), 1-16.

Smith, A. (1995). Carrying on in criminal court: when criminal defense is not so sexy and other grievances. *Clinical Law Review, 1*(3), 723-747.

Smith, A. (2015). *U.S. Smartphone Use in 2015*. Retrieved from http://www.pewinternet.org/2015/04/01/us-smartphone-use-in-2015/

Sterling, G. (2016). Nearly 80 percent of social media time now spent on mobile devices. *Marketing Land*. Retrieved from https://marketingland.com/facebook-usage-accounts-1-5-minutes-spent-mobile-171561

Stevens, R., Brawner, B. M., Gilliard-Matthews, S., Dunaev, J., & Woods, M. K. (2017). The digital hood: Social media use among youth in disadvantaged neighborhoods. *New Media and Society, 19*(6), 950-967. doi:10.1177/1461444815625941

Stevenson, B. (2014). *Just mercy: A story of justice and redemption*. New York, NY: Spiegel & Grau.

Stuart, F. (2011). Constructing police abuse after Rodney King: How Skid Row residents and the Los Angeles police department contest video evidence. *Law & Social Inquiry, 36*(2), 327. doi:10.1111/j.1747-4469.2011.01234.x

Stuart, F., Armenta, A., & Osborne, M. (2015). Legal control of marginal groups. *Annual Review of Law and Social Science, 11*(1), 235-254. doi:10.1146/annurev-lawsocsci-120814-121433

Tassone, C., Martini, B., Choo, K. K. R., & Slay, J. (2013). Mobile device forensics: A snapshot. *Australian Institute of Criminology,* pp. 1-7. Retrieved from https://aic.gov.au/publications/tandi/tandi460

Taylor, M. (2016). New York City opens its $10 million cybercrime lab. *Forensic Magazine*.

Tracy, S. (2013). *Qualitative research methods: Collecting evidence, crafting analysis, communicating impact*. Malden, MA: Wiley-Blackwell.

Treem, J. W., & Leonardi, P. M. (2012). Social media use in organizations. *Communication Yearbook, 36*(1), 143-189.

Trottier, D. (2012). Policing social media. *Canadian Review of Sociology, 49*(4), 411-425. doi:10.1111/j.1755-618X.2012.01302.x

Tsetsi, E., & Rains, S. A. (2017). Smartphone Internet access and use: Extending the digital divide and usage gap. *Mobile Media & Communication, 5*(3), 239-255. doi:10.1177/2050157917708329

Turner, P., & Turner, S. (2013). Emotional and aesthetic attachment to digital artefacts. *Cognition, Technology & Work, 15*(4), 403-414. doi:10.1007/s10111-012-0231-x

Van Brunt, A. (2015). Poor people rely on public defenders who are too overworked to defend them. *The Guardian*. Retrieved from https://www.theguardian.com/commentisfree/2015/jun/17/poor-rely-public-defenders-too-overworked

Verbeek, P. C. (2015). Beyond interaction: a short introduction to mediation theory. *Interactions (ACM), 22*(3), 26-31. doi:https://doi.org/10.1145/2751314

Vincent, J. (2006). Emotional attachment and mobile phones. *Knowledge, Technology & Policy, 19*(1), 39-44. doi:10.1007/s12130-006-1013-7

Wacquant, L. (2001). Deadly symbiosis. *Punishment & Society, 3*(1), 95-133.

Wang, S. S., & Stefanone, M. A. (2013). Showing off? Human mobility and the interplay of traits, self-disclosure, and Facebook check-ins. *Social Science Computer Review, 31*(4), 437-457.

Watson, A. (2018, February 8 2018). Top challenges and changes in the use of digital forensic evidence. *Cellebrite*. Retrieved from https://www.cellebrite.com/en/blog/webinar-top-challenges-and-changes-in-the-use-of-digital-forensics-evidence/

Weiss, M. S. (2005). *Public defenders: Political motivations to represent the indigent*. New York, NY: LFB Scholarly Publishing.

Wice, P. B. (2005). *Public defenders and the American justice system*. Westport, CT: Praeger.

Wressler, N. F. (2018). The Supreme Court's groundbreaking privacy victory for the digital age. *ACLU*. Retrieved from https://www.aclu.org/blog/privacy-technology/location-tracking/supreme-courts-groundbreaking-privacy-victory-digital-age

Wright, K., & Webb, L. (2011). Preface. In K. Wright & L. Webb (Eds.), *Computer-mediated communication in personal relationships* New York, NY: Peter Lang.