Communication Privacy Management and Digital Evidence in an Intimate Partner Violence Case

FANNY A. RAMIREZ
Louisiana State University, USA

JEFFREY LANE
Rutgers University, USA

This article uses a case study of an intimate partner violence criminal case to examine the relationship among communication privacy management, evidence acquisition and retrieval, and the use of digital evidence in criminal court. We followed the case of Krista and Alex (pseudonyms) for a period of four months from August 2017 to November 2017. Data were collected from observations in two locations: the digital forensics laboratory of the public defender who handled the case and the courtroom in which the trial took place. Findings indicate that the couple engaged in preemptive and after-the-fact privacy management strategies, which complicated the process of acquiring digital evidence and had implications for how the evidence was used at trial. The case study joins communication privacy management and legal research to show why digital evidence falls short as a "model witness" and may expose female complainants to greater privacy turbulence than male defendants.

Keywords: electronic communication, intimate partner violence, privacy, digital evidence

Communication through information communication technologies (ICTs) has become a central component of close, personal relationships (Jin & Peña, 2010). Romantic partners rely on texts, calls, and social media messages to remain connected throughout the day (Laliker & Lannutti, 2014). Research has found that mobile phones, in particular, play a key role in day-to-day relationship maintenance (Hall & Baym, 2012). Exchanges that take place through ICTs are different from face-to-face communication in that they leave a record (Ling, 2012). This makes electronic communication a compelling source of evidence in criminal cases, in which it has been used to show criminal intent, associate defendants, and raise doubts about the credibility of witnesses (Boux & Daum, 2015; Sholl, 2013). In cases of intimate partner violence (IPV), police and prosecutors now routinely seek electronic communication to move forward with criminal charges (Haselschwerdt & Hardesty, 2017). If the case goes to trial, defense attorneys, judges, and jurors may also rely on these records (Powell, 2015). In fact, adjudicating actors increasingly privilege digital evidence ("information stored or transmitted in binary form that may be relied on in court") (National

Fanny A. Ramirez: ramirez1@lsu.edu
Jeffrey Lane: jeffrey.lane@rutgers.edu
Date submitted: 2018–12–12

Copyright © 2019 (Fanny A. Ramirez and Jeffrey Lane). Licensed under the Creative Commons Attribution Non-commercial No Derivatives (by-nc-nd). Available at http://ijoc.org.

Institute of Justice, 2016, para. 2) over the verbal statements of intimate partners According to Dodge (2017), this is because digital evidence is considered a "model witness" in IPV cases, which are often limited to he-said/she-said accounts.

Digital communication, however, is also subject to deletion, revision, and other alterations (boyd, 2010). These omissions and changes in the record limit the availability and reliability of digital evidence (Stratton, Powell, & Cameron, 2017). Using a study of an IPV case, we explain why digital evidence falls short as a model witness in IPV cases. We draw on communication privacy management (CPM) theory (Petronio, 2002) as a theoretical framework. We believe CPM helps legal scholars and judicial actors better understand how digital evidence may be biased by the decisions intimate partners make concerning disclosure and privacy. Couples engage in preemptive and after-the-fact communication strategies (Häkkilä & Chatfield, 2005; Wise & Rodriguez, 2013) to limit access to private information or reclaim ownership of information that has already been disclosed (Child, Haridakis, & Petronio, 2012; Lang & Barton, 2015). We argue that CPM practices shape what type of evidence can be discovered, admitted, and examined. Both personal practices (e.g., taking screenshots) and practices negotiated as a couple (e.g., choosing to communicate through ephemeral channels) influence the pool of potential evidence. Approaching IPV cases from a communication perspective helps make sense of how interpersonal factors limit the availability and reliability of digital evidence. In return, CPM theory also benefits from being applied in legal contexts. Partner violence is a prevalent aspect of intimacy. According to the Centers for Disease Control (2012), "more than 27% of women and 11% of men in the United States have experienced contact sexual violence, physical violence, and/or stalking by an intimate partner in their lifetime and experienced an intimate partner, violence-related impact" (para. 7). As part of our argument, we propose that IPV victims may be forced to choose privacy turbulence—the forfeiture and disruption of privacy rules and boundaries—as a legal recourse against their partners. In IPV cases, the victims/complainants, who are usually women, bear the brunt of their CPM practices (both those made individually and collectively as a couple) because the defendants, usually men, rarely take the stand. To seek justice, IPV victims must open themselves to scrutiny and answer for the communication history between both partners.

Literature Review

Communication Privacy Management

Electronic communication is deeply embedded in everyday interactions. Whether in the form of social media updates or text messages sent to a friend, individuals document their personal, social, and professional lives through electronic communication (Forgays, Hyman, & Schreiber, 2014; Wang & Stefanone, 2013). Research shows that individuals in a relationship use mobile phones more frequently than those who are single (Jin & Peña, 2010), and that couples use electronic communication to stay in touch during the day (Khunou, 2012). Content shared through ICTs addresses both the positive and unpleasant aspects of a couple's relationship. For some, electronic communication is an opportunity to share family photos and brag about restaurant visits and holiday trips (Wang & Stefanone, 2013). Yet, ICT use is also how couples deal with relationship conflict (Fox, Osborn, & Warber, 2014) and where they argue about a wide range of issues, from trivial decisions to social and political matters (Cionea, Piercy, & Carpenter, 2017).

