13

Privacy, sociality and the failure of regulation: lessons learned from young Canadians' online experiences

VALERIE STEEVES

When Canada first considered enacting private sector privacy legislation in the late 1990s, it was primarily in response to the 1995 European Union Directive restricting the flow of personal data to countries that did not have data protection laws in place. Because law reform was seen as a way to avoid the erection of trade barriers between Canadian companies and their European trading partners, privacy was cast as a commercial issue rather than a social or political issue. The desire to comply with European laws also meant that legislators looked to data protection as the regulatory tool of choice (Bennet and Raab 2002). Data protection, it was reasoned, would not only promote harmonization; it would help Canadian companies compete by leveling the playing field and reigning in rogue companies that did not follow the information practices that were generally accepted by the international business community at the time (Industry Canada and Department of Justice 1998). In addition, data protection was an attractive way to build consumer trust in the emerging information economy at home, because it would provide individuals with more control over their personal information (Industry Canada and Department of Justice 1998).

Given the strong international consensus behind data protection in general, and the commercial imperatives behind the Canadian approach to privacy legislation in particular, it is somewhat surprising that young people were, and continue to be, an important part of Canadian privacy policy discourses. However, from the beginning Canadians legislators ascribed young people a key role in their digital privacy strategy. As savvy digital natives, they were presumed to have a "natural" affinity for both technology and innovation (Shade 2011; Bailey 2013; Bailey and Steeves 2013). Because of this, legislators believed that early uptake of networked technologies by youth would help fuel the digital economy and drive

wealth creation. Since the absence of strong privacy protections was seen as a barrier to this uptake, data protection for youth was an attractive market intervention because it ostensibly gave them control over the collection, use and disclosure of their personal information without unduly hampering commercial entities that sought to commoditize it.

At the same time, there were competing discourses within the legislative debate that sought to position privacy as a human right and social value. Legislators situated in this perspective argued that a private life is an essential element of human dignity, and lays the foundation that enables us to exercise other rights such as the right to free expression and free association. In addition, privacy enables us to enjoy a degree of autonomy and enter into relationships with others based on trust. They concluded that data protection alone, with its narrow focus on individual forms of redress, cannot fully protect these elements of privacy because it does not interrogate the social and public goods and harms associated with surveillance (Industry Canada and Department of Justice 1998). They called for broad restrictions on surveillance and remedies that would make privacy, especially privacy of networked communications, the default rather than the exception. However, these alternative discourses were marginalized within the legislative debate (Shade 2011; Steeves 2015a); and when the federal government passed the Personal Information Protection and Electronic Documents Act (PIPEDA) in 2001, it positioned the law – which contained a set of ten data protection practices – as a cornerstone of its emerging e-commerce agenda.

Inherent in PIPEDA is the assumption that transparency on the part of data collectors will enable young people (and their parents) to make informed decisions about what they choose to disclose about themselves (Steeves 2015b)[1]. In other words, young people can protect their privacy by choosing to withhold information that they deem "private." This

[1] In Canadian law there are no express provisions regarding the age of consent regarding the collection of personal information. Although contract law would suggest that parental consent is required for at least younger minors, PIPEDA is silent on the issue and the legal position of mature minors is unclear. Except for websites specifically targeting young children, most sites do not have a mechanism to ensure that minors participate only with parental consent; and those sites targeting young children typically only ask for parental consent for minors under the age of thirteen, mirroring the requirements of American law. In any event, children typically slip between the cracks, making their own decisions about what information to disclose. Facebook is an excellent example. Even though its terms of use indicate persons under the age of thirteen cannot join the network, our 2013 survey indicated that 32 percent of eleven- and twelve-year-olds have a Facebook account.

assumption is particularly conducive to commercial interests because it legitimizes the ongoing collection and commodification of the information young people do choose to disclose online. It also helps insulate the marketplace from more onerous regulations, such as opt-in consent provisions and blanket restrictions disallowing the collection of information from minors, that may slow innovation and competitiveness in the emerging information economy (MediaSmarts 2014).

