

Reasonable Expectations of Privacy in an Era of Drones and Deepfakes: Expanding the Supreme Court of Canada's Decision in *R v Jarvis*

Kristen Thomasen and Suzie Dunn


Abstract

Perpetrators of technology-facilitated gender-based violence are taking advantage of increasingly automated and sophisticated privacy-invasive tools to carry out their abuse. Whether this be monitoring movements through stalkerware, using drones to nonconsensually film or harass, or manipulating and distributing intimate images online such as deepfakes and creepshots, invasions of privacy have become a significant form of gender-based violence. Accordingly, our normative and legal concepts of privacy must evolve to counter the harms arising from this misuse of new technology. Canada's Supreme Court recently addressed technology-facilitated violations of privacy in the context of voyeurism in *R v Jarvis* (2019). The discussion of privacy in this decision appears to be a good first step toward a more equitable conceptualization of privacy protection. Building on existing privacy theories, this chapter examines what the reasoning in *Jarvis* might mean for “reasonable expectations of privacy” in other areas of law, and how this concept might be interpreted in response to gender-based technology-facilitated violence. The authors argue the courts in Canada and elsewhere must take the analysis in *Jarvis* further to fully realize a notion of privacy that protects the autonomy, dignity, and liberty of all.

Keywords: Reasonable expectation of privacy; equality; *R v Jarvis*; deep-fakes; drones; stalkerware

The Emerald International Handbook of Technology-Facilitated Violence and Abuse, 555–576

Copyright © 2021 Kristen Thomasen and Suzie Dunn

 Published by Emerald Publishing Limited. This chapter is published under the Creative Commons Attribution (CC BY 4.0) licence. Anyone may reproduce, distribute, translate and create derivative works of these chapters (for both commercial and non-commercial purposes), subject to full attribution to the original publication and authors. The full terms of this licence may be seen at <http://creativecommons.org/licenses/by/4.0/legalcode>.

doi:10.1108/978-1-83982-848-520211040

Introduction

Advances in technology over the past several decades have changed our understandings of what is considered “private” in relation to both location and information (Bailey, 2009; Scassa, 2010). Technologies such as drones, stalkerware, and hidden cameras have impacted our expectations of privacy. Traditional approaches to privacy law that drew a bright line between private and public spaces – a conceptual division that has not historically benefitted women (Allen, 1988) and has been rejected by many privacy scholars (Nissenbaum, 2010) – are further broken down by what we describe in the first section of this chapter as “technologies of exposure and control.” These technologies provide third-party access to once private realms and allow for the unwarranted gathering and sharing of private information in ways never seen before (Dodge, 2016; Khoo, Robertson, & Deibert, 2019). As privacy norms shift to incorporate these new technologies, it is important to acknowledge the ways in which privacy norms have and continue to neglect the interests of women and other marginalized groups (Bailey, 2014). As noted by Anita Allen (1988), women have had too much of the wrong type of privacy (requiring them to be modest in public or risk inviting privacy invasions, such as sexual harassment), and not enough of the right type of privacy (some privacy norms failed to protect women from gender-based violence in the private sphere, such as intimate partner violence, which was considered a private affair not deserving of state or outside intervention). Gendered privacy norms meant that experiences of domestic violence, workplace and street harassment, voyeurism, and stalking of women long went un- or under-protected in law (Balos, 2004).

Gendered privacy invasions have evolved in the digital era. Unfortunately, perpetrators of technology-facilitated gender-based violence are taking advantage of privacy-invasive tools that are increasingly sophisticated and user-friendly to carry out their abuse (Bailey & Mathen, 2019; Powell & Henry, 2017). Today, we grapple with issues of whether it is appropriate to take sexualized photos of women in public without their knowledge, dox¹ them without consent using facial recognition technology (FRT), replicate their images through technology in sexist ways, or trace their activities using tracking software or drones. Accordingly, our normative and legal concepts of privacy must evolve to counter the gender-based harms arising from this misuse of new technology. This evolution must include the court’s assessment of when a person can reasonably expect privacy against the use of these emerging technologies.

Oftentimes in the Canadian legal system, legal protection of privacy interests and remedies for invasions of privacy are framed around the concept of a “reasonable expectation of privacy” (REP). This concept of REP can serve as a legal threshold that a person claiming protection must establish. Generally, to assess a claimant’s REP, courts will consider the context of an alleged privacy invasion to determine whether an imagined “reasonable person” would have expected privacy in those circumstances. This may include considering factors

such as the location of the invasion, what was accessed, why it was accessed, how it was accessed, who accessed it, and/or the privacy interests in whatever was accessed. The most substantial REP jurisprudence in Canada emerges from Section 8 of the *Charter of Rights and Freedoms* (1982), which prohibits sanctionless state searches that interfere with one's REP, such as warrantless police searches (McGill & Kerr, 2012). However, REP is also significant when assessing whether other laws prohibit gender-based privacy intrusions, or where a survivor of such intrusions can seek compensation or another remedy (Aikenhead, 2018). For instance, Canada's voyeurism and nonconsensual distribution of intimate image offenses (*Criminal Code*, 1985, ss. 162 & 162.1) require an analysis of a claimant's REP in order to convict. Analysis of a plaintiff's expectation of privacy also arises in civil claims for invasion of privacy, and for the nonconsensual distribution of intimate images (e.g., *Jane Doe 72511 v Morgan*, 2018; *Intimate Images Protection Act*, 2018). Further, REP guides an analysis of whether police interview records, therapy records, or other intimate records related to a sexual assault complainant must be provided to an accused in a sexual assault criminal trial, engaging the complainant's privacy interests as well as the retraumatizing experience of a sexual assault trial (*R v Mills*, 1999; see also Gotell, 2006). In all of these cases, the REP concept is the conceptual hurdle to the legal system's denunciation of gendered privacy invasions.

When the courts address these privacy issues, we argue that they must consider equality as a guiding factor in the REP analysis in order to recognize and refute sexist and other discriminatory privacy norms that could otherwise be replicated alongside these new technologies (Aikenhead, 2018; Bailey, 2008). Canada's Supreme Court recently addressed technology-facilitated violations of privacy in the context of criminal voyeurism in *R v Jarvis* (2019). In this decision, the court listed several factors that could be relevant in a REP analysis under the voyeurism offense; however, it did not note equality as a specific factor. This was despite the case's relevant equality issues related to the gender and age of the complainant, and the argument by two intervenors that equality should be a relevant factor in the REP analysis. This decision appears to be a good first step toward a more equitable conceptualization of privacy protection (Bailey, 2020). However, we argue that neglecting to explicitly acknowledge equality as a distinct factor in the REP analysis was a missed opportunity. Including equality in the REP analysis is a necessary next step in the advancement of REP jurisprudence.

To provide a technological context to our privacy discussion, the first section of this chapter introduces examples of privacy-invasive technologies of exposure and control, highlighting the ways in which technology can be used for gender-based abuse. The chapter then moves on to a summary of *R v Jarvis* examining the REP framework it established. The subsequent section builds on previous privacy scholarship to discuss why and how equality could be considered when assessing expectations of privacy, particularly in response to the ways in which technologies of exposure and control are used to specifically invade the privacy of women and other equality-seeking groups. The chapter concludes with a summary of how the contextual approach to privacy in *Jarvis* (2019) must extend even further to address new technology-facilitated ways of exposing and controlling

one another that have significant equality impacts for privacy-marginalized groups, including women.