When interacting with others, whether face-to-face or through electronic media, people make decisions about how much to disclose, to whom, and under what circumstances. These decisions are best understood in terms of the practices or strategies individuals develop around their communicative encounters. CPM theory provides a framework for making sense of the dual process of sharing and concealing information (Petronio, 2002, 2013). In the context of IPV, CPM has been used to examine how women manage the coercive control of abusive partners (e.g., Dutton & Goodman, 2005) in addition to the self-blame and social stigma of abuse by maintaining the secrecy of IPV until they decide to disclose the abuse for support or help (Haselschwerdt & Hardesty, 2017). We stipulate that CPM theory can be used to study not only the concealing and revealing of the abuse itself, but once they have been reinterpreted in the judicial context, to situate how CPM practices developed during and after a relationship become problematic. Specifically, we argue that practices, such as identity concealment and the use of ephemeral communication channels, could be used to raise doubts about the claims and postassault behavior of the victim.

Three main principles underscore CPM theory: privacy ownership, privacy control, and privacy turbulence (Child & Petronio, 2017; Petronio, 2002, 2013). Privacy ownership asserts that people own their private information and can decide to give others access, thereby creating information co-owners. Privacy control assumes that people develop and use privacy rules to manage the flow of private information. These privacy rule decisions are made on the basis of stable, core criteria tied to socialization, culture, and so forth, and also more event-specific, catalyst criteria that trigger rule changes. Privacy turbulence addresses the fact that privacy management systems can be disrupted and break down (Petronio, 2002, 2013). When breakdowns happen, individuals must deal with loss of privacy and may consider ways to reclaim ownership of shared information.

CPM has been used to examine communication in a range of digital contexts, including texting, blogging, and social media (Baruh, Secinti, & Cemalcilar, 2017; Child et al., 2012; Child, Petronio, Agyeman-Budu, & Westermann, 2011). Scholarship in this area shows that people engage in various preemptive and after-the-fact strategies to control electronic communication and deal with privacy turbulence. Preemptive strategies refer to decisions made before engaging in communication. The intent of preemptive strategies is to protect private information or limit its audience ahead of time (Häkkilä & Chatfield, 2005). One way to manage privacy preemptively is to select a mode of communication that others are less likely to intercept (Häkkilä & Chatfield, 2005; Worthington, Fitch-Hauser, Välikoski, Imhof, & Kim, 2012). Research on perceptions of mobile communication shows that text messages are believed to imply greater levels of privacy than spoken exchanges. This is because the content of text messages, unlike that of calls, is not susceptible to eavesdropping by bystanders and is assumed to be a personal exchange between sender and receiver (Worthington et al., 2012). In similar research, Ngcongo (2016) explains that couples develop rules about the content they feel is appropriate to share via electronic communication. For privacy purposes, some romantic partners choose not to discuss family issues and finances over the phone (Ngcongo, 2016). Partners in violent relationships may use different electronic communication channels to enact abuse and when communicating with each other (Dragiewicz et al., 2018).

Other studies of CPM and technology have found that users strategically engage in preemptive deception to manage privacy, such as representing information in a false manner, withholding information, or using unclear expressions (Child & Starcher, 2016; Wise & Rodriguez, 2013). Mobile phone users were found to explore punctuation and word choice when composing messages to create ambiguous meanings and deceive others (Wise & Rodriguez, 2013). Scholars have cited fears about lurking as a motive for strategically using unclear language on social media. Child and Starcher (2016) refer to this practice as "vague-booking" and note that concerns about lurking are correlated with higher levels of social media privacy management. Last, users may preempt the loss of privacy by adopting security practices, such as clearing their browsing history or turning off location tracking on a phone (Boyles, Smith, & Madden, 2012).

After-the-fact strategies refer to actions taken to reclaim ownership of information that has already been shared (Worthington et al., 2012). One popular strategy for managing privacy is to delete unwanted communication. In their research on blogging behavior, Child et al. (2012) found that bloggers react by deleting parts or the entirety of their blog entry when second-guessing their initial decision to disclose information in an online post. Deleting information that has been disclosed is a way to reclaim ownership of that information and reestablish a sense of privacy. To reclaim ownership of information disclosed by a co-owner of information, such as a tagged Facebook photo, individuals turn to various after-the-fact strategies, such as removing the tag from a photo, reporting a photo to Facebook, changing privacy settings, asking the uploader to remove a photo, and even unfriending the uploader (Lang & Barton, 2015).

Digital Evidence and Intimate Partner Violence Cases

Beyond the two parties involved in the incident, there are rarely any witnesses to acts of intimate partner violence (Boux & Daum, 2015). This is why IPV cases tend to operate on a he-said/she-said dynamic in which the complainant's version of the events is pitted against that of the defendant. Victims of IPV are also treated differently from victims of other crimes; they are often dismissed as liars or as exaggerating the extent of the assault (Boux & Daum, 2015). More than other victims, they depend on evidence—digital or physical—to support their statements. Research shows that IPV cases have a complex relationship with technologies and digital evidence. Some forms of digital evidence, most notably photographs of injuries, have helped bolster the testimonies of IPV victims (Powell, 2015). The adoption of digital photography by police departments in the late 1990s made it possible to better capture a victim's physical suffering; it was believed to offer "an accurate depiction of the event" (Garcia, 2003, p. 580). Even when victims are unable or unwilling to cooperate, photographs make it possible to mount prosecutions because the evidence works as a stand-in for the victim (Dodge, 2017). A comparison between IPV cases with digital photographic evidence and those without showed that digital evidence positively influenced case outcomes and led to more guilty pleas, higher conviction rates, and more severe sentences (Garcia, 2003).

Photographic evidence continues to be an influential prosecutorial tool in IPV and sexual assault cases. In 2012, the sexual assault case of a 16-year-old girl in Steubenville, Ohio, made the headlines because the aggressors took photographs of the assault and later shared those images among friends and on social media. Digital evidence played a key role in bringing the case to trial and obtaining a conviction (Oppel, 2013). Dodge (2017) states that in this particular case, "digital evidence was able to act as a model witness, providing extensive proof of the assaults, proof of the victim's incapacitated state and proof of the offenders' state of mind" (p. 4). The Steubenville case stands out because of the comprehensive amount of digital evidence that was available to the prosecution, and because vigilante supporters stepped in as intermediary help-seekers who spoke up for the victim (Wellman, Reddington, & Clark, 2017).