Although there has been a continuing debate about the need for stronger regulations that better protect the role that privacy plays in young people's social lives, particularly given the growing commercialization of young people's social spaces enabled by seamless commercial online surveillance (Lawford 2008), the parliamentary committees reviewing PIPEDA have consistently eschewed a broader approach to protecting the social value of privacy and instead have tinkered with parental consent provisions or education to help young people understand the existing law (Standing Committee on Access to Information, Privacy and Ethics 2014). Often the lesson is that children who want to protect their privacy should not post information about themselves on social media. The corollary is that children who do post information have consented to its collection and use by a variety of actors, from corporations and marketers to schools and gaming companies, because they no longer "care" about privacy. Moreover, when risks to children have been identified (e.g. exposure to offensive content, cyberbullying), legislators have typically looked to surveillance as a way to protect young people from harm, further eroding their ability to enjoy private communications (Bailey and Steeves 2013). Either way, protecting the social value of privacy recedes as a policy alternative.

This chapter draws on qualitative and quantitative research on Canadian young people's use of networked technologies to revisit the assumptions behind the current policy framework and test the efficacy of the privacy protections that are currently in place. I start by examining the evidence regarding young people's technical skills, especially in regard to innovation, and their general attitudes to privacy. I then examine how transparent commercial information practices are to Canadian youth, and whether the data protection model – that assumes consent mechanisms will provide opportunities to protect the privacy of information through intentional non-disclosure – resonates with their lived experiences and expectations. Finally, I provide some evidence to measure the level of trust young people have in e-commerce in general and the current regulatory framework in particular.

The evidence does not paint an encouraging picture. I argue that, although Canadian young people have not demonstrated a natural affinity for technological innovation, they have flocked to networked technologies as a way to enrich their social lives. In that context, they have developed a number of social norms around exposure in an attempt to enjoy the benefits of online publicity while still carving out private socio-technical spaces for self-expression and intimate communication. Young people accordingly seek privacy and publicity at the same time and in the same socio-technical space, by carefully crafting networked communications for a variety of contexts and audiences. Accordingly, young Canadians' experiences of privacy are defined by their interaction with others and are not just a feature of individual decisions to disclose or withhold information in networked spaces.

Because of this, the legislative model adopted by Canadian legislators fails to fully capture the ways in which privacy is implicated in young people's lives. Moreover, PIPEDA privileges notions of consent that legitimize commercial practices of mining the social world; this mining in turn has the potential to restructure young people's social relationships and restrict the kinds of identity performances available to them. This constitutes a profound invasion of young people's privacy, by unintentionally creating invasive online spaces and restricting the social norms that enable young people to negotiate the kinds of privacy they need to meet their developmental goals and enjoy networked sociality.

I conclude by suggesting that a social model of privacy more fully captures the richness of both online publicity and online privacy in young people's lives, and better explains the relationship between privacy, identity, sociality and trust. Once privacy is seen as a social negotiation between actors who seek a comfortable boundary between self and others, disclosure of information does not negate a privacy interest; rather, privacy is mutually constructed when the individual seeking privacy has his or her privacy claim respected by others, independent of whether they are aware of the disclosure. In the words of one fourteen-year-old, "just because someone can see something doesn't mean they should look." A failure to respect a privacy claim – to look – erodes trust because it signals that the other does not acknowledge the claimant as a person requiring dignity and respect for boundaries. Since privacy is co-constructed with others, it is also closely linked to both identity and reputation in interlinking ways. A successful presentation of the self requires control over which audience sees which performance, and when audiences cross over boundaries or performances are unsuccessful, disputes can be

managed by moving between public and private spaces to enlist others in reputational repair. By conceptualizing privacy as a social construction, we move away from simplistic models that focus on consent and control over the flow of information, and create the space for legislative solutions that more closely align with young people's needs, such as "right to forget" clauses, and restrictions on data mining and behavioral advertising.