While the *Jarvis* (2019) decision arises out of a criminal law proceeding, we recognize that the criminal justice system is not necessarily a substantially effective or appropriate mechanism for addressing sexual and gender-based violence, like voyeurism, from the perspective of survivors, offenders, or society as a whole. Nevertheless, what the Supreme Court of Canada (SCC) has to say about privacy in general, and the nonconsensual collection and use of intimate images specifically, sets social norms. It is therefore important to examine these aspects of the decision, while simultaneously considering how we as a society can better respond to sexual violence (Thomasen & Dunn, 2019).

The Technological Landscape

Digital technologies are becoming increasingly sophisticated, compact, affordable, and user-friendly, changing the landscape of accessible tools that can be used to invade another person's privacy (Citron, 2019; Khoo et al., 2019). While these new tools often have beneficial social uses, they can also be used in privacy-invasive ways that target equality-seeking groups. In fact, some are specifically designed and marketed with the intention to invade people's privacy, including targeting women. Stalkerware has been advertised as a "girlfriend tracking" application (Parsons et al., 2019, p. 69), and facial recognition tools have been promoted to help people match strangers they find attractive in public places with their social media accounts, regardless of whether that person is interested in being identified (Royakkers, Timmer, & KoolRinie van Est, 2018; Walker, 2016). In this section, we define and look at examples of two groups of technology that we have termed "technologies of exposure" and "technologies of control" to explore the ways that technology shifts the ability of people to invade other people's privacy, thus impacting societal expectations of privacy. These groupings are not meant to be mutually exclusive, but rather allow us to focus on the new privacy-invasive capabilities that these technologies bring with them. We will highlight some of the ways these technologies are used to expose and/or control women and other equality-seeking groups.

Technologies of Exposure

Technologies of exposure are technologies that can be used to identify, share, publish, create, or decontextualize information about another person that they might not want discovered or used in a particular context.² This section reviews several current examples of technologies of exposure that have facilitated gendered privacy intrusions, including the use of FRT to identify women without their consent (Brinckerhoff, 2018); social network platforms used to dox women (Rothrock, 2016); deepfake videos (Chesney & Citron, 2019); and creepshots (Laidlaw, 2017). The examples cited in this section help demonstrate how these technologies are specifically, though certainly not exclusively, targeted against

women. Abusers of this technology expose women's information to intentionally draw unwanted attention to them, sometimes encouraging groups of people to collectively harass the exposed individual (Citron, 2014). They typically draw attention to women in ways that sexualize their everyday activities, shame them for engaging in sexual activity, or threaten them for transgressing patriarchal gender norms (Hargreaves, 2014; Henry & Flynn, 2019; McGlynn, Rackley, & Houghton, 2017). Decontextualized information further reinforces sexist ideas about women, such as publishing collections of images on "revenge porn" or creepshot sites that suggest women deserve to be sexually objectified and criticized, and that men are entitled to view and sexualize images of their bodies without their consent (Dunn & Petricone-Westwood, 2018; Henry & Flynn, 2019). This can cause women to disengage from digital spaces, puts them at risk of harassment and violence, and creates additional burdens for women who feel the need to modify their self-expression to avoid being exposed (Powell & Henry, 2017), as is discussed at further length in the next subsection on technologies of control.

Facial Recognition and Doxing

FRT uses biometric data to map a person's facial structure to identify the individual by matching data points from their image to previous images of them (Introna & Nissenbaum, 2011). Many facial recognition systems have been notoriously unreliable, particularly with respect to accurately identifying people of color, and women of color more specifically, as the data sets used in these programs have not included a wide diversity of images of these groups of people to learn from (Buolamwini & Gebru, 2018; Grother, Ngan, & Hanaoka, 2019). Nevertheless, some designers boast statistically significant accuracy rates in identifying the targeted person (Lippman, Cassimatis, & Renn, 2019). Disturbingly, this technology has been used to identify and dox women who appear in sexual content online. Both individual hobbyists and organized groups have used FRT for this purpose. For example, many sex workers choose not to associate their real names or contact information with their online sexual content for privacy or safety reasons (Nelson, 2019). In 2016, there were media reports that a group in Russia used a facial recognition app, FindFace, to create a database that matched images of female escorts and pornography actors with their social media profiles (Rothrock, 2016). Once matched with their social media information, the group shared the women's sexual content with their family and social media contacts, and publicly posted their identifying information and contact information, encouraging others to harass the women (Rothrock, 2016). In May 2019, a computer programmer, Li Xu, published a post on Weibo claiming he had used FRT to identify over 100,000 women from adult pornography videos by cross-referencing their images with images he had scraped from social media sites. The stated purpose of his program was to allow men to find out if their girlfriends had ever been featured in sexual content online (Dickson, 2019). Neither Xu nor the FindFace group used this technology to expose the men featured in the sexual content.

Sex workers are not alone in being targeted for appearing in sexual content online by technologies of exposure. Some users of websites hosting so-called “revenge pornography,” child pornography, or sexual exploitation content identify and reveal the names and contact information of the people in these images (Powell & Henry, 2017; Powell, Henry, & Flynn, 2018). Young women who were coerced into being featured in the popular GirlsDoPorn videos were often doxed in the comments section of the videos once they were published on Pornhub without their consent. The women featured in these films were typically promised that the videos would not be posted on the internet. Once viewers identified the cities and towns the women lived in, they would share the sexual content with members of that community and harass the women featured in the films (Cole, 2019). This causes fear in the women who were doxed and encourages mob harassment (Citron, 2014), which is closely connected to issues of control discussed below, in particular, the intended and practical silencing of women’s contributions online.

Deepfakes

The term “deepfake” refers to the use of “deep learning,” or machine learning techniques, to create “fake” images or videos of people. This is done using an artificial intelligence technique that maps out the details of a person’s face in order to superimpose that person’s face onto the face of another person in a video (Chesney & Citron, 2019). Deepfakes have gained recent attention out of concerns that malicious actors could use this technique to create disruptive fake political videos (Caldera, 2019). However, a recent report by Deeptrace Labs found that 96% of all deepfake videos were pornographic and nonconsensual videos made of women (Ajder, Patrini, Cavalli, & Cullen, 2019). While this technique can also be used in ways unrelated to gender and gender-based abuse, creating an opportunity for new forms of reputational and dignitary abuse (as a woman’s face can be superimposed on any number of base videos, not just sexual ones), these videos most often bring unwanted sexual attention to the targeted women and can negatively impact their sexual autonomy by presenting them in sexual scenarios in which they did not participate (Flynn, 2019; Henry et al., 2020).

