Archived version from NCDOCKS Institutional Repository http://libres.uncg.edu/ir/asu/

Violations Of Sexual And Information Privacy: Understanding Dataraid In A (Cyber)Rape Culture

By: **Martha McCaughey** and Jill Cermele

Abstract

Technology-facilitated sexual violence is a violation unique to the digital age that extends the analog-era rape culture, but electronic privacy invasions are often an overlooked part of these violations. This article examines three emblematic cases of information privacy violations that get used, framed, or rationalized in connection with violations of sexual privacy. In showing how aggressive electronic intrusions borrow the well-worn tropes of rape culture, we show how violations of sexual and information privacy are linked in the digital age. Digital violations of both sexual and information privacy are impacted simultaneously by rape culture and surveillance culture, which are mutually reinforcing.

McCaughey, M. and Cermele, J. (2021). Violations of Sexual and Information Privacy: Understanding Dataraid in a (Cyber)Rape Culture. *Violence Against Women*, accepted for publication August 2021. *Pub date: forthcoming 2021/2022*. Publisher version of record available at: https://us.sagepub.com/en-us/nam/journal/violence-against-women

Violations of Sexual and Information Privacy:

Understanding Dataraid in a (Cyber)Rape Culture

Martha McCaughey

Appalachian State University

Dept of Sociology

Chapell Wilson Hall

Appalachian State University

Boone, NC 28608

mccaugheym@appstate.edu

Jill Cermele

Drew University

jcermele@drew.edu

Authors' Note: The authors wish to thank the journal reviewers as well as Kristin Anderson, Samuel Avery-Quinn, Neal King, Christine Labuski, and Henry Wansker for valuable feedback on earlier drafts of this paper.

Key words: technology-facilitated sexual violence, datarape, dataraid, sexual privacy, surveillance

Abstract

Technology-facilitated sexual violence is a violation unique to the digital age that extends the analog-era rape culture, but electronic privacy invasions are often an overlooked part of these violations. This article examines three emblematic cases of information privacy violations that get used, framed, or rationalized in connection with violations of sexual privacy. In showing how aggressive electronic intrusions borrow the well-worn tropes of rape culture, we show how violations of sexual and information privacy are linked in the digital age. Digital violations of both sexual and information privacy are impacted simultaneously by rape culture and surveillance culture, which are mutually reinforcing.

INTRODUCTION

Modern information and communication technologies have created a whole new frontier for the surveillance of consumers, students, and political activists. Indeed, we now live in a "surveillance society," where location tracking, facial recognition, and monitoring of political and consumption patterns are everyday realities; many forms of individual and group data are collected for the purpose of governing, regulating, managing, or influencing what people do in the future (Surveillance Studies Network, n.d.). These technologies have also multiplied the ways in which a person can both express their sexuality and be stalked, harassed, and sexually assaulted (Clough 2016).

The same portable and remote-access technologies that allow for new, technology-facilitated forms of sexual violence also allow for relatively easy and inexpensive data searches and seizures—a privacy invasion that we will call dataraid. And yet while feminist scholars have been concerned with technology-facilitated sexual violence, they have not addressed digital privacy invasions as such—even when they occur as part of technology-facilitated sexual violence. Similarly, although information privacy advocates have worked to protect against theft or exposure of our digital information, they have not considered the parallels with technology-facilitated sexual violence. Recent work has asked scholars studying surveillance and privacy to pay more attention to feminist concerns about gender and other forms of inequality (Dubrofsky & Magnet, 2015), but this paper also urges feminist scholars to pay more attention to privacy in a surveillance society. We will show that, in the digital age, sexual and information privacy converge, and both rape culture and surveillance culture reinforce one another.

We first review technology-facilitated sexual violence and then move into the subject of dataraid by presenting three exemplary cases of information privacy invasions or dataraid that show

the breadth, impact, and power relations they involve: (1) a data company's capture of a woman's pictures she sent from a laptop; (2) the police warrantless seizure and search of computer files of a professor employed at a public university (who is also an author of this paper), which is one of the first cases of its kind to make national news; and (3) the search of text messages between state employees using workplace-issued pagers. In all three cases, sexuality came into focus and informed how the targets of dataraid were treated: the woman's pictures were sexually intimate; the professor's computer was searched for obscenity after the computer was confiscated in order to find anti-rape activists; and the state employee's pager contained sexually explicit text messages. Of course, countless cases of information privacy invasions exist (see Cannatasi et al., 2016; "Privacy", nd.; Kerr et al., 2009; Orenstein, 2017) and thus these three cases barely scratch the surface. It is beyond the scope of this paper to survey all cases or, even more broadly, discuss the differential impact of surveillance on people situated differently across multiple axes of power and privilege. We discuss these three cases to give an idea as to the range of issues and people who are subject to these digital invasions and to draw attention to dataraid as well as the cultural assumptions that enable its perpetuation and acceptance, calling attention to sexualized invasions of privacy and highlighting the ways in which rape culture and surveillance culture have become mutually reinforcing. Likewise, we show how a violence against women framework helps us better understand (and challenge) dataraid, particularly that which involves sexually explicit material and relies on the tropes of our rape culture.

INVASIONS OF PRIVACY AS ACTS OF POWER

Gender-motivated attacks that were, prior to the digital era, often focused on flesh-and-blood bodies and committed person-to-person, face-to-face, are now also carried out in virtual spaces or directed at people (primarily women) in physical spaces using technology (see Anderson & Cermele,

2014; Fisher, 2016; Powell & Henry, 2017; Vera-Gray, 2017). For example, Vera-Gray (2017) found that women in online public spaces suffer much abuse from men there, and argues that such technology-facilitated harassment must be understood as an online extension of traditional forms of stranger intrusion in physical spaces (such as street harassment) and, thus, "...within a violence-against-women frame" (p. 67). Technology-facilitated sexual violence can take place in private or public spaces, on physical bodies or virtual bodies, by an anonymous perpetrator or a known one. In all cases, it is characterized by an imbalance of power, a lack of consent, and a context of a rape-supportive environment.

Almost all behaviors, including sexual behaviors, are now technologically mediated, and as long as people have been having consensual cybersex, there have been nonconsensual versions of the same. In the early days of the Internet, the term "cyberrape" emerged in both popular culture and academic literature to describe the use of one's online game avatar to rape another's avatar in virtual communities (see, e.g., Dibbel, 1995, Michals 1999). Back then, such acts were body-less. Today a much wider range of information and communication technologies are being used to perpetrate acts of sexual violence and exploitation. Moreover, technology-facilitated sexual violence now includes installing spywear in the target's home or buying and selling computers with remote-access technology built in so as to view or make secret-camera porn videos of the person who is unknowingly using the infected device. It further includes the nonconsensual sharing of intimate and private images of a person (including "revenge porn", "involuntary porn", and rape memes), and the use of small digital cameras for video voyeurism (such as taking up-skirt fetish photos or "creepshots" of women in public). These acts not only extend rape culture to our virtual spaces but also bring new technologies into our private physical spaces—even whilst not physically touching the bodies of their targets.

Technology-facilitated sexual violence, then, encompasses a wide variety of intrusive acts in which some technological method is used to invade someone's sexual privacy, defined as "the social norms (behaviors, expectations, and decisions) that govern access to, and information about, individuals' intimate lives" (Citron, 2019, p. 1874). It is beyond the scope of this paper to catalog all of the ways someone can use technology to facilitate sexual violence or to distinguish between which forms are actionable under which laws and policies in which countries. The important point, for our purposes, is that these acts use technology to hack into the *private physical space* of the targeted person.