Young Canadians' experiences – privacy, performativity and social connection

The Canadian government's early commitment to encouraging young people to adopt networked technologies as tools for learning and innovation has had mixed results. On the one hand, young Canadians are among the most wired in the world. Of children between the ages of nine and seventeen, 99 percent have access to the Internet outside of school, largely through portable devices, (Steeves 2014b: 7), and by age seventeen, 85 percent have their own cell phone (Steeves 2014b: 10). In addition, almost all students have at least basic technical skills across a variety of platforms (Steeves 2014a: 14). On the other hand, there is little evidence that suggests that Canadian youth are particularly savvy or innovative, and most prefer to consume content that has been posted by others. For example, the majority of older students (65 percent) do not know how to use advanced search functions to find information online, and half never look beyond the first page of search results (Steeves 2014a: 15). And although 75 percent of young people rank YouTube as one of their favorite sites, only 4 percent post their own videos with any frequency (Steeves 2014b: 32). One teacher summarized it this way: "I don't think students are all that Internet-savvy. I think they limit themselves to very few tools ... They're locked into using it in particular ways and don't think outside the box" (Steeves 2012b: 9).

Although high levels of connectivity have not led to significant gains in learning or innovation, young Canadians have flocked to networked tools that enable them to access entertainment content and communicate with their friends and family (Steeves 2014b: 17). Corporations such as Facebook have often pointed to this activity to argue that young people no longer care about privacy and are content to trade it away for access to websites and apps (Hill 2010). However, Canadian youth have consistently reported a high interest in networked privacy. As early as 2000, qualitative interview participants indicated that they were attracted to online media precisely because they believed them to *be* private. They reasoned

that, since most adults at the time were unable to access the Internet, their online activities were largely anonymous, and they enthusiastically used this privacy to experiment with ways of being that were difficult or impossible to experience offline (Media Awareness Network 2001: 17).[2] For example, chat functions enabled them to interact anonymously with others in a public space, to experiment with flirting and to "try on" a variety of identities. As one thirteen-year-old boy in Toronto put it in 2004, "Sometimes I pretend to be a boy looking for a girl. Sometimes I pretend to be a girl looking for a boy. And sometimes I pretend to be a girl looking for another girl" (Media Awareness Network 2004). This kind of interaction provided a unique opportunity to explore the broader social world at little risk to themselves because their actions were shielded by a veil of privacy.

The unrestricted access young people enjoyed in the early years of the Web was increasingly restricted as policymakers raised concerns about offensive content and online predation (Bailey and Steeves 2013); schools introduced highly invasive surveillance mechanisms, such as keystroke capture software (Steeves and Marx 2014), and many parents began to proactively monitor their children's online interactions as a form of care (Steeves 2015b). However, young people have consistently devised strategies to avoid this surveillance and keep their networked communications and activities private. In 2004, for example, interview participants reported that they used instant messaging language that was difficult for adults to understand and deleted their browsing history so they could not be tracked, precisely because it was important to them that their communications – which continued to take place on publicly accessible media and were therefore accessible to those who looked – remained private (Media Awareness Network 2004: 1–16).

This need for private socio-technical spaces where children can participate in social interactions with their peers and experiment with their own identities is closely tied to their developmental need to individuate and explore who they are outside the family (Shade 2011). In effect, this networked social interaction helps them co-produce their subjectivity through their interaction with others, who reflect their performances back to them so they can evaluate them and either incorporate or reject the type of identity they have portrayed into their sense of self (Mead 1934; Goffman 1959; Phillips 2009). Social identities and peer group membership are accordingly reinforced through what Licoppe calls "connected

[2] See also Livingstone 2009: 91.

presence," that is the distribution of social interactions across a variety of platforms through which "the (physically) absent party gains presence through the multiplication of mediated communication gestures on both sides, up to the point where copresent interactions and mediated distant exchanges seem woven into a single, seamless web" (Licoppe 2004: 135). This online connectedness is particularly key for adolescents, who construct and display their identities by mapping their social relationships with peer groups and making them visible to others (Livingstone 2009).

Privacy is central to this process because it is what enables them to draw boundaries around their various identities (for example as friend, sibling and student) and manage their social relationships with a variety of audiences, from peers to parents and family to teachers. Privacy is accordingly not sought through selective non-disclosure of personal information that young people consider to be private. Instead, they disclose a great deal of personal information as they perform a variety of identities, and then rely on social norms that govern their interactions with others to maintain the boundaries between their various performances to ensure that some performances are (not) seen by (some) others.