Discrete Camera Technology

Discrete and high-resolution cameras constitute a technologies of exposure when used for gender-based privacy invasions colloquially called “creepshots” (Burns, 2018). Creepshots are photos taken using cameras, sometimes hidden in everyday objects such as pens or shoes. These cameras are concealed so that they can be used to take pictures of women’s bodies without their consent or awareness while they are out in public. The women in the images are typically clothed, but the images are focused on their bodies in a sexualized manner and can be posted online along with other sexual commentary (Tran, 2015). Some photos are taken up a woman’s skirt or down her blouse, known as “upskirting” or “down-blousing” (Flynn & Henry, 2019; McGlynn, Rakley, & Houghton, 2017). It is not just the camera

technology that allows for creepshots, but the ability to share the images with a larger audience online. The images on creepshot websites, forums, and hashtags are almost exclusively focused on women (Thompson & Wood, 2018). In Canada, a man hosted a “CanadaCreeps” Twitter page where he had over 17,000 followers and posted images of women and girls to the account who were photographed without their knowledge while walking in public (Laidlaw, 2017). Research has shown that the allure of creepshots includes taking the image of a woman without her noticing, and then consuming it without her consent (Burns, 2018; Oliver, 2016). This is made easier through technological improvements that increase the resolution and decrease the size of cameras, making them more discreet and operable at greater distances, fueling this form of privacy intrusion. These exposure concerns also arise in relation to drone technology, discussed below as a technology of control.

Technologies of Control

Technologies of control are those that can be used to monitor, track, or observe the conduct and activities of a person in ways intended to either cause that person to self-regulate their behavior or permit someone else to control or affect their behavior, such that they do not feel free to do as they please. Studies have shown that surveillance technologies can cause a person to alter or self-censor their behaviors if they believe they are being watched (Manokha, 2018). Much has been written about the panoptic effect of technology – where the feeling of being observed (sometimes even without actually being observed) limits one’s sense of freedom to act, move, or speak as they would otherwise (e.g., Koskela, 2000; Koskela, 2002a). Surveillance technologies that monitor, track, follow, and report back to another contribute to different forms of self-regulation or avoidance of different spaces and the sense of an external exertion of control over how the targeted individual conducts their daily life. These technologies can also build on the disempowering effects of unwanted exposure by subjecting individuals on an *ongoing* basis to monitoring and potential subsequent exposure, or the sense thereof. Surveillance technologies like drones and spyware/stalkerware make monitoring – or even just the perception of it – easier to carry out, and in some cases these technologies permit fully automated monitoring. Similar to the targeting by technologies of exposure noted in the previous section, technologies of control are often specifically targeted toward women and other equality-seeking groups (Bailey, 2020; Gilliard, 2020; Waldman, 2019; see also Anderson, 2015). The following subsections discuss two examples of emerging technologies of control that will challenge the way privacy expectations are currently understood by Canadian precedents: drones and stalkerware.

Public Space Drone Surveillance

Countless examples of the use of drone technology to spy on and harass women in public spaces have made media headlines in recent years, to the point of becoming a notable (and overly simplistic) media trope (Kaminski, 2013; Thomassen, 2018).

Drone technology is becoming increasingly accessible on the consumer market in terms of availability and cost. Because a drone operates remotely from its pilot – with ranges commonly up to several hundred meters – the technology can overcome not only physical barriers like fences and walls but also normative barriers, like expectations that a person will not take photographs in a particular location, or stare at someone for too long. Drone technology has been used to film or photograph women on their balconies, in backyards, on public beaches, and at public pools. Instances of drones being used to stalk, intimidate, and harass women have been cited in different countries (see examples in [Thomasen, 2018](#)). These encounters can affect how targeted individuals are able to freely access, use, and enjoy public and publicly visible spaces, risking inequitable exclusion from or enjoyment of these spaces.

The features of drone technology – including its remote operation, aerial overhead nature, and increasing commercial availability – give it the potential to exacerbate existing privacy-invasive experiences of unwanted monitoring and photography, street harassment, and intimidation, in terms of both the frequency and the quality of the experience ([Davis, 1994](#); [Koskela, 2000, 2002b](#); [Thompson, 1993](#); [Vera-Gray, 2016](#)). Footage collected by a drone can take on a further invasive quality when posted and shared online, leading to exposure concerns such as those discussed in the sections above.

Spyware/Stalkerware

Commercially available applications of spyware can be installed on mobile devices and used to illicitly track the location of, and gather information from, a device and share it with another person ([Parsons et al., 2019](#)). Spyware can be used for a range of malicious surveillance activities, but numerous investigations have revealed a gendered dimension to the use of spyware. Citizen Lab recently released two reports on stalkerware (spyware used for the purpose of surveillance in contexts of intimate partner violence). The reports, among other things, emphasize the frequent use of different spyware apps in the context of intimate partner violence, often targeted at spying on women specifically ([Parsons et al., 2019](#)), and assess legal and policy responses to this technology ([Khoo et al., 2019](#)). The reports emphasize the ways in which this technology can be used (and in some cases, is specifically designed) to exert control and power over another individual. As the authors explain:

Spyware has a wide range of capabilities, including pervasive monitoring of text and chat messages, recording phone logs, tracking social media posts, logging website visits, activating a GPS system, registering keystrokes, and even activating phones' microphones and cameras, as well as sometimes blocking incoming phone calls. These capabilities can afford dramatic powers and control over an individual's everyday life. And when this software is used abusively, it can operate as a predator in a person's pocket, magnifying the pervasive surveillance of the spyware operator.

Intimate partner violence, abuse, and harassment is routinely linked with efforts to monitor and control a targeted person. As new technologies have seeped into everyday life, aggressors have adopted and repurposed them to terrorize, control, and manipulate their current and former partners. (Parsons et al., 2019, p. 25)

This technology, like the ones discussed above, is not the reason that control and monitoring occurs in intimate partner relationships and elsewhere, but it alters the ease and secrecy of collection, and the quantity and quality of monitoring in ways that are poorly restricted by the current legal system. These new technologies also do not create or cause gendered violence, but emerging technologies do make such exposure and control easier to carry out, expanding and potentially deepening the range of privacy intrusions experienced by women and other equality-seeking groups.

Each of the above technologies generates new sociolegal challenges and exacerbates gendered and systemic privacy challenges, to which legal and other institutions must adjust and respond. We argue that one crucial component of this response will be for courts to recognize the ways in which privacy invasions can reflect inequality, and to incorporate an analysis of this reality into the legal protections of privacy. In particular, into the concept of REP which serves as a threshold for obtaining legal recourse.

Technology and Equality-conscious Assessments of Privacy Expectations

The above section demonstrates how emerging technologies have been used to, or in some cases are explicitly designed to, permit gender-based invasions of privacy. These technologies exacerbate systemic privacy challenges by increasing the quantity and changing the quality of intrusions and by taking advantage of weaknesses in legal protection. The selective targeting of women in these examples is central to understanding how equality and privacy issues intersect. In other words, some groups are more targeted for privacy invasions and less protected by law because legal protections were not historically developed to respond to their privacy experiences. Accordingly, new theoretical approaches are needed to better address this disparity. We need approaches that take equality into account, particularly when considering the legal understanding of a REP. Several privacy laws that require a REP analysis, including those prohibiting voyeurism and nonconsensual distribution of intimate images, were enacted in Canada specifically in response to privacy violations that typically target vulnerable groups, including women and children (Bailey, 2020; Department of Justice, 2002; Department of Justice, 2013), yet do not explicitly address equality. The introduction of these laws helps protect against gender-based privacy invasions (Bailey, 2016; Dunn & Petricone-Westwood, 2018). However, we argue that although the courts are moving toward a contextual approach that could support

an equality analysis (Bailey, 2020), the gendered and equality impacts of these invasions are not sufficiently addressed in the courts' privacy analysis as it stands.