Feminist scholars would likely agree that the starting point for a definition of rape is that a person's body is penetrated sexually without that person giving consent, and penetration can be by an object or a body part. Feminists expanded what counts as rape, such as in Robin Warshaw's 1988 book *I Never Called It Rape,* which argued, over many people's objections, that date or acquaintance rape is a violation that should be included in the scope of rape. The notion of technology-facilitated sexual violence extends the domain of sexual violence to the digital environment. We do not suggest that these acts are the same as sexual assault in physical spaces, but at the same time we do not dismiss them as insignificant or as disembodied harms.

The targets of technologically-facilitated sexual misconduct suffer real-world consequences. One study found that a sample of survivors of cyber-sexual assault had nearly the same trauma symptomatology (e.g., trauma guilt, emotional dysregulation, post-traumatic stress disorder, depression) as survivors of sexual assault in traditional settings (Holladay, 2016). For example, Paris Hilton, whose infamous sex video was shared across the web without her consent in 2003 (the first widely known act of revenge porn), did not speak of the violation until 2017, when she said, "I could not leave my house for months. I was so depressed, humiliated. I didn't want to be seen in

public" (Carmon, 2017, para. 22). In some cases, such as revenge porn where the material is sent to and seen by hundreds, or even hundreds of thousands of people, the emotional distress can be particularly acute and unending (Holladay, 2016). Survivors of revenge porn reported feelings of betrayal and a loss of trust, as well as depression, anxiety, suicidal ideation, symptoms of post-traumatic stress disorder, and loss of self-esteem, confidence, and control (Bates, 2017).

It might already be clear that technology-facilitated sexual violence involves and requires digital privacy invasions—e.g., having your intimate images captured without your knowledge because you're using a computer infected with spyware, or finding that the nude pictures you shared consensually with one person are now being shared nonconsensually with millions of people because a hacker got into your SnapChat account, as actress Jennifer Lawrence experienced (Farrell, 2014). In these cases, breaching digital information privacy is part of the aggressive project of technology-facilitated sexual violence. Such an event is not only psychologically distressing (Clough, 2016) but can also been seen an invasion of privacy (Citron, 2019; Clough, 2016; Franks, 2017; Šepec, 2019) as well as a compromise to the sexual integrity and identity of the victim (Šepec, 2019).

Whereas law enforcement recognizes cyber-stalking as a problem precisely because it carries a threat of *physical* harm, no physical bodily boundaries or material possessions are violated in many cases of digital privacy intrusions. This can create the illusion of lesser or no harm. Yet for targets of remote-access technology that spy on people via the camera on their device, finding out that others have been watching them is terribly unsettling. Despite unshared dimensions of rape in physical space and cyberspace, the cyber-perpetration can be experienced as genuinely intrusive, unethical, controlling, and even violent—as is rape in physical space. While rape in physical space impacts the physical body in ways that sexual violence in cyberspace does not, the harm of both, to some extent, is to the self invested in that body—whether that body is a physical entity or a

culturally designated place. The social rules creating the boundaries of our embodied identities in virtual places mirror the social rules creating the boundaries of our embodied identities in physical spaces, and, of course, the feelings of vulnerability and empowerment in virtual places are not necessarily separable from those in our physical spaces.

Technology-facilitated sexual violence is now an area of public concern—indeed, a moral panic over girls' sexting and their susceptibility to such abuse emerged in the last decade (Hasinoff, 2015). It is also now an area of scholarly study, and is a feminist issue insofar as it takes place within a broader context of online misogyny and harassment, reveals a social tolerance of sexual violence against women, and therefore stems from and supports rape culture (see Backe et al, 2018; Crooks, 2018; Powell & Henry, 2017). We do not suggest that the wide variety of nonconsensual forms of technology-facilitated sexual violence all constitute the same kind of crime, harm, or lived experience, nor are we legal scholars trying to make a legal argument. Our point, rather, is simply that technology-facilitated sexual violence extends an analog-era problem, and further, that sexually aggressive online banter, online game add-ons and hacks that allow players to simulate rapes, and rape memes[1] all provide a climate supportive of abuse because they normalize more extreme actions along a continuum of online violence (Powell & Henry, 2017).

The "Marines United" Facebook page, exposed in 2017, illustrates the intensely personal boundary violations and power dynamic of technology-facilitated sexual violence, where active-duty and veteran male Marines posted and viewed nonconsensually taken or obtained nude photos of female service personnel ("Nude photo scandal rampant…", 2017). Various states and organizations disagree on where to draw legal lines in cases like this. For instance, when a fraternity at Penn State

[1] See Dahl (2013) for an account of a rape victim's suicide after her rape was turned into a mocking meme that spread widely across the Internet.

in 2015 was engaged in a similar practice sharing nonconsensually obtained images over social media, they argued, successfully, and in agreement with the ACLU's position, that the images were meant as satire rather than *to harass*, and were therefore not against the state's nonconsensual pornography law (Franks, 2017). Our point is not to enter a debate with lawmakers, but to emphasize how feminists can frame these actions as *privacy violations in furtherance of an act of power*.[2] Specifically, modern information and communication technologies make images of nude people easy to obtain and share, which underscores the point of these actions by the fraternity or the Marines being that they are non-consensual acts of power. After all, neither Marines nor college fraternity brothers would have any trouble finding images of women who freely share their own semi-nude selfies on social media or who consensually make pornographic images and videos available. The point is that they took and shared non-consensually obtained images, those that violate women's boundaries. As Franks (2017) puts it, "Treating nonconsensual pornography as a harassment issue instead of a privacy issue demotes the harm it causes from an invasion of privacy to something more akin to hurt feelings," which is "a misguided and patronizing approach."

To be sure, not all privacy violations in furtherance of an act of power are sexual. The digital privacy invasions where technology is used to hack into or otherwise access a person's digital files or digital presence considered to be private has been labeled colloquially "datarape" (see, e.g., "datarape", 2015). While such a term may be crass and insensitive to sufferers of physical invasions, it is no coincidence that such aggressive, nonconsensual invasions of privacy have been so

[2] While the targets of cyberrape in this example are women, LGBTQ+ individuals are frequently targeted (see, e.g., "Tyler Clementi's Story", n.d.). Heterosexual cis-men have been targeted as well (see, e.g., Crocker, 2014).

labeled. We use the term "dataraid" instead, and argue that as technology-facilitated sexual violence is gendered, so too is dataraid, in the dynamics around power, violence, and victimization, which bell hooks (2015) describes as patriarchal violence—that is, where violence is regarded as an acceptable means of social control, regardless of the gender of perpetrator or victim. To be clear, the target of dataraid is not the technology itself (e.g., the computer or smartphone being accessed), but rather the individual whose technology, and therefore cyber-self, has been invaded or violated. The digital presence or information considered to be private may or may not include sexually explicit images, chats, or details. Our focus here, though, is when and how dataraid is sexualized. As our case studies show, people invoke the well-worn tropes of rape culture to understand, and rationalize, the aggressive intrusion into people's private digital spaces.

It is within this feminist approach that our argument is grounded: that intrusions into our technological data or data-selves can be understood theoretically, practically, and affectively in connection with acts of bodily rape in the physical world, and to acts of technology-facilitated sexual violence that may more closely mirror traditional sexual assault. Just as rape has been seen as an assertion of the assailant's power through the violation, dataraid can—and, we argue, should—be understood as an assertion of power. Further, a technological invasion can be intimate and personal, particularly when it is experienced or framed as sexual. As technology has expanded, so have our technological selves; these aspects of the self are as personal and real as our flesh-and-blood bodies. In consequence, we can experience real harm online or through our digital presence. Just as controlling one's body and/or one's sexuality is a privacy interest (Pracher, 1981, p. 745; Citron, 2019), so, too, is controlling one's technological self, particularly when the digitized information is about one's body or sexuality. Our point here is not that rape, technology-facilitated sexual violence, and dataraid are all the same experiences, in life or in law, but that analyzing them together

can generate new insights about the convergence of information privacy and sexual privacy, and the discourses that rationalize aggressive privacy invasions. Put another way, if we accept that technology-facilitated sexual violence is harmful in some way, and therefore want to combat the problem, it follows that we must better understand and challenge the dataraid that is so often a part of the intrusion.