This equal importance of privacy and publicity, and the complex negotiations that enable young people to enjoy both, are perhaps best exemplified by young Canadians' experiences on social media. Given young Canadians' predilection to socialize online, it is unsurprising that the vast majority have incorporated social media into their daily lives. Penetration is highest among older youth: for example, 95 percent of seventeen-year-olds are on Facebook and 63 percent use Twitter. Posting on these and other social media accounts is one of the most frequent activities reported, as is perusing what others had posted on their accounts: almost three-quarters (72 percent) of seventeen-year-olds read or post on friends' social network sites at least once a day or once a week (Steeves 2014b: 28). Social media use also starts early. Almost one-third (32 percent) of younger children (aged nine to eleven) have a Facebook account even though the terms of use on the site forbid children under the age of thirteen from joining the network, and social media supplants playing online games as the most popular online activity by age twelve (Steeves 2014b: 22).

Our interview participants in 2013 indicated that this high degree of connectedness is a way to monitor the "drama" that publicly unfolds among their peer group and to stay in the loop with respect to the latest gossip. In addition, since their social media posts are visible to others in their social circle, they can explicitly step in and out of the online

gaze to play pranks on each other, and demonstrate their competence in the online environment. The visibility of social media also provides an opportunity to carefully monitor peer reaction to their own and others' postings, in order to identify online presentations that are successful (and perhaps worth imitating) and those that are not (Steeves 2012a: 6–8).

Peer reactions were particularly important to them, since the ease with which unsuccessful performances (e.g. a bad photo or losing control of a sext) can be seen, copied and forwarded poses significant risks to their social status. Although public display is clearly part of the fun of social media, poor public displays can be devastating and open them up to ridicule and embarrassment. Young people accordingly spend a great deal of time and effort carefully selecting photos that present a positive image, or at least avoid a negative one, before they post them publicly, and take steps to make sure bad photos are kept out of public view. As these fifteen-year-old girls put it:

Diana: I just don't take stupid pictures that I know could ruin my reputation, or something.
Leah: I don't think any of my friends would.
Diana: Exactly. And if I take stupid pictures on a camera, then I delete it, right.

(Steeves 2012a: 33)

Young people also closely monitor the way they are being portrayed in photos taken by others so they can preemptively stop certain kinds of images from being posted publicly. For example, interviewees reported that friends would frequently take snap shots of them goofing around in private. However, as the following discussion illustrates, they routinely go into each other's phones or cameras and proactively delete any they do not want seen by others, in order to manage the way they are viewed publicly on social media:

Emma: Cause ... if there's a picture of my goofing off, like making a funny face, you don't want everyone to see that, it's between you and your friends.
Taylor: Yeah, other people, other people probably all make fun of you, and then that'll stay around for a while because that's happened before.
Emma: Yeah, only your friends understand why you're doing it ...
Taylor: Yeah, and then everyone else, like, sees it and then they're kind of like, "oh, why are you doing this?"

(Steeves 2012a: 32)

Failing to provide access to photos so they can be pruned is seen as a breach of friendship, and can justify breaking into the friend's phone or social media account without permission to directly delete an

embarrassing image. Persisting in posting an unflattering photo without permission signals the end of the friendship. On the other hand, close friends keep potentially embarrassing photos on a private device, such as a smart phone; the fact the image is privately held and will not be distributed is understood to be a sign of intimacy and trust. For example, thirteen-year-old Lya in Toronto pulled out her phone and showed a particularly funny photo to her best friend Allie, who was also in the group. The photo showed Allie making a face. Even though others in the group wanted to see it, Lya refused to show it to them, indicating that is was something only for her and Allie to enjoy.

Friends are also expected to proactively monitor comments and photos posted of friends and, in the event that someone does post something embarrassing or mean, go online and repair the damage to the friend's reputation. This was illustrated when twelve-year-old Emma recounted that one of her schoolmates had posted a bad photo of her on Facebook and people began to post derogatory comments about her appearance. She texted her friends, who immediately responded by posting comments such as: "'No, Emma looks cool, she's awesome, she's so brave' and stuff, and [Emma] was like, 'I love you guys'" (Steeves 2012a: 32).

Again the distinction between the public and the private spheres is crucial here. Although the public nature of the posts in Emma's case exacerbated the social consequences since they were seen by so many of Emma's peers, that publicity also enabled Emma to privately monitor her online persona and call on her friends to defend her. Emma did not publicly challenge the attack, but instead privately marshalled her social resources in response. Emma's friends then entered the public sphere to repair the harm that had been done to her online reputation.