The SCC recently considered the privacy-invasive nature of technology-facilitated voyeurism in *R v Jarvis* (2019). The next subsection outlines the SCC's decision. While the decision had many positive features, it neglected to explicitly consider equality as a factor in the privacy analysis. The following subsection discusses why this is a problem and outlines some theoretical approaches that could help decision-makers integrate equality into the REP analysis in the future.

R v Jarvis: Reasonable Expectation of Privacy Analysis

The criminal voyeurism appeal in *R v Jarvis* (2019) asked the SCC to consider whether young women had a REP in the semipublic place of their high school. Ryan Jarvis, a teacher, had been using a camera hidden in a pen to secretly take photos of his female students while they were on school property, for his personal sexual use. Dozens of videos found on the device focused predominantly on his female students' breasts and upper bodies.³ One of his female colleagues was also the focus of his recordings.

Jarvis was charged with voyeurism under a *Criminal Code* provision that hinges on whether the complainants had a REP in the circumstances in which they were recorded. At the trial level, Jarvis was acquitted, as the court did not conclusively find the images were taken for a sexual purpose. The Ontario Court of Appeal upheld the acquittal, however, this time on the basis that the young women did not have a REP. This assessment was based on the fact that the girls were in a semipublic space in their school at the time of the recording; that there were CCTV security cameras in the school and students were aware they were being filmed by those cameras; and the girls' bodies were available for public gaze because they were not completely concealed by conservative clothing. That decision was overturned by the SCC, which recognized the privacy expectations of the women filmed by Jarvis.

The majority of the SCC recognized that privacy expectations are not solely predicated on whether the girls were in a public or a private space, finding instead that the determination must be based on a variety of contextual factors. The relative privacy of the space was only one factor to consider among many. Chief Justice Wagner, for the majority, noted a nonexhaustive list of nine factors relevant to assessing the complainants', and any future complainant's, REP under the voyeurism offense, including:

- The location the person was in when she⁴ was observed or recorded;
- The nature of the impugned conduct, that is, whether it consisted of observation or recording;
- Awareness of or consent to potential observation or recording;
- The manner in which the observation or recording was done;
- The subject matter or content of the observation or recording;

- Any rules, regulations, or policies that governed the observation or recording in question;
- The relationship between the person who was observed or recorded and the person who did the observing or recording;
- The purpose for which the observation or recording was done; and
- The personal attributes of the person who was observed or recorded (*R v Jarvis*, 2019).

Applying these factors, the majority of the Court found that the complainants in this case did have a REP against being secretly recorded by their teacher for a sexual purpose, even though they were in a semipublic place. In particular, the majority emphasized that Jarvis's use of technology to collect sustained, focused, and long-lasting images engaged the students' reasonable expectations of privacy in the semipublic spaces of their high school.

At the SCC hearing, two interveners argued that equality should be a factor in the REP analysis given the gendered dynamic at issue in this case and in voyeurism more generally, putting the Court on notice that equality could be a relevant issue to address in the REP analysis (CIPPIC, 2019; LEAF, 2019). In the end, the Court did not list equality as a factor to consider, nor did it specifically address the gendered nature of the privacy invasion at issue in this case. As previously noted by Moira Aikenhead (2018) and Jane Bailey (2020), while this decision moves the REP analysis closer to an equality-focused approach to privacy, it was a missed opportunity to include equality in the analysis, leaving a critical gap in Canadian privacy jurisprudence.

Equality

As demonstrated in the previous sections, the development and use of privacy-invasive technologies are not neutral. Technology, like the camera pen used by Jarvis or drones used to photograph women, have disparate impacts on equality-seeking groups who are uniquely targeted (Thomassen, 2018). Not only are women the primary targets of creepshots (Burns, 2018) and deepfakes, technology like stalkerware has been overtly marketed to surreptitiously invade women's privacy and monitor their private moments, communications, and life choices (Parsons et al., 2019). Women with intersecting marginalities are further targeted by invasive technologies. LGBTQI people have had their sexual orientation or birth sex "outed" and exposed to homophobic social groups in ways that put them at risk (Ashley, 2018; Waldman, 2019). Racialized women activists have been stalked and tracked online due to their race and gender, including by governments and law enforcement (Amnesty International, 2018; Office of the Privacy Commissioner of Canada, 2013). When private or identifying information is published online, it has been paired with derogatory sexist, racist, and homophobic commentary and images (Jane, 2014). These privacy invasions are specifically tied to equality factors such as gender, sexuality, and race. This discriminatory targeting and marketing, combined with the challenges that targets

face in having protective laws applied or enforced, results in inequality that must be addressed by the legal system (Citron, 2019; Dunn, Lalonde, & Bailey, 2017; Khoo et al., 2019). Without directly recognizing this inequality, the legal system risks neglecting discriminatory norms that impact equality-seeking groups' autonomy and signaling that important equality factors in privacy are not worth directly addressing.

Inequality in privacy is nothing new, modern technologies only reemphasize the need to acknowledge equality when considering REP. Privacy norms, and the laws that protect them, illuminate the ways in which dominant groups have controlled who benefits from privacy protection – or the lack thereof. Whether it be legally permissive male access to women's bodies (Koshan, 2017), institutionally sanctioned homophobic invasion of LGBTQI spaces (Bérubé, 2003), or colonial surveillance of Indigenous, Black, and racialized people (Browne, 2015; Choudry, 2019; Crosby & Monaghan, 2018; Magnet, 2011; Tulloch, 2018), examining *whose* privacy is protected and whose is permissibly breached, both historically and currently, exposes the lived impacts of privacy norms on equality-seeking groups.

In order to properly address systemic and substantive equality issues related to privacy, legal decision-makers must explicitly inform privacy law-making and enforcement with equality in mind. Without considering equality, the law only grants permeable protection to those vulnerable to intrusions due to their social location. On the surface, it would seem that the SCC considered some factors that could be affiliated with equality in their REP analysis in *Jarvis* (2019). Factors such as the personal attributes of the individual targeted or her relationship to the perpetrator could be used to address some of the power imbalances that are rooted in inequality. In fact, the Court recognized the girls' youth as a factor that contributed to their REP. However, the Court was surprisingly quiet on how their gender influenced their REP, despite the highly gendered nature of this crime. As noted by Jane Bailey (2020), neglecting equality leaves the burden on future victims to weave an equality argument into the REP analysis within the current factors. If equality had been explicitly recognized as a factor relevant to REP, we believe the Court would need to actively examine whether the claimants were members of an equality-seeking group and how that may impact their experience of privacy and their REP. This recognition and analysis from the Court would go a long way in countering discriminatory privacy norms.