Privacy rights include a right to be protected from intrusion or harassment (Elshtain, 1997), but of course sexual privacy and information privacy are not exactly the same (see, e.g., Strahilevitz, 2005; Citron, 2019). Thus, we do not suggest that sexual privacy or sexual integrity is *really* information privacy, but rather that both the practice and the subjective experience of dataraid can be seen as analogous to the experience of bodily rape in physical space in the following ways: the aggression targeted at one's core identity; the power dynamic at play; how the act is feminizing (regardless of whom it targets); the betrayal and subsequent emotional and psychological outcomes experienced by those targeted; the way the violation limits one's autonomy and ability to participate in civic life; and in the individual, social, and structural responses to the act.

THE DATARAID IN TECHNOLOGY-FACILITATED SEXUAL VIOLENCE

Individuals and groups using surveillance technologies to target people for sexualized purposes is a subset of the practices by individuals, governments, and corporations that target people through those same technologies for other purposes. Technology-facilitated sexual violation dovetails with the violation of privacy that occurs when non-sexual forms of our online selves are violated, taken from us, or invaded without our express or affirmative consent. Just as we argued that those who experience technology-facilitated sexual violence can be traumatized, those who find their electronic data raided can also experience the same sort of surreal blending of bodies and technologies, and thus experience those electronic searches as compromising their privacy, their

dignity, their autonomy, and their very selves. As with sexual violence in physical space, acts of sexual violence in cyberspace and dataraid are not just about harm, damage, or injury to one's physical body or to one's property, but about harm, damage, or injury to the self.

While invading, taking, and sharing our (non-sexual) data without our consent may not overtly simulate an act of interpersonal violence in the material world, or necessarily involve intimate images or sexualized information, it can nonetheless be a violation or invasion both theoretically and tangibly similar to acts of sexual assault. In drawing parallels between sexual violence in physical space, sexual violence in cyberspace, and dataraid, we do not suggest they are or ought to be indistinguishable in life or in law. It may be easy enough for people to see the parallel between rape and "cyberrape", but when we consider dataraid alongside these, it becomes possible to understand the harm all these violations have in common: boundary violations and the invasion of privacy. While we have seen more and more forms of technology-facilitated sexual violence become punishable by law, we have arguably seen our protections against dataraid dramatically eroded. Examining a number of cases here will illustrate how and why dataraid and sexual violence can be seen as mutually shaping forces and discourses. Put differently, technology-facilitated sexual violence is enabled by a rape culture that has moved online (a cyberrape culture), and digital intrusions are enabled by a surveillance culture, in which we take for granted the digital invasions of privacy in general, and now surveillance culture and rape culture mutually reinforce one another. We turn now to three cases of dataraid, showing how the rationalizations for these aggressive intrusions borrow the well-worn tropes of rape culture, and how rape culture and surveillance culture work together to rationalize violations of information and sexual privacy.

Case 1: Corporate Remote-Access Spyware on Laptop

Susan Clements-Jeffrey, a substitute teacher in Springfield, Ohio, United States, bought a laptop in 2008 from a high school student where she worked, not knowing that the student himself had purchased it from someone else who had stolen it. The school district that had purchased the laptops had a contract with Absolute Software, Inc, a theft recovery service that gathered information to try to identify the user of a stolen machine. Believing her communications over her password-protected laptop to be secure, Clements-Jeffrey had exchanged sexually explicit messages and photos with her long-distance boyfriend, Carlton Smith, via her laptop's camera while in her home. Absolute ran remote-access software, LoJack for Laptops, designed to help people recover stolen computers, and had Clements-Jeffrey's computer download certain software that allowed remote access to her machine and files in real time without her knowledge. Absolute then discovered the sexually explicit photos, and furnished them to the police. Police showed up at Clements-Jeffrey's house in search of the stolen computer, showing her the sexually explicit photos of herself, mocking her, and calling her stupid (Massoglia, 2014).

One issue in this case is a person's having a reasonable expectation of privacy per the 4th Amendment in/on a device that was stolen if they did not know it was stolen, which a federal judge affirmed in 2011 (Welsh-Huggins, 2011). The other issue is how Clements-Jeffrey was treated by both the Absolute employees and the police. Neither furnishing sexually explicit webcam images, nor mocking and humiliating her, were necessary for recovering the laptop or identifying its thief. Clements-Jeffrey and Carlton Smith sued both the Springfield police and Absolute, arguing that they had a reasonable expectation of privacy in their computer communications. By 2011, Absolute had settled with Clements-Jeffrey and Smith, providing an undisclosed sum (Welsh-Huggins, 2011). The accessing and downloading of her sexually explicit photos by Absolute, and the harassment she experienced at the hands of the police, are noteworthy in their unnecessariness; it seems unlikely that

photos of her cat or webcamming with her sick mother would have resulted in this same treatment. Instead, her sexuality was immediately targeted as a way to punish her for having presumably stolen the laptop, or simply to help the Absolute workers and police officers intimidate Clements-Jeffrey.[3]

Case 2: Police Search and Seizure of Computer Files

A second case involved a professor, Martha McCaughey (also an author of this paper), whose workplace computer was seized and searched by campus police in 2002.[4] This event became national news because, at that time, such situations were still relatively new and people did not know how to articulate what harm had been done. Precipitating this event was a group of protesters spray-painting anti-rape graffiti across sidewalks and buildings on the campus of a U.S. public university where the professor was employed. Some hours later, a group claiming responsibility for the graffiti sent an anonymous e-mail "manifesto" defending the group's act of property defacement as politically necessary given the problem of rape. The manifesto indicated no future action or plans to deface more property or hurt people. One such recipient was McCaughey who, in her capacity as Director of the Women's Studies Program, forwarded the message (with an explanatory preface) to her colleagues on the program's listserv because such current events often get discussed in their classes. Although the email manifesto said that the Women's Studies Director was one of several

[3] To be clear, neither exposure of a sexual nature nor involvement of a female target are requirements for a situation to be dataraid. For instance, a man described feeling invaded when photographs, log messages, and screenshots were captured by a similar remote-access technology, even though the photos captured him playing poker (see Massoglia, 2014, para. 13).

[4] This incident is described with regard to academic freedom, but not with regard to violence against women or as dataraid, in McCaughey (2003).

people being sent the manifesto because she was perceived by the senders to be sympathetic to their cause, she neither claimed nor denied any sympathy for their manifesto or form of protest.

In forwarding the email to her colleagues, McCaughey attracted the attention of the campus police, who wanted the message to trace its origin and catch the senders/vandals. Some days later, a campus detective asked the professor for her entire computer to perform an email recovery operation. Despite her refusal to hand over her entire computer and files, uniformed armed police officers later appeared at her campus office and confiscated the computer with all her files on it. When McCaughey asked for a search warrant, the officers told her that they did not have or need a warrant because the computer was university property. Of course, the professor's own electronic files saved on the computer were distinct from the machine itself--the object that was university property. The police and the University strategically ignored this distinction, took the machine, and copied the entire harddrive before returning the computer to the professor's office.