Our quantitative survey indicated that these kinds of steps are common among the population as a whole. Of the students surveyed, 97 percent reported that they would take steps to protect themselves if someone posted a photo of them online that they did not want others to see. Asking the poster to take the photo down was the most common response (80 percent). "Untagging," as a form of direct action, rose dramatically as children aged, and was especially common for older teens (72 percent). Calling on friends for help was also one of the top three responses for dealing with online conflict for all age groups (Steeves 2014c: 22–3).

These findings suggest that the construction of networked privacy is a highly social activity. Friends rely upon each other to mutually manage their public image by creating boundaries around what is and is not exposed to public view, and keeping certain images private signals

intimacy. Friends also privately monitor the ways in which other friends are portrayed online and step into the public sphere to respond to attacks and repair reputational harm.

Interestingly, the teenagers we spoke to in 2013 reported that maintaining boundary control was much more difficult for them because of parental concerns around online safety. Although almost all of them enjoyed connecting with family online, the kinds of surveillance to which many of them are subjected was disheartening, and made it difficult for them to enjoy both private interaction with friends and relationships of trust with family. For their part, the parents we talked to were ambivalent about monitoring their children online. Although most thought monitoring was necessary because they needed to protect their children both from strangers and from the consequence of their own poor judgment, they were also uncomfortable about invading their children's privacy.

The teens we spoke to responded empathetically and acknowledged that parents were only trying to protect them. However, they all took a variety of steps to make sure parents could not access their interactions with their friends. Many used technical controls, such as privacy settings and the routine deletion of histories, to evade "lectures." When one girl from the fifteen to seventeen-year-old age group indicated that "My mom keeps on [posting] me, 'You're on Facebook! Get off! Do your homework!' And I'm like ... de-friend" (Steeves 2012a: 17), the group exploded with similar stories about taking steps to ensure that their interactions with friends remain inaccessible to their parents. Even many of our youngest survey respondents felt that parents should not force their children to friend them on social media sites (56 percent) or read their texts (44 percent), and took steps to avoid being watched. The equivalent percentages among older children were much higher (77 percent and 83 percent, respectively) (Steeves 2014c: 34).

Again, this heightened concern among teenagers is consistent with a developmental need for privacy from parents. A private sphere provides older children with the autonomy they need to explore the "public-private boundaries of the self" (Peter *et al.* 2009: 85) and "renegotiate their familial relationships ... seek to define themselves within a peer group ... [and] venture out into the world without parental supervision" (Draper 2012: 223). One teen in Toronto summarized: "There should be a point where parents will just, like, leave you alone and not have to know every single thing about you. Like, I get, the protection side, but they don't need to know every single thing about you" (Steeves 2012a: 18).

Failure to meet this need for privacy creates tensions within the family and abrogates the reciprocal trust that is at the heart of family life. The teens we spoke to were vituperative about parents and other family members "spying" on them, even though they were aware of the fact that their social media posts are public and can be seen by others. For example, after one teen found out that her cousins "snitched" on her by telling her mother about a photo she had posted on social media, "the same night I go and delete them ... then [my mom] gets mad, she's like 'don't delete your family members.' I'm like, well, tell them to stop stalking me" (Steeves 2012a: 18). Another teen facing the same situation blocked her little brother because "he's like a little spy for my mother" (Steeves 2012a: 18).

This loss of privacy also makes it harder for teens to express themselves online because performances intended for peers can be taken out of context by family members. This in turn disrupts their "ability to disclose private information in appropriate ways and settings" (Peter *et al.* 2009: 83) with both friends and family, and complicates the boundary negotiation between their various roles, because they can be held to account by all their audiences for comments that were intended for one particular group and not another.

To summarize, Canadian young people have accordingly consistently sought ways to protect their privacy from others online, while at the same time embracing online publicity for the purposes of identity construction and social connection. Our participants carefully crafted different personas for their various audiences (family, friends, schoolmates, employers, teachers) and used privacy settings and other strategies to try to keep one performance (e.g. girlfriend) from leaking into another (e.g. daughter). Although the introduction of social media in particular has complicated their efforts to maintain a sense of privacy because social media largely collapse the lines between their various audiences, young people continue to respond to a lack of privacy by developing new techniques to shield themselves from unwanted observers in an attempt to reinsert comfortable boundaries as they continue to disclose parts of themselves to others as a means to social connection and identity experimentation.