Integrating Equality into the Reasonable Expectation of Privacy Analysis

The SCC's decision in *Jarvis* (2019) was a clear step forward in addressing many concerns regarding the advancement of technology and its impact on privacy norms (Thomasen & Dunn, 2019). The Court acknowledged how a recording device allows for a level of scrutiny and permanence that is fundamentally different than human observation and permits repetitive viewing. The recording device also allows for the potential redistribution of the images in question. Beyond the important recognition that technology changes the REP analysis, the Court also recognized the role that the relationship between the person using

technology to invade privacy and the person targeted plays in the REP analysis, as well as the personal attributes of the person targeted (*R v Jarvis*, 2019). These factors can be used to understand some of the issues of power and vulnerability that affect privacy invasions. The Court in *Jarvis* (2019) noted the power imbalance between the teacher and his students and the vulnerability of the young people filmed. However, while these factors may provide space for courts to recognize the effect of inequalities between the specific parties in a particular case, the factors as they stand now do not go far enough to ensure systemic inequalities will be addressed in the REP analysis. This was a significant gap in the REP framework set out by the SCC.

In this section, we examine some of the ways the court could have incorporated equality into the decision in *Jarvis* (2019). Drawing on several privacy theories, we highlight a selection of equality issues that were central to this case and argue that including these considerations would have led to a more fulsome decision that could better address substantive equality in this case and future cases. We suggest that acknowledging equality in the REP analysis by actively examining the intersecting social locations of the individual(s) targeted, the challenges women and other equality-seeking groups face in remaining obscure, and the ways that inequality affects the capacity to trust would encourage an analysis that more adequately addresses privacy in the technological age.

First, by incorporating equality into the analysis, courts would be expected to recognize the ways in which an individual's social location will influence their experiences of privacy. The Court in *Jarvis* (2019) included the personal attributes of the claimants in the list of factors to consider in the voyeurism REP analysis, something that could allow equality factors like age and gender to be addressed. This "personal attributes" factor creates space for an equality-based argument from claimants, but it does not go far enough. It does not require courts to address equality considerations directly and explicitly. Ideally, courts would take an intersectional approach to acknowledge the ways in which gender and other sites of oppression can change the quality and quantity of privacy intrusions, and accordingly strengthen one's REP.

For instance, in applying this factor in *Jarvis* (2019), the Court noted the young age of the claimants and the particular vulnerability of young people. However, the claimants were not specifically targeted or made vulnerable solely because they were *young* people. No young boys were the focus of Jarvis's films. Furthermore, it is often overlooked that Jarvis not only filmed his young female students but also filmed an adult female colleague, suggesting youth alone was not the reason for his focus. The social location in terms of *both* the age and gender of the complainants was relevant in this case, as was pointed out by two interveners. Yet gender was not noted as a relevant personal attribute of the claimants by the Court, even though all shared the same gender. Had the Court been expected to look to equality factors, we argue that both age and gender would likely have been addressed, and importantly, the analysis of Jarvis's conduct would have more fully reflected the claimants' lived experiences and expectations of privacy – enhancing their REP against this use of technology that deepens (and creates a permanent record of) existing social vulnerabilities.⁵

For the courts to ensure equal protection of privacy interests, judges must resist any formalist application of the law and recognize that because different groups of people have different lived experiences of privacy, protection needs to respond to, rather than overlook, those differences. [Anita Allen \(1988, 2010\)](#) has found that women, people of color, and LGBTQI people have not historically benefited from privacy norms and laws in the same ways as cis-gender white men (see also [Allen & Mack, 1991](#)). Certain groups face repetitive and sometimes daily privacy invasions as part of their reality. As women and girls experience more regular invasions of privacy, there is a cumulative effect in addition to the specific effect of each invasion. Street harassment, digital stalking, doxing, and the decontextualization of their sexuality can cause women to avoid certain behaviors or spaces in anticipation of privacy invasions ([Henry et al., 2020](#)). This denies women the respite, anonymity, and self-exploration that others might enjoy in physical and digital public spaces ([Allen, 2000](#); [Citron, 2019](#)).

Inequitable privacy norms can be seen in the ways in which others, particularly those in dominant groups, might feel entitled to invade a woman's privacy by inquiring about or touching her body, questioning the legitimacy of her gender or sexual expression, commenting on her in digital spaces, or tracking her movements through public space, depending on her intersecting social locations. A pregnant Indigenous ciswoman ([Ridgen, 2020](#)) may experience privacy-related interactions differently than a transgender lesbian ([Ashley, 2018](#)), or a woman experiencing a long-term disability (*Milner v Manufacturers Life Insurance Company, 2005*), though all should be entitled to equal legal protection for their REP, even if what is necessary and reasonable differs based on circumstances and identity factors.⁶

The specificity and regularity of privacy invasions can cause many women and girls to have a heightened awareness that their privacy may be unfairly invaded. Overlooking that reality obscures an essential part of the harm women experience, including the reasons why they may have a different sense of what is "reasonable" in regards to their privacy and the role the courts should play in correcting these societal harms.

In the case of *Jarvis (2019)*, the young girls Jarvis filmed faced higher risks of having their images taken and sexualized in general due to the societal hypersexualization and fetishization of young women's and teen girls' bodies, as we have seen is the case in voyeuristic creepshots ([Burns, 2018](#)). If the REP analysis is meant to be based in the circumstances of the case, the scope of these circumstances must expand to address systemic realities. Courts must recognize how inequality contributes to the normalization of certain types of intrusion and condemn discriminatory privacy norms as "unreasonable" in their REP analysis. This should be the case regardless of who is carrying out the intrusion – be it the state, a company, or a private individual.

Second, building on the recognition of differing privacy experiences between equality-seeking groups, courts also need to recognize the ways in which circumstantially dominant groups (i.e., the members of this group might change depending on the circumstances) can rely on normative privacy protections that

are not always available to minority groups, and fill in those gaps with law. Woodrow Hartzog (2018) has defined the concept of “obscurity” as

...the notion that when our activities or information are unlikely to be found, seen or remembered, it is, to some degree, safe. People calculate risk every day based on how obscure they are or are likely to be. (p. 108)

Women’s, girls’, and many transgender people’s bodies do not remain obscure in the same way cis-men’s and boys’ do, and as such they are not able to take the same kinds of risks in regards to their sexual and gender expression (Ashley, 2018; Dodge, 2016). For example, women are much more likely to be policed for their sexual conduct on digital platforms (Powell & Henry, 2017), targeted by sexual deepfakes (Chesney & Citron, 2019), doxed if they are sex workers (Rothrock, 2016), and experience violence due to the outing of their transfeminine gender identity (Ashley, 2018).

A person’s social location can draw unwanted attention toward them, as was the case for the girls and woman in *Jarvis* (2019). Due to their gender, they could not benefit from obscurity in the ways that the men and boys in the school were able to. Incidents like these can influence how girls and women in the future perceive privacy in their schools and workplaces, diminishing the benefits they have in these spaces as their expectations of these types of privacy invasions are heightened (even though they should not *reasonably* have to expect such targeting). In addition, where technology makes intrusive conduct easier or allows conduct to become more deeply intrusive, it undermines one’s expectations that physical and normative barriers will protect against different types of invasions (Hartzog, 2018). This can be seen in the increasing ease of surveillance and control of women that accompanies increasingly automated and remote technologies like drones and spyware apps that provide access to once private spaces and information (Khoo et al., 2019; Thomassen, 2018). Technologies like Jarvis’s camera pen overcome the practical barriers that would otherwise prevent his long-term visual access to the complainants’ bodies.