Confiscating an entire computer hard drive to access one email message meant copying thirty gigabytes of information to get a four-kilobyte email file from the anti-rape graffiti spray-painters—copying over *7.5 million times* the information they needed. Without a warrant, which would have limited the scope of the search, the police deemed everything on the computer fair game for searching. The professor's own counter-surveillance of her hard drive, once her computer was returned to her, revealed that the police had opened some of her files, including, for example, those saved with words like "WS Pictures" and "Sex Toy Parties". The searched documents were all part of bona fide research projects, most of them published already, and the file (suspiciously?) called "WS Pictures" was a file of photos of illustrious women (in their clothes), which had been on the program's website. The police later admitted to McCaughey that they had opened these files because they thought they might be obscene.

Regarding the search for the sender of the anonymous email and the graffiti spraypainters, University tech specialists recovered the deleted email but were unable to trace it to any sender's computer. The professor was never arrested, fired, or reprimanded on obscenity or any other charges; yet the confiscation of her computer files was disturbing for her personally and chilling for many of her colleagues. Further, people reading about the case in some newspapers and magazines suggested that the professor ought not to have had an expectation of privacy in any electronic files stored on a state-issued computer in the first place, or was asking for the intrusion because she forwarded the email.

The legitimating discourse paralleled almost exactly the very narratives that attempt to rationalize sexual assault: that a professor's research on sexual and/or feminist topics renders her necessarily dataraid-able; that a professor who will not "cooperate" with the intrusion deserves what she gets (in other words, they would not have had to engage in the aggressive intrusion to get the data if she had not had the audacity to say 'no' in the first place); that a professor's computer and the files stored thereon are not really her property, but that of her employer, making capricious computer searches and seizures the "right" of the state (much as rape was, until recently in American history, the "right" of the husband who, in a legal marriage, owned his wife); and, finally, that a professor being "loose" with her computer deserves the intrusion–as one commentator remarked, "in forwarding the offending e-mail to a Listserv, rather than simply deleting it, [the professor] can hardly argue that she was attempting to keep the whole matter private" (Sheilds, 2004, p. 6). Her promiscuous forwarding of her email categorized her as a "cyber-slut". Clearly, dataraid is rationalized in terms of entitlement to access, and the victim is often blamed for inviting or deserving it. When using a computer network itself sets one up as blameworthy, it is eerily similar to the bygone days when rape victims had to establish themselves as virgins to garner sympathy and

avoid blame. No act of *sexual* aggression was committed against the professor, but the aggressive, entitled invasion of privacy in this circumstance, coupled with the manner in which it was rationalized, reveals the parallels between virtual and physical privacy violations.

Case 3: Employer Searches of Employees' Text Messages

Our final example is the 2010 case of police Sergeant Jeff Quon, whose case made "sexting" a household word. Here, Sergeant Quon argued--unsuccessfully--that his employer, the Chief of Police in Ontario, California, U.S.A., had no right to read the text messages he had sent using his work-provided pager. The police chief had decided to obtain and read the transcripts of text messages on the pagers of employees who had the highest data-use fees. Sergeant Quon had dutifully paid any overage charges for his data use in excess of the city's monthly character limit, but the Police Chief presumably wanted to see whether the city's limit was too strict or what had caused the high usage fees. The search revealed that Sergeant Quon had been sending sexually explicit text messages to both his wife and his girlfriend (also a coworker). The police department's policy made it clear that incidental personal use of the pagers was allowed and that the Police Chief told officers that their usage rates, but not message content, would be monitored. Quon sued the city and the company, Arch Wireless, which had voluntarily provided the transcripts of the officer's text messages, for invasion of privacy (Mears, 2010). The Supreme Court's ruling in the Quon case—in favor of the government employer—indicated that the police chief's rifling through Sergeant Quon's text messages was an allowable search because there was a business reason to conduct that search, although not because any data or communications on state-issued or employer-issued device cannot be private (Savage, 2010).

One writer for the *Chicago Tribune* showed no sympathy for Sergeant Quon: "It takes a special kind of chutzpah to send sexually explicit messages on your employer-issued pager and then

howl that your privacy was violated when you get caught. Especially if you're a cop" ("No Sexting on the Job", 2010, para. 1). Here Quon is blamed for dataraid, arguably because he violated some expected norm of sexual propriety, in a manner similar to the way victims of rape are blamed. The remark, "especially if you're a cop", is particularly interesting, and perhaps meant to imply that we should hold police officers to higher standards of conduct, although it is unclear if those standards are relating to personal use of professional technology or to sexual behavior. But it might also reflect the mistaken belief, held by many, that, since cops are government employees, they ought *not* expect privacy. However, like the public university professor in the previous example, government employees typically have *more* privacy protections than non-government employees *precisely* because the U.S. Constitution was designed to protect citizens from government intrusion. As in Clements-Jeffrey's case, it likely would have been an easier case had Quon been texting Bible quotes or writing bad poetry to his wife. The revelation of intimate or embarrassing information is precisely what makes some people less sympathetic as targets of privacy invasion.

Even those who don't have a mistress and don't ever send sexy text messages usually use connected devices at home and at work. Our superconnected culture now makes using one device for multiple purposes normal and sometimes even necessary. Further, we can see that the targets of dataraid get blamed by suggesting that they either have no property rights or have loose sexual morals--in other words, that they deserved the intrusion. In Quon's case, it was both; some invoked Quon's sexual morals to blame him, while others suggested that he had no right to privacy on a work-issued device.

UNPACKING THE CASES: UNDERSTANDING DATARAID IN CYBERRAPE CULTURE

Dataraid is a power move: whether involving a person's sexuality and sexual behaviors or not, it grabs private parts, spaces, or information and violates an individual's sense of control in a

way that has a real material and affective impact. Technology studies scholars and body studies scholars have explained why someone would have an intimate connection with their digital information such that their exposure would feel like a real intrusion. For example, Deborah Lupton's (1995) early work on the "embodied computer/user" describes the emotional and embodied relationship that computer users have with their PCs; similarly, Elizabeth Grosz's (1994) work describes a computer as a machine that is not separate from one's body, but a prosthetic extension of it. More recently, Irma van der Ploeg (2012, p. 177) describes our bodies as "defined in terms of information. Who you are, how you are, and how you are going to be treated in various situations, is increasingly known to various agents and agencies through information deriving from your own body; information that is processed elsewhere, through the networks, databases, and algorithms of the information society". Indeed, today more than ever, our material bodies and networked technologies are inescapably entwined (Smith, 2016).

Technology-facilitated sexual violence, and the rationalizations for it, extend modes of gendered power and control and blur boundaries between physical bodies and technobodies. This analysis enables us to see that the harm of rape is not that it is done to a body, *per se,* but to a body-self, and that the techno-self, virtual-self, or information body can be both gendered and violated in real and meaningful ways. A sequelae of cyberrape is the production of an immediate, aesthetic, bodily affect; violation of the physical body is not required. In a study of cyberporn, Zabet Patteson (2004) argues that pornography changes when it is viewed on the computer, because the technology itself carries an "affective charge" (p. 120) that embodies new forms of pleasure. That particular affective charge, of course, is related to our existing categories of sexual and gendered experiences. That an invasion is done through technology and its related components does not mean there is no affective charge experienced by the person as a result of the intrusion.