Revisiting the regulatory framework

The current regulatory model, with its focus on transparent information practices and informed consent, fails to capture this rich interplay between privacy, performativity and social connection because it assumes that privacy is an individual choice to withhold or disclose information. From this perspective, privacy is best protected when organizations that collect personal information are transparent about their information practices, so individuals can make informed decisions about what they disclose and what they keep private. The corollary follows that young people who voluntarily disclose information about themselves on a technological platform have consented to the terms of use associated with that platform, and have willingly abandoned any further privacy interest in their data. All that is needed after disclosure is to provide rights of access and correction so young people can ensure that the data collected from them are accurate.

For this model to work, corporations must be transparent about their information practices so data subjects can make informed decisions about what they choose to disclose. However, the evidence suggests that young Canadians are not well informed about the informational practices of the corporate platforms they use. For example, 65 percent of youth aged eleven to seventeen report that no one has ever explained a terms of use policy or a privacy policy to them, and 68 percent mistakenly believe that the presence of a privacy policy on a site ensures that the personal information they post will not be shared with anyone. And although 66 percent indicate that they have been taught how companies collect and use personal information, 39 percent believe that companies are not interested in what they say and do online (Steeves 2014c: 38–9). This suggests that there is a significant gap between corporate practices and young people's expectations.

This lack of knowledge could arguably be addressed by additional education and outreach. However, full transparency may not be a complete corrective. Even when young people understand the commercial model behind their favorite sites, many report that they have no choice but to accept the terms of use, because doing so is the only way they can access the socio-technical spaces they increasingly rely on for social connectedness. Two girls in Ottawa put it this way:

> Like, if we had a choice to say no, I would choose no. We can't or else we can't go on the thing for some of them [fifteen-year-old].
>
> Depending on the consequences of saying no cause sometimes if you say no to like download something, it just like can't do anything with it and then it's just, yeah [fourteen-year-old].
>
> (Burkell *et al.* 2007: 14)

From this perspective, young people are often not given any real choice: children who do not wish to register or consent to the collection of

their personal information are simply told not to use the service (Steeves 2006, 2007). Many young people report that, in those circumstances, they just press "click" and accept whatever terms of service are imposed on them, whether they like them or not (Burkell *et al.* 2007: 14).

But the deeper problem with the regulatory model is the assumption that information, once disclosed, cannot attract a privacy interest. Although young Canadians do sometimes choose to withhold information to keep it private, they more typically choose to disclose information and then negotiate their privacy as they interact with others in networked spaces. Their privacy expectations are accordingly driven less by the fact that unintended others may be able to see what they post, and more by strong ideas about who should and should not be looking. Although they are sometimes unable to successfully negotiate a comfortable degree of privacy (especially because of surveillance related to adult concerns about cyber-safety), the privacy they seek is defined by a complex interplay of opening and closing to a variety of social relationships in a variety of social settings where their interactions can be seen by others. Notions of transparency and consent simply cannot help them to protect their privacy because young people do not operate within a binary division between non-disclosure/private and disclosure/public.

Moreover, the bad fit between the regulatory understanding of privacy and young people's lived experiences of privacy has made it difficult for PIPEDA to construct trust in the digital economy. Although young people tend to be most concerned about privacy from people in their social world, they see commercial surveillance as "creepy" and a type of "stalking" (Burkell *et al.* 2007: 15; Steeves 2012a: 25). Attitudes towards the marketing embedded in the socio-technical spaces they inhabit range from ambivalent to distrustful, and a number report that online corporations are trying to "fool" them or "trick" them into releasing information (Steeves, 2012a: 24). Many have little faith in the data protection process, arguing that corporations intentionally write their privacy policies in language that is incomprehensible so they can "Take advantage of the kids ... cause they can't read at university level" (Burkell *et al.* 2007: 15).