The SCC introduced the idea of privacy by obscurity into its *Jarvis* (2019) factors by emphasizing the differences between human observation and a recording. Obscurity that might exist in human forgetfulness or the fleeting nature of an interaction is lost when the interaction is recorded and becomes storable and sharable. Yet, if equality had been recognized, the Court could have taken notice of who is more likely to be captured by these technologies by voyeurs, not just how these technologies change the observation. Canadian case law clearly demonstrates that women and girls are less likely to benefit from obscurity when it comes to voyeuristic recordings as they are the primary targets of voyeurs (Bailey, 2020). Women and girls walking in public for everyday reasons or engaging in normal activities in private spaces are more likely to have their photos surreptitiously taken by people who want to collect and share photos of women they find sexually attractive (Burns, 2018). As

such, a woman's ability to remain obscure is limited in a way that the obscurity of a man in the same situation is not. Of course, men's obscurity might be affected by their social locations in other ways, as is the case of men on gay dating apps (Waldman, 2019), or Black men targeted for greater police scrutiny in public spaces (OHRC, 2018), a reality that similarly must be accounted for in the REP analysis. This amplified scrutiny can be better accounted for in the REP analysis through, among other things, a recognition of the ways in which certain people gain privacy protection through obscurity that those in equality-seeking groups may not. Members of equality-seeking groups should nevertheless be entitled to reasonably expect the same amount of privacy protection as others. The REP analysis should fill any practical gaps in obscurity created by invasive technologies, recognizing that everyone should be entitled to reasonably expect the same amount of privacy by obscurity, even if in practice those experiences differ.

Finally, by considering the relationship between the parties as a factor in the *Jarvis* (2019) REP analysis, the SCC implicitly acknowledged that trust can serve as an important mechanism for expecting privacy when sharing information or space with others (Hartzog, 2018; Richards & Hartzog, 2017; Waldman, 2018). This relationship factor allows for a consideration of what a claimant should reasonably be able to expect, for instance, in what should be a trusting relationship between students and a teacher. Recognizing the importance of trust in this relationship helps to mitigate the vulnerability and power imbalance that can arise when sharing information or space in the context of such a relationship (Waldman, 2018). However, similar to obscurity, the Court could have taken this analysis a step further and recognized the ways in which trust, as a mechanism for subjectively experiencing privacy, is inequitably distributed in society. Due to the gendered nature of the common misuses of invasive technologies, such as Jarvis's use of a hidden camera, and systemic gendered norms, such as the societal hypersexualization of teen girls' bodies, women and girls may have legitimate reasons to be less trusting in certain circumstances, even in what should be relationships of trust (Powell & Henry, 2017). The court in its REP analysis should be prepared to supplement the interpersonal trust that individuals are able to rely upon in their lived experiences, even where claimants lose out due to their social location. In fact, one of the students filmed by Jarvis has since reported that she now lives in fear of people she thinks may be taking photos of her (Dodge, 2020). Her day-to-day expectation of privacy through trust has been undermined as a result of her experience. The courts must nevertheless assure that her equal access to legal protection of her privacy, including through trust, remains intact.

The Court's reasoning in *Jarvis* (2019) lays important precedential groundwork to justify further nuancing of REP analyses, both under the voyeurism offense and hopefully in other areas of the law as well. We argue that equality should be explicitly incorporated as a guiding factor in the REP analysis in order to prompt courts to consider the systemic conditions that impact claimants' expectations and experiences of privacy.

Conclusion

The technologies of exposure and control highlighted in this chapter reveal some of the equality issues that arise when considering a person's REP. With gendered privacy violations on the rise, it is time for the courts to consider equality in their REP analysis. While the SCC decision in *Jarvis* (2019) took positive steps toward a REP analysis that addresses privacy issues in an era of modern technology, it did not go far enough. Gendered privacy invasions have shaped the introduction of privacy laws in Canada, including laws prohibiting the nonconsensual distribution of intimate images and voyeurism, but the equality factor has yet to be adequately addressed by legislators and the courts. For privacy laws to be effective at addressing the realities of deepfakes, creepshots, drones, and stalkerware, the courts must explicitly examine the ways these technologies impact equality-seeking groups.

In this chapter, we highlighted how women and other equality-seeking groups may not share equal benefits from obscurity and have legitimate trust concerns that impact their privacy experiences due to their social location. Courts need to recognize this reality. Including equality in the REP analysis would not only provide a more fulsome understanding of the privacy questions before the courts, but decisions that address equality would assist in denouncing privacy norms that rely on discriminatory standards to minimize the severity of certain types of invasions. Excluding equality from the REP analysis minimizes the lived experiences of members of equality-seeking groups and misses a key contextual factor in the REP analysis. For our laws to truly address privacy breaches in modern society, equality must be a factor.

Notes

1. Doxing is the unwanted publication of private or identifying information, such as a person's name, address, and contact information.
2. For an understanding of contextual integrity in relation to privacy, see [Nissenbaum \(2010\)](#).
3. Madison Woodburn, one of the complainants in this case, fought to lift a publication ban that prevented her from speaking firsthand about her experiences throughout the criminal investigation and court proceedings ([Dodge, 2020](#)).
4. It is worth noting that the SCC used female-gendered pronouns when referring to the neutral singular person throughout the decision, and its hypotheticals exclusively featured women or girls as the victims, suggesting that the Court may have been alert to the gendered impacts of the voyeurism offense.
5. No details were provided about other social identity factors about the claimants and we recognize there may have been other equality issues at stake here that could have been addressed.
6. The privacy rights and interests of Indigenous women in Canada have too long been overlooked in Canadian colonial state policies. For example, pregnant Indigenous women are statistically more likely to have their births reported to social services through a "birth alert" system that flags their files to social services, increasing the chances that their child will be taken into state care at birth.

Additionally, Canadian criminal and privacy law fail to account for the dignitary interests and privacy expectations of transgender individuals in the ways they do cis individuals. Transgender people who want to choose when to disclose their status as a transgender person may be forced to disclose due to heteronormative and transphobic concerns of gender fraud. Further, privacy law has been permissive of intense public space scrutiny of individuals who claim insurance benefits for workplace injuries and long-term disabilities. These are just some examples of the ways a person's social location and status in an equality-seeking group will affect the privacy norms surrounding them and what sort of intrusions the courts determine they should expect.