Just as living in a rape culture impacts one's body and affect, so too does living in a cyberrape culture and a surveillance culture. Indeed, online sexual activity—whether consensual activity like consuming online porn, sharing one's nude selfies through social media, and using hookup apps like Tindr, or nonconsensual activity such as cyberstalking—is now so commonplace that it is a likely part of the subject formation and daily bodily habits of young people today (Puar, 2011). For these same reasons, living in a surveillance culture in which the very personal information we are encouraged to post or store in digital spaces can be hacked or otherwise taken and viewed without our consent has an impact on our overall affect and style of citizenship.

In the case of the substitute teacher, private nude photos of a woman were taken by a tech company and given to the police, both traditionally and stereotypically masculine organizations, without reason, and without cause. The perpetrators in the campus computer seizure case were the campus police and university administration, who embody a violent, entitled masculinity and stereotypically masculine traits when they seize and search someone's data without consent, a warrant, or viable explanation. The target's cyber-self, the perpetrators clearly feel, is theirs for the taking. It is not coincidental, and, in fact, would be almost comical if it were not horrifically ironic, that the professor was the target of a dataraid in the context of an investigation of people who were protesting rape in physical space. Nor it is coincidental that the professor targeted for dataraid, and then subsequently investigated for obscenity, was a women's studies professor presumably linked to anti-rape activism and suspected of having inappropriate sexual content on her computer.

That Sergeant Quon is a man and that the perpetrator/perpetrating organization are male/masculine does *not* mean that the dataraid was not gendered or patriarchal. The violation of Quon's sexual privacy was rationalized with implicit appeals to normative expectations of gender and sexuality. Quon was considered to have violated the norms of appropriate behavior around both

the workplace and sexuality. He was framed as having been inappropriately loose both with his sexuality and with his electronic device. Through the invocation of the same blaming tactics typically used toward victims of rape and sexual assault, Quon was rendered an unsympathetic victim and blamed for the privacy violation.[5] In the professor's case, some suggested that she was being loose with her computer by forwarding the protester/vandal's message to colleagues. In Clements-Jeffrey's case, some might still blame her for having expected that her intimate exchanges going across the Internet would be private or that, if she had stolen a computer then she would deserve the invasion of her sexual privacy. The targets of dataraid get framed, in the vernacular of rape culture, as "asking for it" and deserving of no respect, privacy, or sympathy.

Feminization is a mode, function, and effect of sexual violence (Mulder et al 2019). Rape victimization is "a doubly feminine phenomenon: (a) because it entails (interpersonal) victimization, triggering associations of weakness and vulnerability traditionally associated with femininity and (b) because it forces the victim into a particular role within sexual relations that is typically allocated to the feminine party" (Mulder et al 2019, para 2). On this basis rape is described as a *gendering* crime--one that has the potential to feminize its victims (Mardorossian, 2014). Sexual violence is a

[5] We note that readers might find it interesting or ironic that the target of this dataraid is himself a police officer, but it is beyond the scope of this paper to review literature on police officers' participation in surveillance as opposed to their being objects of it. We make no claim here about how often police officers get punished or get excused for actions that are illegal or perceived as morally wrong. For a discussion of police culture, including the strains of having hostile and punitive supervisors, and the relationship between police officers' attitudes toward their supervisors and citizens, see Terrill, et al (2003).

feminizing experience for the victim, regardless of the sex, gender identity, or sexual orientation of the people involved; blaming victims for their assaults, in general or as a function of having traits such as "a trusting nature" or "poor judgment", involves seeing those same victims as more feminine, regardless of the gender identity of the victims (Howard 1984, p. 274). The issue of victim blame is complicated (see Davies & Rogers, 2006 for a review of the literature), with beliefs about masculinity impacting beliefs about male victims in particular with respect to attributions of cause, blame, responsibility, and victim status. Thus rape, whether in cyberspace or physical space, is a gendered act. It stands to reason that dataraid is victimizing, and feminizing, in a parallel fashion. In cases of cyberrape and dataraid, our digital bodies, files, and personae—digital representations of self—are violated. In the process we and our files are treated as up for grabs, much the same way as feminized bodies in physical space are treated as up for grabs, literally and figuratively.

In these three cases, the targets are sexualized/gendered, and revealed or constructed as sexual beings—an element that almost automatically ruins one's credibility and claim to civil liberties, regardless of gender identity or sexual orientation. If Quon's texts were not sexts but, say, Bible quotes or recipes, would people have been less likely to blame him? If the professor's computer was full of quantum physics files rather than women's studies files would she have been subjected to the additional searches that were unrelated to the original investigation? Would people have been more sympathetic to the dataraid target if no seemingly salacious files were on their computer? Rape culture's pull to blaming the victim leads people to be suspicious of anyone who seems like a sexual being—at least, when the sexual being is the target of an aggressive invasion of privacy.

While doing something sexual might repeal potential sympathy in a dataraid case, simply doing something technological may be enough for people to blame the victim. The targets of dataraid we described were framed as cybersluts—people who are loose with their data, devices, or computers (in addition to, in some cases, their sexuality). Such cybersluttiness made it even easier, in a (cyber)rape culture and a surveillance culture, to claim that the dataraid targets were "asking for it." Another parallel to rape culture lies in the exhausting work people are expected to do in order to avoid predation. In his essay on the burdensome work of being surveilled, Smith (2016) describes the efforts people make to anticipate and mitigate their vulnerability in the context of the "involuntary visibility" of surveillance culture. Smith's description of such efforts, and the ways our neoliberal society expects individuals to bear the burden of self-protection, reads remarkably like women's accounts of their experiences living in a rape culture.

Regardless of the gendered or sexual nature of the targets, images, or messages, privacy has its own value, and intrusions into privacy are experienced as violations. Violations of the privacy we expect to be afforded in the technological extensions or ourselves and our identity constitute what we call dataraid. Precisely because privacy has value, separate from the nature of any specific act a person might want to keep private, we can imagine being disturbed if, while doing something as mundane as cooking dinner, someone was standing outside our kitchen window watching us do it. Similarly, perfectly good workers might not want their employer spying on them through the company computers, even though they have nothing to hide, just as people might not want their bosses dropping by their houses unannounced to check on their behavior outside of work hours. The academic freedom professors are afforded requires a certain amount of privacy so that they can conduct their scholarship without interference from government, corporate, or political interest

groups.[6] As we hope our examples in this article have illustrated, such surveillance not only compromises one's privacy, but affects one's actions and creates psychological harm, whether or not it harms the physical body, just as stalking is now recognized as an invasion of privacy that creates psychological harm, even if no physical contact with the target is made.

Many would argue that if people like Ms. Clements-Jeffreys or the professor had "nothing to hide" then they should not have cared who might be watching them remotely. This "nothing to hide" argument is based on mistaken views about what it means to protect privacy and the costs and benefits of doing so. Proponents of this argument believe that privacy is unnecessary when people are behaving appropriately, and that violating privacy is a small price to pay in order to expose the illegal or dangerous behavior of others (Solove, 2013). This is a false dichotomy; for example, activists, minorities, and citizens who might one day feel compelled to question a government, corporate, or community practice will need privacy from government surveillance and intrusion. This example is not hypothetical; in September of 2017, the Department of Justice under the Trump Administration sought to force Facebook to release the account information of individuals they deemed to be "anti-administration activists" (Schneider, 2017, para. 2).