Digital evidence, however, is rarely so overwhelming, and can be used to attack the victim's case. In 2012 at a house party, several boys assaulted Rehtaeh Parsons. Despite the existence of a picture showing one of the boys appearing to sexually assault Parsons from behind, local law enforcement deemed there was not enough evidence to move forward with formal charges (MacDonald, 2015). The scene depicted in the photograph was considered unclear and open to alternative readings (Dodge, 2017). The decision not to proceed with sexual assault charges was also based on a series of messages exchanged between Parsons and her friends on the night of the assault. In those messages, the young woman expressed that she "did a stupid thing . . . that she made a mistake and regretted it" (Segal, 2015, p. 79). According to law enforcement officers, these messages indicated self-blame and, therefore, they contradicted her earlier statements to the police. Parsons' case illustrates how digital evidence can be used to cast doubt on a victim's reliability as a witness. Her communication after the fact did not conform to the socially accepted, postassault behavior of a victim, and criminal justice professionals used the messages to diminish her credibility (Boux & Daum, 2015; Dodge, 2017).

The different outcomes of the two cases just described highlight that digital evidence hardly speaks for itself, although court actors place high evidentiary value on electronic communication trails (Feigenson, 2014; Sherwin, 2012). Rather, law enforcement officials, prosecutors, and defense attorneys actively shape the meaning of text messages, Facebook posts, and other digital evidence from electronic conversations. Using this type of evidence to make assessments about the state of mind and credibility of victims is further complicated because unique linguistic norms that cannot be taken at face value govern online spaces. Dodge (2017) notes that "the use of mood indicators/emoticons and laughing indicators can be misleading as it is common for social media users to attempt to portray happier and more likable versions of themselves regardless of how they are feeling" (p. 14). Even so, social media evidence is increasingly used in a wide range of cases to make credibility claims. In divorce cases, for example, such evidence is regularly applied to establish character flaws and poor past decisions, such as infidelity and drunken behavior (Raybin & Raybin, 2011; Sholl, 2013).

Digital technologies may also serve as the locus of the crime itself. Weathers, Canzona, and Fisher (2019) note that smartphones and social media are used to enact controlling behaviors and verbal and psychological abuse, which are themselves sometimes criminal acts. Harris and Woodlock (2019) use the phrase "technology facilitated coercive control" to refer to the use of mobile devices and digital media to "stalk, harass, threaten, and abuse partners or ex-partners" (p. 533). In the context of IPV, partners also use electronic channels for nonaggressive communication. Victims communicate digitally with abusive partners or ex-partners as a mode of coping (Weathers et al., 2019) or for necessary practical purposes, such as child visitation (Davies, Ford-Gilboe, & Hammerton, 2009).

Privacy Management and Digital Evidence in Intimate Partner Violence Cases

Despite efforts to improve prosecution rates, intimate partner violence is often considered less serious than other forms of assault, and only a fraction of IPV cases make it to trial (Hartley, 2001). Low conviction rates are blamed on the he-said/she-said nature of these cases as well as issues concerning the complainant's credibility (Boux & Daum, 2015; Tuerkheimer, 2017). We use a case study of an IPV incident between Krista and Alex (pseudonyms) to examine why digital evidence falls short as a model witness, and draw on literature about the electronic communication habits of romantic partners, CPM theory, and the known challenges of using digital evidence in IPV cases. Our argument revolves around two core issues. First, we stipulate that a couple's CPM strategies shape what kind of evidence can be discovered, admitted, and examined as part of case processing. We address this with the following research questions:

RQ1: What CPM strategies were used by the defendant and the complainant?

RQ2: How did CPM strategies shape evidence acquisition and retrieval?

Second, because defendants—usually men—rarely take the stand, we believe that couples are not made to answer for their offline and online behaviors equally when the case is presented in court. We anticipated that the complainant (Krista) would be confronted about her CPM strategies and her pre- and postassault behaviors to a much greater degree than the defendant (Alex), which would lead to an unequal impact of CPM and digital evidence on Krista and Alex:

RQ3: How was digital evidence used and interpreted at trial? What roles did the CPM strategies of the defendant and the complainant play?

Method

Case Study Overview

The case study on which this article is based concerns the assault of a 19-year-old woman named Krista by her then 21-year-old boyfriend, Alex. Pseudonyms are used to protect the identity of the parties involved. The couple was attending a party when they began an argument, which became physical. As part of the altercation, Alex allegedly hit and strangled Krista. Alex was charged with two counts of strangulation—a felony—and two counts of assault in the third degree—a misdemeanor. The case went to trial in October 2017. Digital evidence was introduced at multiple points during Krista's testimony and cross-examination. Alex did not take the stand. The jurors spent two days deliberating, which suggests that the jury gave the case considerable thought. Ultimately, Alex was acquitted on the felony strangulation charges and one of the misdemeanor assault charges. Instead, he was convicted of two counts of criminal obstruction of breathing or blood circulation, which is a lesser strangulation charge and only a misdemeanor. He was also convicted of the assault charge misdemeanor. Alex was sentenced in November 2017 to eight months in jail. He was given a five-year order of protection, which prohibited him from going near Krista.

Data Collection

Data were collected through observations. The first author followed the developments of the case for a period of four months from August 2017 until the sentencing hearing in November 2017. Observations took place in two locations: the digital forensics laboratory of the office of the public defender, who represented Alex, and the courtroom where the trial took place.