References

- Aikenhead, M. (2018). A 'reasonable' expectation of sexual privacy in the digital age. *Dalhousie Law Journal*, 59(2), 273–300.
- Ajder, H., Patrini, G., Cavalli, F., & Cullen, L. (2019). *The state of deepfakes: Landscape, threats, and impact*. Amsterdam: Deeptrace.
- Allen, A. (1988). *Uneasy access: Privacy for women in a free society*. Totawa, NJ: Rowan & Littlefield.
- Allen, A. (2000). Gender and privacy in cyberspace. *Stanford Law Review*, 52, 1175–1200.
- Allen, A. (2010). Privacy torts: Unreliable remedies for LGBT plaintiffs. *California Law Review*, 98(6), 1711–1764.
- Allen, A., & Mack, E. (1991). How privacy got its gender. *Northern Illinois University Law Review*, 10, 441–478.
- Amnesty International. (2018). *#ToxicTwitter*. London: Amnesty International.
- Anderson, E. (2015). The white space. *Sociology of Race and Ethnicity*, 1(1), 10–21.
- Ashley, F. (2018). Genderfucking non-disclosure: Sexual fraud, transgender bodies, and messy identities. *Dalhousie Law Journal*, 41(2), 339–377.
- Bailey, J. (2008). Towards and equality-enhancing conception of privacy. *Dalhousie Law Journal*, 31(2), 267–311.
- Bailey, J. (2009). Life in the fish bowl: Feminist interrogations of webcamming. In I. Kerr, V. Steeves, & C. Lucock (Eds.), *Lessons from the identity trail: Anonymity, privacy and identity in a networked society* (pp. 283–301). Oxford: Oxford University Press.
- Bailey, J. (2014). 'Sexualized online bullying' through an equality lens: Missed opportunity in *AB v. Bragg?* *McGill Law Journal*, 59(3), 709–740.
- Bailey, J. (2016). *Canadian legal approaches to 'cyberbullying' and cyberviolence: An overview*. Ottawa Faculty of Law Working Paper No. 2016-37.
- Bailey, J. (2020). Implicitly feminist? The Supreme Court of Canada's decision in *R v Jarvis*. *Canadian Journal of Women and the Law*, 32(1), 196–220.
- Bailey, J., & Mathen, C. (2019). Technology-facilitated violence against women & girls: Assessing the Canadian criminal response. *Ontario Bar Review*, 97(3), 664–696.
- Balos, B. (2004). A man's home is his castle: How the law shelters domestic violence and sexual harassment. *Saint Louis University Public Law Review*, 23(1), 77–105.
- Bérubé, A. (2003). Resorts for sex pervers: A history of gay bathhouses. *Journal of Homosexuality*, 44(3/4), 33–53.

- Brinckerhoff, R. (2018). Social network or social nightmare: How California courts can prevent Facebook's frightening foray into facial recognition technology from haunting consumer privacy rights forever. *Federal Communications Law Journal*, 70, 105–156.
- Browne, S. (2015). *Dark matters: On the surveillance of blackness*. Durham, NC: Duke University Press.
- Buolamwini, J., & Gebru, T. (2018). Gender shades: Intersectional accuracy disparities in commercial gender classification. *Proceedings of Machine Learning Research*, 81(1), 1–15.
- Burns, A. (2018). Creepshots and power: Covert sexualised photography, online communities and the maintenance of gender inequality. In M. Bohr, & B. Sliwinska (Eds.), *The evolution of the image: Political action and the digital self* (pp. 27–40). New York, NY: Routledge.
- Caldera, E. (2019). Reject the evidence of your eyes and ears: Deepfakes and the law of virtual replicants. *Seton Hall Law Review*, 50(1), 177–205.
- Canadian Charter of Rights and Freedoms, s 8, Part 1 of the Constitution Act, 1982, being Schedule B to the Canada Act 1982 (UK). (1982), c 11.
- Chesney, R., & Citron, D. (2019). Deep fakes: A looming challenge for privacy, democracy, and national security. *California Law Review*, 107, 1753–1819.
- Choudry, A. (2019). *Activists and the Surveillance State: Learning from Repression*. London: Pluto Press.
- CIPPIC. (2019). R v Jarvis, 2019 SCC 10, Factum of the intervenor Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic. Retrieved from https://www.scc-csc.ca/WebDocuments-DocumentsWeb/37833/FM030_Intervener_Samuelson-Glushko-Canadian-Internet-Policy-and-Public-Interest-Clinic.pdf
- Citron, D. (2014). *Hate crimes in cyberspace*. Cambridge, MA: Harvard University Press.
- Citron, D. (2019). Sexual privacy. *The Yale Law Journal*, 128(7), 1870–1960.
- Cole, S. (2019, October 16). 'Girls Do Porn' was a crime ring, not a porn site, industry experts say. *Motherboard*.
- Criminal Code, RSC 1985, c C-46, s 318(1)(a), ss 162 & 162.1.
- Crosby, A., & Monaghan, J. (2018). *Policing Indigenous movements: Dissent and the security state*. Winnipeg, MB: Fernwood Publishing.
- Davis, D. (1994). The harm that has no name: Street harassment, embodiment, and African American Women. *UCLA Women's Law Journal*, 4, 133–178.
- Department of Justice. (2002). *Voyeurism as a criminal offence: A consultation paper*. Department of Justice Canada.
- Department of Justice. (2013). *Cyberbullying and the non-consensual distribution of intimate images*. Department of Justice. Canada. CCSO Cybercrime Working Group.
- Dickson, E. (2019, May 31). How facial recognition technology could bring a slut-shaming nightmare. *Rolling Stone*.
- Dodge, A. (2016). Digitizing rape culture: Online sexual violence and the power of the digital photograph. *Crime, Media, Culture: An International Journal*, 12(1), 65–82.
- Dodge, A. (2020). This voyeurism case changed Canadian privacy laws. It also changed this victim's life. *CBC News*. Retrieved from <https://www.cbc.ca>

- Dunn, S., Lalonde, J., & Bailey, J. (2017). Terms of silence: Weaknesses in corporate and law enforcement responses to cyberviolence against girls. *Girlhood Studies*, 10(2), 80–96.
- Dunn, S., & Petricone-Westwood, A. (2018). More than ‘revenge porn’: Civil remedies for the non-consensual distribution of intimate images. CCLA 38th Civil Litigation Conference publication.
- Flynn, A. (2019). Image-based abuse: The disturbing phenomenon of the “deep fake”. *Monash Lens*, March 12.
- Flynn, A., & Henry, N. (2019). Image-based sexual abuse: An Australian reflection. *Women & Criminal Justice*.
- Gilliard, C. (2020, January 9). *Caught in the spotlight*. Urban Omnibus.
- Gotell, L. (2006). When privacy is not enough: Sexual assault complainants, sexual history evidence and the disclosure of personal records.(Canada). *Alberta Law Review*, 43(3), 743–778.
- Grother, P., Ngan, M., & Hanaoka, K. (2019). *Face recognition vendor test (FRVT). Part 3: Demographic effects*. NISTIR 8280. Washington, DC: National Institute of Standards and Technology, US Department of Commerce.
- Hargreaves, S. (2014). Jones-ing’ for a solution: Commercial street surveillance and privacy torts in Canada. *Laws*, 3(3), 388–409.
- Hartzog, W. (2018). *Privacy’s blueprint the battle to control the design of new technologies*. Cambridge, MA: Harvard University Press.
- Henry, N., & Flynn, A. (2019). Image-based sexual abuse: Online distribution channels and illicit communities of support. *Violence Against Women*.
- Henry, N., McGlynn, C., Powell, A., Scott, A. J., Johnson, K., & Flynn, A. (2020). *Image-based sexual abuse: A study on the causes and consequences of non-consensual nude or sexual imagery*. New York, NY: Routledge.
- Intimate Images Protection Act*, RSNL 2018, c I-22.
- Introna, L., & Nissenbaum, H. (2011). *Facial recognition technology: A survey of policy and implementation issues*. Lancaster University management school. Working Paper 49012.
- Jane, E. (2014). ‘You’re a ugly, whorish, slut’: Understanding e-bile. *Feminist Media Studies*, 14(4), 531–546.
- Jane Doe 72511 v Morgan*, 2018. ONSC 6607.
- Kaminski, M. (2013). Drone federalism: Civilian drones and the things they carry. *California Law Review*, 4, 57–74.
- Khoo, C., Robertson, K., & Deibert, R. (2019). *Installing fear: A Canadian legal and policy analysis of using, developing, and selling smartphone spyware and stalkerware applications*. Toronto, ON: Citizen Lab.
- Koshan, J. (2017). The judicial treatment of marital rape in Canada: A post-criminalisation case study. In M. Randall, J. Koshan, & P. Nyaundi (Eds.), *The right to say no marital rape and law reform in Canada, Ghana, Kenya and Malawi* (pp. 257–298). Portland, OR: Hart Publishing.
- Koskela, H. (2000). ‘The gaze without eyes’: Video-surveillance and the changing nature of urban space. *Progress in Human Geography*, 24(2), 243–265.
- Koskela, H. (2002a). ‘Cam era’: The contemporary urban panopticon. *Surveillance and Society*, 1(3), 292–313.
- Koskela, H. (2002b). Video surveillance, gender, and the safety of public urban space: ‘Peeping Tom’ goes high-tech? *Urban Geography*, 23, 257–278.