IMPLICATIONS: UNDERSTANDING AND CHALLENGING DATARAID AND CYBERRAPE TOGETHER

To claim that technology-facilitated sexual violence is a feminist issue probably requires no justification, even when we acknowledge that not all of these types of violations hurt a physical body. We have attempted to establish that there is a dataraid dimension to many cyberrapes, and

[6] For an excellent synopsis of the Supreme Court of Virginia's decision on the importance of the privacy of email communication among public university professors, see Halpern (2014).

that the tropes of (cyber)rape culture get invoked to rationalize dataraid. Surveillance and digital intrusions reflect and perpetuate the abuses of power that feminists oppose. An intersectional feminist lens helps us see dataraid as a potential extension of (cyber)rape culture. And, just as feminist analyses have helped lawmakers and others come to terms with the fact that physical harm is not the necessary or only harm in technology-facilitated sexual violence, feminist analyses can help show how and why financial harm is not the only harm caused in cases of dataraid, and that physical privacy is not the only form of privacy to expect or to be violated. Privacy around one's sexual boundaries, so necessary for a sense of agency and control over one's own intimate and sexual life, now often goes hand-in-hand with electronic privacy.

Despite the obvious connection between interpersonal violence and privacy (rape violates bodily privacy, escaping a batterer requires the right to be left alone, and new technologies require information privacy to be safe from such abuses), feminists have had a conflicted relationship with privacy. Prior to feminists identifying rape as a structured social practice rather than a personal trouble, as an act of domination and a crime fueled by a rape-supportive environment or *rape culture* (Brownmiller, 1975; MacKinnon, 1989; Renzetti et al., 2017), rape, especially marital rape, was often considered a private matter (Pracher, 1981). Feminists criticized the way women suffered under imposed privacy in the home, where the domestic and sexual abuse of women and children were hidden ("Gender and Electronic Privacy", n.d.; Furedi, 2004, p. 72). Feminists understandably feared that the most socially, economically, and politically vulnerable people--such as women and children--would be harmed if the most powerful people--such as adult men--were free from government intrusion. As Cohen (1997, p. 135) points out, "as innumerable feminists have insisted, the public/private dichotomy has thereby served to reinforce and perpetuate social hierarchies and inequity between the sexes in all spheres of life." Thus, even while privacy is necessary for women

escaping abuse, feminists have often been skeptical of privacy as a place of refuge, viewing it instead as a shield for destructive behavior that harms women and children. Feminists have thus sometimes seen government intrusions into people's private lives and information as helpful in protecting the vulnerable.

And yet privacy has also been critical for women's escape from violence. Going to shelters in secret locations, for example, has been key for women's ability to leave abusers safely. The ability to maintain their own privacy and anonymity is critical for women, given how 21st Century technologies enable abusers to surveille, threaten, and control their victims. Privacy is not only spatial (privacy in one's physical space), and physical (bodily privacy); it includes decisional autonomy and information autonomy as well. Privacy rights secure our ability to develop intact identities of our own (Cohen, 1997, p. 154). Seen in relation to one another, understandings of control, identity, and intimacy provide that a definition of privacy involves "control over the intimacies of [one's] personal identity" (Gerety, 1977, as cited in Pracher, 1981, p. 743). In this way, privacy protects the essential aspects of our selfhood by presuming a boundary between one's intimate life and public life. And sexual privacy, as Citron (2019, p. 1874) puts it, "sits at the apex of privacy values because of its importance to sexual agency, intimacy, and equality."

Jennifer Doyle (2015) and Laura Kipnis (2017) have criticized those feminist anti-rape advocates who have uncritically aligned themselves with state security and protection measures that unilaterally limit people's rights to privacy. More broadly, programs of state surveillance complement state violence and disproportionately control people of color, who have historically been regarded as the "dangerous classes" in need of surveillance, not privacy (Roberts & Vagle, 2016). Indeed, contemporary surveillance technologies and practices have been linked historically to surveilling and policing Blacks under slavery, such as through branding and lantern laws

(Browne, 2015). Through this lens, enhancing state surveillance powers leads to the abuse of the more marginalized members of society, particularly racial and ethnic minorities, people with disabilities, and poor people (Elshtain, 1997). Privacy, then, is a value necessary for the autonomy, choice, and social participation that intersectional feminism espouses, and a lens through which both technology-facilitated sexual violence and dataraid can be understood and challenged.

Sensitivity to abuses of power and inequality are hallmarks of feminist analysis. Feminists have emphasized the importance of affirmatively expressed consent in the context of face-to-face rape. We could readily apply the decades-old chant that "yes means yes and no means no" to users of networked systems in order to highlight the importance of clear and simple privacy terms with opt-in and opt-out choices, and the need for companies and other organizations to seek and confirm the consent of a person, for example, to publish identifying information. Likewise, feminists are particularly insightful when it comes to debates about what constitutes meaningful consent, and could help answer questions surrounding, for instance: when consent to being photographed or videotaped occurs; when exposing parts of one's body (or other personal information) is consensual and when it is not; and how extensive such consent can be. Feminists can help understand and oppose online privacy violations as such, challenging the patronizing self-esteem-based interventions women and girls receive, which ultimately blame them for online victimization (see Hasinoff, 2015). A feminist analysis can help explain to perplexed attorneys, investigators, and others that, for example, a voluntary display of something "private" to ten people when done live at Mardi Gras is still not the same as being videotaped without one's consent and having one's videotaped image broadcast to millions of people or to sell a "Girls Gone Wild" video (see Stech, 2014).

Some feminist scholars have already challenged state or administrative overreach in some cases of sexual violence in physical space, arguing that securing a safe place for women must not come at the price of civil liberties (Kipnis, 2017). They have also challenged the notion that being a sexual subject removes one's innocence or possibility of being a victim of sexual violence (Doyle, 2015). This type of analysis offers a promising parallel for cyberspace, and might be applied to computer privacy and dataraid as well. Posting sexually explicit images in a way that is consensual, or sharing information of any kind through digital information and communication technologies, does not make one too "loose" to have a legitimate expectation of privacy and a complaint about dataraid.

Further, in line with critiques of state surveillance against the marginalized (Browne, 2015; Roberts & Vagle, 2016), feminist investment in our online liberties would make feminists more careful not to support policies and laws that trample cyberliberties as they attempt to keep women (or others) safe from new forms of violation. An example of overlooking a constitutional right in an attempt to protect victims can be seen when, as the Violence Against Women Act was reauthorized in 2013, the U.S. Congress redefined what actions constituted cyberharassment, casting such a wide net that simply causing *substantial emotional distress* (to the victim or the victim's immediate family) would now count as harassing someone online. This winds up threatening those who wish to speak up over social media about abuse or other social injustices as that could be construed as causing emotional distress (Fakhoury, 2013). In 2011 the federal anti-stalking law was applied to a man who posted criticism of a public figure on Twitter (U.S. v. Cassidy, 2012). While a federal judge dismissed the indictment on First Amendment grounds (Volokh, 2012), there is reason to worry these laws will be abused.

Feminists might find common cause with cyberliberties groups in other ways as well. Just as some feminists have emphasized the advantages of resisting sexual victimization through empowered resistance strategies such as self-defense (McCaughey & Cermele, 2015), electronic privacy advocates like the Electronic Frontier Foundation offer cyber-self-defense measures for encrypting one's data, and increasing awareness of ways to safeguard one's privacy rights. Although individual approaches to one's security in cyberspace have been criticized as neo-liberal fixes that neglect to target the perpetrating organization (see, e.g., Smith 2016), feminist self-defense scholars have argued that advocating such measures can be accompanied by strategies that target perpetrators. Feminist self-defense scholars, in joining the conversation about cyber-self-defense, would offer important insights to ensure that those cyber-self-defense recommendations do not parallel the recommendations in physical space that fail to connect with broader social changes or that constrict women's freedom and mobility. Just as in physical space, people in cyberspace can engage in cyber-self-defense that allows them freedom, autonomy, and agency, in ways that challenge rather than support the (cyber)rape culture. Indeed, Powell and Henry (2017, p. 254) argue that any cyber-self-defense strategies against technology-assisted sexual violence "must promote gender *and* digital equality".