The first author was conducting fieldwork in the digital forensics laboratory of the public defender office for a project on digital evidence in criminal cases when she learned about the case in question. Alex's attorney had come to the lab to request assistance with the digital evidence components of the case. Specifically, the attorney requested that an extraction be performed on Alex's phone. A phone extraction is a mobile forensics data-gathering technique used by digital forensic analysts to retrieve text messages, chats, call logs, and other electronic communication records. The attorney was particularly interested in recovering communications from the day of the assault, but requested that the analysts retrieve all available interactions between Alex and Krista. The attorney also shared with the lab a copy of Krista's call detail records (CDRs), which had been obtained from the mobile phone provider by the prosecutor's office. CDRs include information about the date and time of incoming and outgoing calls and text messages (Sammons, 2014). Alex's attorney told the analysts that, although her client had admitted to getting into a fight with his girlfriend, he was adamant that Krista had provoked him and had subsequently harassed him with phone calls. The defense attorney wanted to learn the truth of Alex's claim and gain a better understanding of the couple's relationship and the events that had transpired the night of the alleged assault. In the lab, Kelly, one of the analysts for the defender office, took on the case.

During observations, the first author watched as Kelly extracted data from Alex's phone and examined Krista's CDRs. The first author sat within view of Kelly's computer screen and carefully listened as she described her work process and thoughts on the case. As part of these observations, the first author took note of when Kelly encountered data recovery and sense-making challenges. For example, the first author observed that Kelly recovered previously deleted text messages, which were marked with a red *x* to indicate they had been deleted from the phone, but had been forensically recovered. The first author also observed how Kelly made sense of Krista's CDRs and discovered Krista's use of an identity concealment technique. During the trial, the first author observed proceedings from the rear of the courtroom. Data were collected in the form of handwritten field notes that were transcribed into longer, typed field notes within 36 hours of the field visit (Emerson, Fretz, & Shaw, 2011; Tracy, 2013). In total, four field visits to the digital forensics laboratory and one full day of courtroom observations yielded 10 pages of single-spaced, typed notes.

Data Analysis

The first author analyzed the typed field notes using an open coding approach. Coding took place in two phases. The first round of early coding involved reading the field notes line-by-line and describing and defining what was happening (Charmaz, 2014). A constant comparative method was applied to analyze the data for similarities and differences. In the second round of coding, the field notes were read again, and the most significant codes were used to "sort, synthesize, integrate, and organize" the entirety of the data (Charmaz, 2014, p. 113). During this process, disciplinary concepts and theories that intersected with the data were considered (Tracy, 2013). The existing literature on preemptive and after-the-fact strategies for managing communication in interpersonal relationships was of relevance for parts of the analysis. Thus, some of the codes were revised to align with established research on preemptive and after-the-fact CPM strategies.

Findings

Krista and Alex's CPM Strategies (RQ1)

The coding of the field notes showed that Krista and Alex had engaged on their smartphones in two preemptive and two after-the-fact CPM strategies. These strategies spanned different periods in their history as a couple, and some happened in the aftermath of the assault. The first author observed the lead digital forensic analyst, Kelly, gradually uncover these strategies over several weeks of data retrieval and examination. Later, the first author confirmed several of these strategies during trial observations. The preemptive strategies were ephemeral communication and identity concealment. The after-the-fact strategies were deletion and documentation.

Ephemeral Communication

The extraction performed on Alex's smartphone recovered only a handful of exchanges between him and Krista. According to the analyst, this was unexpected. Romantic couples typically share a long history of communication and, consequently, there should have been lengthy communication records on Alex's phone. On closer examination, the analyst noted that the application Snapchat had been installed on Alex's phone. After a call to Alex's attorney, the analyst confirmed that the couple had, indeed, used Snapchat for many of their conversations. The ephemerality of communication on Snapchat distinguishes this application from other social media applications. Messages, photos, and videos shared by Snapchat users are automatically deleted after the recipient has viewed them. Unless the other person has taken a screenshot, Snapchat exchanges are not stored for future viewing. During the trial, Krista confirmed that Snapchat was one of the ways they had communicated with each other both before and after the assault.

Identity Concealment

The examination of Krista's CDRs by the forensic analyst showed that she had repeatedly engaged in identity concealment by hiding her mobile phone number when attempting to contact Alex in the weeks and months following the attack. This was achieved by dialing *67 before calls to prevent the display of her caller identification on the receiver's phone. The CDRs showed that during a six-month period, Krista had called Alex a total of 1,349 times, and that 324 of those calls, or approximately 24% of the calls, had been dialed with *67.

Deletion

As noted earlier, the extraction performed on Alex's smartphone showed only a handful of exchanges between him and Krista. On closer examination, Kelly noted that several of the messages and call logs had been previously deleted. The system had marked these items with a red *x* to indicate their status as recovered information. No text messages between Krista and Alex were found for the night of the assault. Although smartphone extractions can recover some deleted content, in this instance, they were able to recover only a handful of text messages and call logs. In later interactions with Kelly, the first author learned that Alex had deleted his communications with Krista because he was married and did not want his wife to find out about the affair. In addition to deleted messages and call logs, the forensic examination also showed that, shortly after the assault, Alex had deleted Krista as a contact from his phone.

Documentation

As part of her examination of the extraction file, Kelly looked through the pictures retrieved from Alex's phone. While scrolling through the list of images, Kelly noticed that some of the images were not actually photographs, but screenshots of text messages. Thirty-two images of screenshots from Alex's phone were retrieved. The screenshots had been saved in an application called Keep Safe, a privacy application that allows users to store content in a protected space on their smartphones. In one of the screenshots, Alex stated that he was purposely saving these messages to document their arguments and Krista's state of mind. Some of the screenshots appeared to be from the night of the assault. Although no exact date was listed, based on the day at the top of the image and the content of the conversation, the lead analyst was fairly confident that the messages had been from the night of the assault. In the messages, Krista had written things, such as "Where are you?" "I love you," "Let's have a good night, baby," and "I'm downstairs. Please come here." Alex, however, had responded with a dismissive text. In addition to screenshots, the extraction performed on Alex's phone showed that he had saved eight voicemails from Krista, which she had left in the months after the assault. The analyst offered to play the voicemails for the first author. Most of them were short messages such as "I love you" or "It's Krista. Please call me back." In a voicemail dating from several weeks after the assault, Krista had asked Alex about "hanging out" after work. Last, Alex had also saved a social media video of Krista getting into a physical fight with a woman. The video showed Krista pushing and shoving another woman on a busy, downtown street at night. Kelly prepared an audio CD with the voicemails and a mobile forensics report that included the screenshots and other recovered data for Alex's attorney to potentially use at trial.