- Laidlaw, E. (2017, July 6). 'CanadaCreep' case highlights need for better privacy laws. *The Canadian Press*. Retrieved from <https://theconversation.com/canadacreep-case-highlights-need-for-better-privacy-laws-79983>
- LEAF. (2019). R v Jarvis, 2019 SCC 10, Factum of the intervenor women's legal education and action Fund. Retrieved from https://www.scc-csc.ca/WebDocuments-DocumentsWeb/37833/FM050_Intervener_Women's-Legal-Education-and-Action-Fund-Inc..pdf
- Lippman, J., Cassimatis, N., & Renn, A. (2019). *Clearview AI Accuracy Test Report*. American Civil Liberties Union.
- Magnet, S. (2011). *When biometrics fail: Gender, race, and the technology of identity*. Durham, NC: Duke University Press.
- Manokha, I. (2018). Surveillance, panopticism, and self-discipline in the digital age. *Surveillance and Society*, 16(2), 219–237.
- McGill, J., & Kerr, I. (2012). Reduction to absurdity: Reasonable expectations of privacy and the need for digital enlightenment. *Digital Enlightenment Yearbook*, 199–217.
- McGlynn, C., Rakley, E., & Houghton, R. (2017). Beyond 'revenge porn': The continuum of image-based sexual abuse. *Feminist Legal Studies*, 15, 25–46.
- Milner v Manufacturers Life Insurance Company*. 2005. BCSC 1661.
- Nelson, S. (2019). Sex work and social media: Policy, identity, and privacy in networked publics and counterpublics. *Journal of the Cultural Studies Association*, 8(1).
- Nissenbaum, H. (2010). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford, CA: Stanford Law Books.
- Office of the Privacy Commissioner of Canada. (2013). *Aboriginal Affairs and Northern Development Canada wrongly collects information from First Nations activist's personal Facebook page*. Ottawa, ON: Office of the Privacy Commissioner of Canada.
- Oliver, K. (2016). Rape as spectator sport and creepshot entertainment: Social media and the valorization of lack of consent. *American Studies Journal*, 61.
- Ontario Human Rights Commission. (2018) A Collective Impact: Interim report on the inquiry into racial profiling and racial discrimination of Black persons by the Toronto Police Service. Retrieved from <http://www.ohrc.on.ca/en/public-interest-inquiry-racial-profiling-and-discrimination-toronto-police-service/collective-impact-interim-report-inquiry-racial-profiling-and-racial-discrimination-black>
- Parsons, P., Molnar, A., Dalek, J., Knockel, J., Kenyon, M., Haselton, B., & Deibert, R. (2019). *The predator in your pocket: A multidisciplinary assessment of the stalkerware application industry*. Toronto, ON: Citizenlab.
- Powell, A., & Henry, N. (2017). *Sexual violence in a digital age*. London: Palgrave Macmillan.
- Powell, A., Henry, N., & Flynn, A. (2018). Image-based sexual abuse. In W. S. DeKeseredy, & M. Dragiewicz (Eds.), *Routledge handbook of critical criminology* (2nd ed., pp. 305–315). Abingdon and New York, NY: Routledge.
- Richards, N., & Hartzog, W. (2017). Privacy's trust gap: A review. *The Yale Law Journal*, 126, 1180–1224.
- Ridgen, M. (2020, January 30). Province of Manitoba to end birth alerts. *APTN*. Retrieved from <https://www.aptnnews.ca/national-news/province-of-manitoba-to-end-birth-alerts/>

- R v Jarvis*, 2019. SCC 10.
- R v Mills*. (1999). 3 SCR 668.
- Rothrock, K. (2016, April 26). Facial recognition service becomes a weapon against Russian porn actresses. *ArsTechnica*. Retrieved from <https://arstechnica.com/tech-policy/2016/04/facial-recognition-service-becomes-a-weapon-against-russian-porn-actresses/>
- Royakkers, L., Timmer, J., & KoolRinie van Est, L. (2018). Societal and ethical issues of digitization. *Ethics and Information Technology*, 20(2), 127–142.
- Scassa, T. (2010). Information privacy in public space: Location data, data protection and the reasonable expectation of privacy. *Canadian Journal of Law and Technology*, 7(1 & 2), 193–220.
- Thomasen, K. (2018). Beyond airspace safety: A feminist perspective on drone privacy regulation. *Canadian Journal of Law and Technology*, 16, 307–338.
- Thomasen, K., & Dunn, S. (2019, February 25). Court ruling on voyeurism could have broad social impact. *IRPP Policy Options*. Retrieved from <https://policy-options.irpp.org/magazines/february-2019/court-ruling-voyeurism-broad-social-impact/>
- Thompson, D. (1993). ‘The woman in the street’: Reclaiming the public space from sexual harassment. *Yale Journal of Law and Feminism*, 2, 313–348.
- Thompson, C., & Wood, M. (2018). A media archeology of the creepshot. *Feminist Media Studies*, 18(4), 560–574.
- Tran, M. (2015). Combatting gender privilege and recognizing a woman’s right to privacy in public spaces: Arguments to criminalize catcalling and creepshots. *Hastings Women’s Law Journal*, 26(2), 185–206.
- Tulloch, M. (2018). *Report of the independent street checks review*. Toronto, ON: Queen’s Printer for Ontario.
- Vera-Gray, F. (2016). Men’s stranger intrusions: Rethinking street harassment. *Women’s Studies International Forum*, 58, 9–17.
- Waldman, A. E. (2018). *Privacy as trust-Information privacy for an information age*. Cambridge: Cambridge University Press.
- Waldman, A. E. (2019). Law, privacy, and online dating: ‘Revenge porn’ in gay online communities. *Law & Social Inquiry*, 44(4), 987–1018.
- Walker, S. (2016, May 17). Face recognition app taking Russia by storm may bring end to public anonymity. *The Guardian*.