As feminists know all too well when it comes to narratives around rape prevention, telling people who do not want to expose themselves to surveillance simply not to use information and communication technologies, even while these dominate our social world, takes for granted as inevitable the culture of predation and places undue burden on the potential victim. Advocating for information privacy need not make one anti-technology, just as fighting against rape need not make one anti-sex. When people get used to the invasions of electronic privacy that technologies have made so easy to accomplish, they risk coming to accept them as normal, inevitable, and necessary,

akin to resigning ourselves to the inevitability of (cyber)rape in a (cyber)rape culture. Just as there is a link between one's bodily autonomy and one's autonomy in our civil society, such a link exists between our informational privacy and our autonomy. A woman's (or anyone's) ability to determine when and how information about her is shared with others—whether that is through location tracking or other forms of surveillance based on our online activities, sexual or not—is a feminist issue.

Feminists historically opposed rape not because, circa the 18th Century, a woman was a man's property or the vagina a sacred flower, but because feminists value self-determination, autonomy, freedom, respect for boundaries, and privacy as necessary for full citizenship in a participatory democracy. For these very reasons, feminists have a powerful role to play in articulating and protecting online privacy rights, just as privacy advocates have a powerful role to play in opposing technology-facilitated sexual violence as invasions of sexual privacy. Acknowledging the parallels between cyberrape and dataraid not only helps protect civil liberties in an age of surveillance but also helps us see the harm in sexually aggressive violations as well. Put differently, our framework makes explicit the violation of boundaries and personal integrity in dataraid whilst highlighting the dataraid involved in technology-facilitated sexual violence. Understanding technology-facilitated sexual violence and dataraid as related forms of digital victimization could help scholars understand various forms of privacy invasion that disable autonomy and social participation. In today's digital surveillance culture, any defense of someone's sexual privacy online must necessarily also promote their information privacy online as well. Feminists and privacy advocates together might find a balance between privacy and safety as they work to protect every person's autonomy over the core components of their selfhood.

References

Anderson, K. L. & Cermele, J. (2014). Public/private language aggression against women. *Journal of Language Aggression and Conflict, 2*(2), 274-293.

Backe, E. L., Lilleston, P., & McCleary-Sills, J. (2018). Networked individuals, gendered violence: A literature review of cyberviolence. *Violence and Gender, 5*(3), 135-146.

Bates, S. (2017). Revenge porn and mental health: A qualitative study of the mental health effects of revenge porn on female survivors. *Feminist Criminology, 12*(1), 22-42.

Brief of Electronic Frontier Foundation et al. as *Amici Curiae* in Support of Respondents, City of Ontario, California, et al., v. Jeff Quon, et al., U.S. (2010) (no. 08-1132). Retrieved from https://www.eff.org/document/eff-amicus-brief-9

Browne, S. (2015). *Dark matters: On the surveillance of blackness.* Durham, NC: Duke University Press.

Brownmiller, S. (1975). *Against our will: Men, women, and rape.* New York: Simon & Schuster.

Cannatasi, J.A., Zhao, B., Vives, J. M., Monteleone, S., Bonnici, J. M., & Moyakine, E. (2016). *Privacy, free expression and transparency: Redefining their new boundaries in the digital age.* Paris, France: United Nations Educational, Scientific, and Cultural Organization.

Carmon, I. (2017, August 14). Paris Hilton is the hardest-working woman in the game. *Marie Claire*. Retrieved from http://www.marieclaire.com/celebrity/a28768/paris-hilton-mogul-dj/

Citron, D. (2019). Sexual privacy. *The Yale law journal 128*:1870-1960.

Clough, J. (2016). Revenge porn: Criminal law responses. *Precedent: Australian lawyers alliance 8*(132): Precedent 30. Retrieved from http://classic.austlii.edu.au/au/journals/PrecedentAULA/2016/8.html

Cohen, J. L. (1997). Rethinking privacy: Automony, identity, and the abortion controversy, in J. Weintraub & K. Kumar (Eds), *Public and private in thought and practice: Perspectives on a grand dichotomy* (pp. 133-165). Chicago, IL: University of Chicago Press.

Crocker, L. (2014, June 28). Too late to 'pologize for NSA revenge porn leak. *Daily Beast.* Retrieved from https://www.thedailybeast.com/too-late-to-pologize-for-nsa-revenge-porn-leak

Crooks, H. (2018). *Reel girls: Approaching gendered cyberviolence with young people through the lens of participatory video*. (Unpublished doctoral dissertation). University of Ottawa, Ottawa, Ontario. Retrieved from https://pdfs.semanticscholar.org/95d3/a2b4ee6022538d8bf9fee0c15c03e4a7478c.pdf

Dahl, J. (2013. April 12). Audrie Pott, Rehteah Parsons suicides show sexual cyber-bullying is 'pervasive' and 'getting worse,' expert says. *CBS News*. Retrieved from http://www.cbsnews.com/news/audrie-pott-rehtaeh-parsons-suicides-show-sexual-cyber-bulling-is-pervasive-and-getting-worse-expert-says

Datarape (2015). In *Urban dictionary*. Retrieved from https://www.urbandictionary.com/define.php?term=Data%20Rape).

Davies, M. & Rogers, P. (2006). Perceptions of male victims depicted in sexual assaults: A review of the literature. *Aggression and Violent Behavior*, *11*(4), 367-377.

Doyle, J. (2015). *Campus sex, campus security*. South Pasadena, CA: The MIT Press.

Dubrofsky, R. E. & Magnet, S. A. (Eds.). (2015). *Feminist surveillance studies.* Durham: Duke University Press.

Gender and electronic privacy (n.d.). *Electronic Privacy Information Center*. Retrieved from https://epic.org/privacy/gender/, accessed 15 October 2018.

Farrell, P. (2014, August 31). Nude photos of Jennifer Garner and others posted online by alleged hacker. *The Guardian.* Retrieved from https://www.theguardian.com/world/2014/sep/01/nude-photos-of-jennifer-lawrence-and-others-posted-online-by-alleged-hacker

Fisher, S. (2016). Review of the literature on gender and cyberviolence: Helping communities respond: Preventing and eliminating cyberviolence directed at girls and young women [White paper]. Retrieved from http://cyberviolence.atwaterlibrary.ca/wp-content/uploads/2016/08/Website-Literature-Review-Aug-2016-formating.pdf

Franks, M. A. (2017). "Revenge porn" reform: A view from the front lines. *Florida law review 69* (1251). September.

Furedi, F. (2004). *Therapy culture: Cultivating vulnerability in an uncertain age.* New York: Routledge.

Grosz, E. (1994). *Volatile bodies: Toward a corporeal feminism.* Bloomington, IA: Indiana University Press.

Halpern, M. (2014). Virginia Supreme Court unanimously supports academic freedom at the University of Virginia. Union of Concerned Scientists Blog. Retrevieved from https://blog.ucsusa.org/michael-halpern/virginia-supreme-court-unanimously-supports-academic-freedom-at-the-university-of-virginia-488?_ga=2.244507655.30239104.1574386655-61403008.1574386655

Hasinoff, A. A. (2015). *Sexting panic. Rethinking criminalization, privacy and consent.* Urbana: University of Illinois Press.

Holladay, K. (2016). An investigation of the influence of cyber-sexual assault on the experience of emotional dysregulation, depression, post traumatic stress disorder, and trauma guilt. *Unpublished doctoral dissertation*. University of Central Florida, Orlando, Florida.

hooks, b. (2015). *Feminism is for everybody: Passionate politics.* New York: Routledge.