Later, during the trial, the first author learned that Krista, too, had taken screenshots of her conversations with Alex, including messages that documented the couple's arguments. Beyond keeping evidence of her conversations with Alex, Krista had also engaged in documentation by taking pictures of the injuries she had incurred at different times in their relationship. These pictures showed bruises and facial swelling, among other injuries.

The Impact of CPM Strategies on Evidence Retrieval (RQ2)

The use of CPM practices complicated the work of the digital forensic analysts in three ways. First, the use of ephemeral communication meant that some content was simply inaccessible. By choosing to communicate via Snapchat as a preemptive CPM strategy, Krista and Alex had made some of their exchanges unrecoverable. The only indication that the couple had communicated through ephemeral communication occurred because Alex had installed the application on his phone and Krista had admitted during trial that she had used the app.

Second, the use of deletion as a CPM practice meant that some content was only partially recoverable, leaving behind incomplete records. The extraction of Alex's phone revealed a few previously deleted text messages and call logs, but Krista's CDR indicated significantly more communication activity between the two. Although CDRs include information about the day, time, and length of phone calls between parties, they typically do not include the content of messages; consequently, the analysts and attorney had to rely on only partial records.

Third, the use of documentation can slow down the work of analysts because evidence gets stored in different formats or in different locations on the phone. This can lead to valuable information being overlooked or require additional examination steps. In Alex's case, the lead analyst, Kelly, discovered the screenshots because she had been scrolling through the pictures section of the extraction. If she had looked only for text messages, she may not have found the screenshots Alex had taken of his conversations with Krista.

CPM and Digital Evidence in the Courts (RQ3)

In court, the first author observed how digital evidence was used during Krista's testimony and cross-examination. Although both parties had engaged in preemptive and after-the-fact CPM strategies, because Alex did not take the stand, only Krista had to answer for the CPM decisions she had made personally and as part of a couple with Alex. The information collected from Alex's phone (voicemails, screenshots, etc.) was brought up only during Krista's cross-examination. Coding of the field notes revealed two different approaches to the use of communication records as digital evidence. The prosecution relied overwhelmingly on photographic evidence to ascertain the severity and truthfulness of Krista's injuries. In this instance, digital evidence appeared to serve the court as a model witness for the victim in corroboration of the victim's statements. The defense, on the other hand, drew on digital evidence to challenge Krista's claims and her reliability as a witness.

Digital Evidence and Prosecution Strategies

The prosecution presented to the jury numerous photographs of the injuries Krista had suffered the night of the assault, taking great care to describe how each injury had been acquired and how painful it had been. The photographs shown included the photos Krista had taken as well as photos taken when she formally pressed charges. One picture showed Krista with a swollen face and a cut on the bottom right of her lip. Another showed a bulging temple. A third photo showed dark bruising on her neck. To contextualize the photos, the prosecutor asked Krista to describe the assault and her pain level in relation to the various injuries. Krista explained that after they had gotten into a verbal argument, Alex had hit her, grabbed her neck, and then began choking her until she nearly lost consciousness. She responded to the question about her pain level by saying that the bruises on her neck were painful to the touch and that the cut on her lip made it difficult to eat and drink. Krista's documentation strategy played a key role in conveying the severity of her injuries and highlighted the potential of digital evidence to corroborate victim accounts. Following the testimony about her injuries, Krista explained that after the assault, she had become afraid of Alex and concerned that he would harm her again.

Digital Evidence and Defense Strategies

After her testimony, the defense cross-examined Krista. Alex's attorney used the couple's postassault communication history, specifically Krista's use of *67 to conceal her identity, to raise doubts about Krista’s alleged fear of Alex following the assault. As part of the cross-examination, the defense attorney brought out Krista’s CDRs and asked her whether she had reached out to Alex at a certain time on a given day. Krista simply responded, “Yes.” The attorney then repeated this process approximately 10 times, referencing different call logs; each time Krista admitted she had contacted Alex. On several occasions, Krista tried to change the direction of the cross-examination by saying that Alex had responded to her calls via Snapchat, but the defense attorney did not engage with her comment. Next, the defense attorney asked Krista whether she was familiar with the use of *67. Krista responded, “Yes.” Krista was then asked to describe why *67 is used. Krista explained that *67 is used to conceal one’s phone number when making calls, and that she had used this strategy when contacting Alex to circumvent the fact that he had blocked her number. The defense attorney then asked Krista whether it was true that she had made more than 1,000 calls to Alex in the months following the assault, many of which had been dialed with *67. As with the previous line of questioning, Krista responded with a simple “yes.”

After the questions about Krista’s phone calls, the defense attorney moved on to the voicemails Alex had saved on his phone. Again, Krista acknowledged that she had reached out to Alex in the weeks following the assault, including one instance in which she had asked him to meet after work. She made no mentions of Alex’s responses. Following the voicemail questions, the defense attorney turned to the social media video. Krista was asked whether she had been involved in physical altercations before her incident with Alex. Krista explained that some time before she had had an argument with a woman that had resulted in a fight. The defense attorney followed up by asking whether Krista knew that there was a Facebook video of the incident. Krista acknowledged the existence of the video. The attorney then asked Krista whether she had watched the video. Again, Krista responded that she had seen the video several times. This completed the digital evidence references of the cross-examination.

Discussion

This study examined how a couple’s CPM strategies shaped the acquisition of digital evidence and the ultimate use of that evidence at trial in an IPV case. Findings show that both the defendant and the complainant engaged in preemptive and after-the-fact strategies to control their communication, including ephemeral communication, identity concealment, deletion, and documentation. These strategies had complicated the work of the digital forensic analyst tasked with retrieving evidence because they made electronic communication unavailable, only partially recoverable, or more time-consuming to locate. We found that during trial, in the absence of testimony from Alex, only Krista was made to answer for their individual- and couple-level CPM strategies as well as pre- and postassault behavior.

The case of Krista and Alex reveals how CPM practices can generate both positive and negative impacts for IPV victims when they seek formal help from police and prosecutors. We discuss first how the CPM practice of documentation brought about a positive case outcome for Krista, and what this suggests about how women must manage the disclosure of abuse to access legal protection. Haselschwerdt and Hardesty (2017) describe a shift from managing the secrecy of abuse to the disclosure as an ongoing process for victims who may face embarrassment, retribution, and other risks. The major decision to confide in police, however, is not necessarily enough to receive formal, legal support. Whereas some officers may take verbal abuse allegations seriously enough to arrest abusers, other officers may act in an unresponsive or discouraging manner (Haselschwerdt & Hardesty, 2017) or may pressure women to document instances of abuse (Harris & Woodlock, 2019).

By photographing her injuries, Krista did the work she needed to be believed and taken seriously by police. When Krista took pictures of her previous injuries from another assault in the months prior to the party, she may have started to think about formal disclosure, but did not go to the police. When the severity of the violence escalated at the party, Krista again prepared for the possibility of disclosure by taking photographs of the new injuries and decided this time to report the assault with evidence in hand. When the prosecution ultimately presented photographs of Krista's injuries, this proved to be a powerful moment in the trial.

From a CPM perspective, being visibly marked by violence may change how victims think about disclosure. They now have an opportunity to counteract the limitations of he-said/she-said dynamics by collecting their own evidence of the assault. This window of opportunity to act is short because these marks may go away with time. Krista's readiness to formally disclose may have increased over multiple instances of being physically marked by violence, photographing these marks, and finally deciding she was ready to report and back up her claims. She may have sensed that pictures are generally seen as model, more reliable digital evidence that is less open to interpretation than other forms. The photos captured the extent of Krista's assault and corroborated her recounting of the events (Garcia, 2003). Unlike text messages or social media posts, judicial actors view injury photographs as more nearly objective evidence (Dodge, 2017). From a legal perspective, the burden of proof is on the prosecution, and victims may not come forward because they are worried about not being able to meet that burden. Here, we see that photo documentation can strengthen IPV prosecution and make victims more confident in their cases.

Next, we discuss how CPM practices may be reinterpreted in the judicial context in ways that undermine the credibility of IPV victims. At trial, Krista's identity concealment and repeated calls and voicemails to Alex were framed by the defense to imply that she was not fearful of Alex because she actively sought contact. The defense focused on how often Krista had called Alex (nearly 1,400 times over six months) and her calling method (using *67 to hide her caller ID). In the process, the defense reduced a complex CPM decision to portray Krista as cunning and relentless. The defense attorney's characterization of Krista served Alex. When defense attorneys go after complainants and witnesses, they consider this their obligation to provide the best defense possible and do not relish their behavior. Alex's attorney noted in a conversation with the first author that she did not want to attack a victim of IPV and hoped her cross-examination of Krista had not been perceived as too ruthless and would not backfire.

From an IPV perspective, Krista's behavior can be understood as a maladaptive coping strategy (Weathers et al., 2019). Victims of IPV often struggle to break free completely from their abusers (Hartley, 2001). The increased access of social media and mobile phone communication can make it still more difficult for women to separate from abusers (Halligan, Knox, & Brinkley, 2013; Woodlock, 2017). In our case study, Krista's calls and voicemails to Alex may be seen as an indication of feeling trapped in a coercive relationship. Halligan et al. (2013) note that abuse does not happen in isolation but is surrounded by positive behaviors and declarations of affection. Victims of IPV tend to hold on to these "sprinkles" of tenderness to cope with the assault. Krista's voicemails to Alex show her pleading with him and attempting to reconcile after the assault. These behaviors are indicative of how IPV victims, who may still harbor feelings for their abuser, struggle to break free from abusive relationships (Halligan et al., 2013).

The defense's references to Krista's CDRs suggested a mostly one-sided interaction, in which she was the one reaching out to her abuser. During the trial, Krista attempted to provide context by saying that Alex had returned her calls via Snapchat. The self-destruction of Snapchat content, however, meant that there was no way to verify the validity of her claims (Ganzenmuller, 2014). Ephemeral communication channels are appealing because they offer the allure of privacy (Waddell, 2016). A common assumption posits that content shared through such channels cannot come back to haunt the user. Yet, in Krista's case, there were repercussions for these missing records. Without Snapchat evidence, jurors had to weigh Krista's explanation of her calling behavior against the defense's interpretation, which was essentially the same dilemma posed by he-said/she-said. Hartley (2001) notes that "jurors may lack knowledge of or hold misconceptions about domestic abuse victims and thus find it difficult to understand the context of the victim's experience" (p. 512). For jurors unfamiliar with the psychological challenges of breaking free from an abusive relationship, it may be easier to accept the defense's interpretation of Krista's calling. From a CPM perspective, perhaps jurors struggled over the two days of deliberation to reconcile Krista's CPM practices with how they, personally, would have reacted in the aftermath of an assault.