Howard, J. A. (1984). The "normal victim": The effects of gender stereotypes on reactions to rape victims. *Social Psychology Quarterly, 47*(3), 270-281.

Kerr, I., Lucock, C., & Steeves, V. M. (Eds.). (2009). *Lessons from the identity trail: Anonymity, privacy and identity in a networked society.* New York: Oxford University Press.

Kipnis, L. (2017). *Unwanted advances: Sexual paranoia comes to campus*. New York: HarperCollins.

Lupton, D. (1995). The embodied computer/user. *Body and Society 1*(3-4), 97-112.

MacKinnon, C. A. (1989). *Toward a feminist theory of the state.* Cambridge, MA: Harvard University Press.

Mardorossian, C. M. (2014). *Framing the rape victim: Gender and agency reconsidered*. New Brunswick, NJ: Rutgers University Press.

Massoglia, D. (2014, December 23). The webcam hacking epidemic. *The Atlantic*. Retrieved from https://www.theatlantic.com/technology/archive/2014/12/the-webcam-hacking-epidemic/383998/

McCaughey, M. (2003, September/October). "Windows Without Curtains: Computer Privacy and Academic Freedom." *Academe 89*:5: 39-42.

McCaughey, M. & Cermele, J. (2015). Changing the hidden curriculum of campus rape prevention and education: Women's self-defense as a key protective factor for a public health model of prevention. *Trauma, Violence, and Abuse 18*(3), 287-302.

Mears, B. (2010, April 19). Supreme Court to hear texting privacy case. *CNN*. Retrieved from http://www.cnn.com/2010/CRIME/04/19/scotus.text.messaging/index.html, accessed 15 October 2018.

Michals, D. (1990). "Cyber-rape: How virtual is it?" In Fallon, D. (Ed.), *Technology and Society* (pp. 113-117). Madison, WI: Coursewise.

Mulder, E., Pemberton, A., Vingerhoets, A. J. J. M. (2019). The feminizing effect of sexual violence in third-party perceptions of male and female victims. *Sex Roles.* Retrieved from https://doi.org/10.1007/s11199-019-01036-w

No sexting on the job (2010, January 5). *Chicago Tribune*. Retrieved from http://articles.chicagotribune.com/2010-01-05/news/1001040281_1_workplace-privacy-boss-messages

Nude photo scandal rampant across U.S. military, not just Marines (2017, March 15). *RT News*. Retrieved from https://www.rt.com/usa/380165-nude-photo-scandal-military/

Orenstein, J. (2017). Judicial engagement with surveillance technology. *Connecticut Law Review,* 49 (5), 1719-1731.

Patteson, Z. (2004). Going online: Consuming pornography in the digital age. In: Williams L (Ed.), *Porn studies* (pp. 104-126). Durham, NC: Duke University Press.

Powell, A. & Henry, N. (2017). *Sexual violence in a digital age.* London, UK: Palgrave MacMillan.

Pracher, M. (1981). The marital rape exemption: A violation of a woman's right of privacy. *Golden Gate University Law Review,* 11, 717-757.

Privacy (n.d.). Electronic Frontier Foundation. Retrieved from https://www.eff.org/issues/privacy.

Puar, J. (2011). Ecologies of sex, sensation, and slow death. *Periscope/Social Text*, *22*(7). Retrieved from http://socialtextjournal.org/periscope_article/ecologies_of_sex_sensation_and_slow_death/

Rape (n.d.). In Merriam Webster dictionary. Retrieved from https://www.merriam-webster.com/dictionary/rape.

Renzetti, C. M., Edleson, J. L., & Bergen, R. K. (2017). *Sourcebook on violence against women* (3rd ed). Thousand Oaks, CA: Sage.

Roberts, D., & Vagle, J. (2016). Racial surveillance has a long history. *The Hill.* Retrieved from https://thehill.com/opinion/op-ed/264710-racial-surveillance-has-a-long-history

Savage, D. G. (2010, June 18). Supreme Court rules in favor of California police chief who read employee's texts. *Los Angeles Times*. Retrieved from http://articles.latimes.com/2010/jun/18/nation/la-na-court-worker-texting-20100618

Schneider, J. (2017, September 20). DOJ demands Facebook information from "anti-administration activists. *CNN*. Retrieved from http://www.cnn.com/2017/09/28/politics/facebook-anti-administration-activists/index.html

Šepec, M. (2019). Revenge pornography or non-consensual dissemination of sexually explicit material as a sexual offence or as a privacy violation offence. *International journal of cyber criminology* 13 (2): 418-438.

Shields, B. (2004). Computer privacy [Letter to the editor]. *Academe, 90*(1) 6-7.

Smith, A. (2015). Not-seeing: State surveillance, settler colonialism, and gender violence. In: Dubrofsky R E and Magnet S A (Eds), *Feminist surveillance studies* (pp. 24-38). Durham, NC: Duke University Press.

Smith, G. J. D. (2016). Surveillance, data and embodiment: On the work of being watched. *Body & Society* 22(2), 108-139.

Strahilevitz, L. (2005). Consent, aesthetics, and the boundaries of sexual privacy after Lawrence v. Texas. *DePaul Law Review* 54, 671-700.

Solove, D. J. (2013). *Nothing to hide: The false tradeoff between privacy and security.* New Haven, CT: Yale University Press.

Stech, K. (2014, February 6). Girls Gone Wild settles with exposed women. *Inforuptcy.* Retrieved from https://www.inforuptcy.com/news/wsjcom-bankruptcy-beat/girls-gone-wild-settles-exposed-woman-0

Surveillance Studies Network. (n.d.). An introduction to the surveillance society. Retrieved from https://www.surveillance-studies.net/?page_id=119

Terrill, W., Paoline, E. J. III, & Manning, P. K. (2003). Police culture and coercion. *Criminology* 41(4): 1003-1034.

Tyler Clementi's story (n.d.). *Tyler Clementi Foundation.* Retrieved from https://tylerclementi.org/tylers-story/

U.S. v. Cassidy, (n.d.). *Electronic Frontier Foundation*. Retrieved from https://www.eff.org/cases/us-v-cassidy

van der Ploeg, I. (2012). The body as data in the digital age of information. In K. Ball, K. D. Haggerty, & D. Lyon (Eds.), *Routledge handbook of surveillance studies* (pp. 176-183). Abingdon, Oxon: Routledge.

Vera-Gray, F. (2017). "Talk about a cunt with too much idle time: Trolling feminist research. *Feminst Review, 115*, 61-78.

Warshaw, R. (1988). *I never called it rape: The "Ms." report on recognizing, fighting, and surviving date and acquaintance rape*. New York: Harper & Row Publishers.

Welsh-Huggins, A. (2011, September 6). Ohio woman settles lawsuit over laptop sex images. *NBC News.* Retrieved from http://www.nbcnews.com/id/44415649/ns/technology_and_science-tech_and_gadgets/t/ohio-woman-settles-suit-over-laptop-sex-images/#.WltbJpM-ck8, accessed 15 October 2018.

BIO STATEMENTS

Martha McCaughey is a professor of sociology at Appalachian State University and an adjunct research faculty member in sociology at the University of Wyoming. McCaughey is the author of *Real Knockouts: The Physical Feminism of Women's Self-Defense,* the editor of *Cyberactivism on the Participatory Web,* and the co-creator of the blog See Jane Fight Back.

Jill Cermele is Professor and Chair of Psychology at Drew University and an affiliated faculty member of their Women's and Gender Studies program. Cermele has authored or co-authored a number of articles on women's resistance to violence and gendered issues in mental health, as is the co-creator of the blog See Jane Fight Back.