The broader circumstances that motivated Krista's adoption of identity concealment and the couple's decision to use ephemeral communication channels were not thoroughly explored at trial. CPM theory argues that decisions to reveal or conceal information are based on a range of personal and situational criteria (Petronio, 2002). From the data, we can reasonably assume that Krista and Alex had mutually negotiated the use of Snapchat as a way to keep their relationship secret from Alex's wife, at least initially. This CPM practice was driven by the complicated situation of an affair. After the assault, Alex continued to use Snapchat, whereas Krista turned to other modes of contact. Yet, at trial, only Krista had to explain the couple's communication dynamics. Under his attorney's advisement, Alex did not take the stand, which would have exposed him to further scrutiny. Although rational from a legal perspective, the onus falls on IPV victims, such as Krista, to provide access to their abuse, open themselves up to privacy turbulence, and justify their postassault behavior. This can be a daunting task. Meanwhile, digital evidence not directly related to the case, such as the Facebook video, which showed Krista's involvement in a physical altercation, was referenced to further diminish her credibility. Victims of abuse may be reluctant to come forward for fear that their past poor decisions will be exposed during trial (Diss, 2013). Social media may make access to such prejudicial evidence easier and potentially pose an additional barrier to formal help-seeking for IPV victims.

Conclusion

This article used a case study of an intimate partner violence felony case to explore the relationship among communication privacy management, the acquisition and retrieval of electronic communication as digital evidence, and the use of digital evidence at trial. It highlights that the preemptive and after-the-fact privacy management strategies of both the complainant and the defendant had an impact on what kind of evidence could be recovered from electronic communication and how that evidence was ultimately used in the courts. Findings show that digital evidence often acts as an uncertain and ambivalent form of evidence in IPV cases. The analysis of Krista and Alex's case shows that defense attorneys strategically used digital evidence to raise doubts about the complainant’s state of mind and behavior in the aftermath of the assault as well as to weaken her credibility as a witness. We have offered for legal scholars a theoretically and empirically grounded explanation of why digital evidence falls short of model witness standards and may actually be biased by the communication management practices of intimate partners. This explanation is in addition to a trial process that exposes the privacy of IPV victims more than abusers. For interpersonal scholars, we show that when court actors become involved in IPV, the couple’s privacy boundaries are renegotiated in a way that exposes and increases the vulnerability of the victim. Future research might examine how privacy management influences the acquisition of electronic communication and the use of digital evidence in a larger sample of IPV cases. Future research would also benefit from access to a broader range of actors involved in IPV cases. The present case study was limited to the defense team and opportunities to observe the prosecution and witness testimony of the victim at trial. To further understand the role of CPM in the legal context, it would be useful to understand how the prosecution prepares its case arguments and whether jurors’ own CPM rules and biases shape how they evaluate the victim’s credibility and the digital evidence of communication between the victim and defendant.

References

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

Boux, H. J., & Daum, C. W. (2015). At the intersection of social media and rape culture: How Facebook postings, texting and other personal communications challenge the “real” rape myth in the criminal justice system. *Journal of Law, Technology & Policy, 2015*(1), 149–186.

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.

Boyles, J. L., Smith, A., & Madden, M. (2012). Privacy and data management on mobile devices. Retrieved from http://www.pewinternet.org/files/old-media/Files/Reports/2012/PIP_MobilePrivacyManagement.pdf

Centers for Disease Control. (2012). Findings from the National Intimate Partner Sexual Violence Survey. Retrieved from https://www.cdc.gov/violenceprevention/pdf/NISVS-StateReportFactsheet.pdf

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

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

Child, J. T., & Petronio, S. (2017). Communication privacy management theory. In M. Allen (Ed.), *The SAGE encyclopedia of communication research methods* (pp. 205–208). Thousand Oaks, CA: SAGE Publications.

Child, J. T., Petronio, S., Agyeman-Budu, E. A., & Westermann, D. A. (2011). Blog scrubbing: Exploring triggers that change privacy rules. *Computers in Human Behavior, 27*, 2017–2027. doi:10.1016/j.chb.2011.05.009

Child, J. T., & Starcher, S. C. (2016). Fuzzy Facebook privacy boundaries: Exploring mediated lurking, vague-booking, and Facebook privacy management. *Computers in Human Behavior, 54*, 483–490. doi:10.1016/j.chb.2015.08.035

Cionea, I. A., Piercy, C. W., & Carpenter, C. J. (2017). A profile of arguing behaviors on Facebook. *Computers in Human Behavior, 76*, 438–449. doi:10.1016/j.chb.2017.08.009

Davies, L., Ford-Gilboe, M., & Hammerton, J. (2009). Gender inequality and patterns of abuse post leaving. *Journal of Family Violence, 24*, 27–39. doi:10.1007/s10896-008-9204-5

Diss, L. E. (2013). Whether you "like" it or not: The inclusion of social media evidence in sexual harassment cases and how courts can effectively control it. *Boston College Law Review, 54*(4), 1841–1880.

Dodge, A. (2017). The digital witness: The role of digital evidence in criminal justice responses to sexual violence. *Feminist Theory, 19*(9), 1–19.

Dragiewicz, M., Burgess, J., Matamoros-Fernández, A., Salter, M., Suzor, N., Woodlock, D., & Harris, B. (2018). Technology facilitated coercive control: Domestic violence and the competing roles of digital media platforms. *Feminist Media Studies, 18*(4), 609–625. doi:10.1080/14680777.2018.1447341

Dutton, M., & Goodman, L. (2005). Coercion in intimate partner violence: Toward a new conceptualization. *Sex Roles, 52*(11–12), 743–756. doi:10.1007/s11199-005-4196-6

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

Feigenson, N. (2014). The visual in law: Some problems for legal theory. *Law, Culture and the Humanities, 10*(1), 13–23. doi:10.1177/1743872111421126

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

Fox, J., Osborn, J. L., & Warber, K. M. (2014). Relational dialectics and social networking sites: The role of Facebook in romantic relationship escalation, maintenance, conflict, and dissolution. *Computers in Human Behavior, 35*, 527–534. doi:10.1016/j.chb.2014.02.031

Ganzenmuller, R. G. (2014). Snap and destroy: Preservation issues for ephemeral communications. *Buffalo Law Review, 62*(5), 1239–1288.

Garcia, C. A. (2003). Digital photographic evidence and the adjudication of domestic violence cases. *Journal of Criminal Justice, 31*(1), 579–587. doi:10.1016/j.jcrimjus.2003.08.001

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

Hall, J. A., & Baym, N. K. (2012). Calling and texting (too much): Mobile maintenance expectations, (over)dependence, entrapment, and friendship satisfaction. *New Media and Society, 14*(2), 316–331. doi:10.1177/1461444811415047

Halligan, C., Knox, D., & Brinkley, J. (2013). Trapped: Technology as a barrier to leaving an abusive relationship. *College Student Journal, 47*(4), 644–648.

Harris, B., & Woodlock, D. (2019). Digital coercive control: Insights from two landmark domestic violence studies. *British Journal of Criminology, 59*(3), 530–550.

Hartley, C. C. (2001). "He said, she said": The defense attack of credibility in domestic violence felony trials. *Violence Against Women, 7*(5), 510–544.

Haselschwerdt, M. L., & Hardesty, J. L. (2017). Managing secrecy and disclosure of domestic violence in affluent communities. *Journal of Marriage and Family, 79*(2), 556–570. doi:10.1111/jomf.12345

Jin, B., & Peña, J. F. (2010). Mobile communication in romantic relationships: Mobile phone use, relational uncertainty, love, commitment, and attachment styles. *Communication Reports, 23*(1), 39–51. doi:10.1080/08934211003598742

Khunou, G. (2012). Making love possible: Cell phones and intimate relationships. *African Identities, 10*(2), 169–179. doi:10.1080/14725843.2012.657860

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

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

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

MacDonald, M. (2015, October 8). Rehtaeh Parsons review finds no prospect of sex assault convictions. *Toronto Star*. Retrieved from https://www.thestar.com/news/canada/2015/10/08/review-into-police-and-crown-handling-of-rehtaeh-parsons-case-to-be-released.html

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

Ngcongo, M. (2016). Mobile communication privacy management in romantic relationships: A dialectical approach. *South African Journal for Communication Theory and Research, 42*(1), 56–74.

Oppel, R. (2013, March 18). Ohio teenagers guilty in rape that social media brought to light. *The New York Times*. Retrieved from https://www.nytimes.com/2013/03/18/us/teenagers-found-guilty-in-rape-in-steubenville-ohio.html

Petronio, S. (2002). *Boundaries of privacy: Dialectics of disclosure*. Albany, NY: State University of New York Press.

Petronio, S. (2013). Brief status report on communication privacy management theory. *Journal of Family Communication, 13*(1), 6–14. doi:10.1080/15267431.2013.743426

Powell, A. (2015). Seeking rape justice: Formal and informal responses to sexual violence through technosocial counter-publics. *Theoretical Criminology, 19*(4), 571–588. doi:10.1177/1362480615576271

Raybin, D. L., & Raybin, B. K. (2011). What to tell clients about Facebook and other social media sites. *Tennessee Bar Journal, 47*(3), 19–21.

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

Segal, M. (2015). Independent review of the police and prosecution response to the Rehtaeh Parsons case. Retrieved from https://novascotia.ca/segalreport/Parsons-Independent-Review.pdf

Sherwin, R. K. (2012). Visual jurisprudence. *New York Law School Law Review, 57*(2012–2013), 11–39.

Sholl, E. W. (2013). Exhibit Facebook: The discoverability and admissibility of social media evidence. *Tulane Journal of Technology and Intellectual Property, 16,* 207–230.

Stratton, G., Powell, A., & Cameron, R. (2017). Crime and justice in digital society: Towards a "digital criminology"? *International Journal for Crime, 6*(2), 17–33. doi:10.5204/ijcjsd.v6i2.355

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

Tuerkheimer, D. (2017). Incredible women: Sexual violence and the credibility discount. *University of Pennsylvania Law Review, 166*(1), 1–58.

Waddell, T. F. (2016). The allure of privacy or the desire for self-expression? Identifying users' gratifications for ephemeral, photograph-based communication. *CyberPsychology, Behavior & Social Networking, 19*(7), 441–445. doi:10.1089/cyber.2015.0677

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.

Weathers, M. R., Canzona, M. R., & Fisher, C. L. (2019). Digital media as a context for dating abuse: Connecting adaptive and maladaptive coping strategies to young adult women's well-being. *Affilia: Journal of Women & Social Work*. Advance online publication. doi:10.1177/0886109919832005

Wellman, A., Reddington, F., & Clark, K. (2017). What's trending? #SexualAssault: An exploratory study of social media coverage of teen sexual assaults. *Criminology, Criminal Justice, Law & Society, 18*(1), 88–105.

Wise, M., & Rodriguez, D. (2013). Detecting deceptive communication through computer-mediated technology: Applying interpersonal deception theory to texting behavior. *Communication Research Reports, 30*(4), 342–346. doi:10.1080/08824096.2013.823861

Woodlock, D. (2017). The abuse of technology in domestic violence and stalking. *Violence Against Women, 23*(5), 584–602. doi:10.1177/1077801216646277

Worthington, D., Fitch-Hauser, M., Välikoski, T.-R., Imhof, M., & Kim, S.-H. (2012). Listening and privacy management in mobile phone conversations: Cross-cultural comparison of Finnish, German, Korean and United States students. *Empedocles: European Journal for the Philosophy of Communication, 3*(1), 43–60. doi:10.1386/ejpc.3.1.43_1