The failure of the current regulatory model to devise a privacy-respectful networked environment is perhaps best illustrated by the finding that the vast majority of young Canadians report that neither the corporations that own the platforms (83 percent) nor the marketers who want to advertise to them (95 percent) should be able to even *see* what they post on social media (Steeves 2014c: 34, 36). Again, just because data is disclosed

on the Internet does not mean that young people have abandoned their privacy interest in who can watch it. Although 28 percent also paradoxically report that they like it when companies use the information they post to advertise to them, three-quarters say they want more control over what corporations do with the photos and information they post online. Clearly, the existing framework is not providing them with enough control.

Conclusion

The dominant understanding of privacy as informational control cannot fully capture the ways in which privacy is implicated in young people's online social interaction, identity and performativity because it focuses on the flow of information across the boundary between self and other, instead of on the boundary itself (Steeves 2009). By focusing on disclosure, regulators have downloaded the regulatory burden onto the individual children who inhabit networked spaces and typically call upon young people to stop disclosing information about themselves to others. For example, when a photo of a young Canadian girl who had committed suicide after an intimate photo of her was circulated electronically was used in an online dating site advertisement, then Information and Privacy Commissioner of Ontario Ann Cavoukian stated:

> The unfortunate reality is that people give out far too much information about themselves, believing that their information is "private" and they are safe behind their screen. You are not! We all need to take steps to protect ourselves online, especially on social networks. Young people must be especially careful to consider the potential risks, and make it a practice to only post photos that they want everyone to see, including strangers and prospective future employers. If not, don't post it!
>
> (Contenta 2014)

This approach conflicts with the nuanced ways in which children seek to negotiate both publicity and privacy in public spaces and ignores the social norms they have developed to manage the expectations of their various audiences. Instead, regulators need to carve out anonymous spaces where young people can interact without being constantly monitored, and reconsider the use of surveillance as a protective mechanism. This is especially important in schools, where privacy plays an essential role in creating an environment where children can learn, express themselves and not be afraid to make mistakes (Steeves and Marx 2014).

In addition, given the commercial goals behind the regulatory framework, further research is needed to better understand how commercial mining of the social world restructures social relationships and restricts the kinds of identity performances available to young people online. Early findings indicate that the algorithms applied to the data collected sort children into categories for marketing purposes, and these categories often reproduce real-world patterns of discrimination. The detailed individual profiles that result enable marketers to integrate mediatized messages into children's social environment, through behavioral targeting and "natural" or immersive advertising. This encourages children to internalize the identity created for them by the algorithmic sort itself (Bailey and Steeves 2015). From this perspective, commercial surveillance is a profound invasion of young people's privacy, because it uses the data it collects to reshape their social world and steer their social interactions. It also creates a feedback loop that reinforces mainstream stereotypes: information architectures lend themselves to certain kinds of identity performances (e.g. highly sexualized performances of girls), and these architectures combine with social norms to open children up to discrimination (e.g. slut shaming, homophobia). Children co-opt stereotypical performances because they are the cultural capital available to them for identity construction, and this both reinforces discriminatory tropes in children's culture and opens up particular children to harassment based on sexism, racism, homophobia, classism and ableism.

Data protection makes it difficult to question these practices, because a binary notion of consent legitimizes commercial uses and makes it difficult to constrain what happens to the data once consent is given. However, conceptualizing privacy as a social value opens up policy to a broader critique that can interrogate the social impact of commercial surveillance. In addition, a social model of privacy more fully captures the richness of both online publicity and online privacy in young people's online lives, and better explains the relationship between privacy, identity, sociality and trust. It also points to legislative solutions that more closely align with young people's experiences, such as "right to forget" clauses, and restrictions on data mining and behavioral advertising.

References

Bailey, J. 2013. "Cogs in the Wheel of Economic Progress? Claims-Making About Girls and Technology in Canadian Policy Discourse." Shirley E. Greenberg Chair for Women and the Legal Profession – Speaker Series. University of Ottawa.

Bailey, J. and Steeves, V. 2013. "Will the Real Digital Girl Please Stand Up? Examining the Gap Between Policy Dialogue and Girls' Accounts of Their Digital Existence," in Wise, J. M. and Hille, K. (eds.) *New Visualities, New Technologies: The New Ecstasy of Communication*. London: Ashgate, pp. 41–66.

(eds.) 2015 (forthcoming). *eGirls, eCitizens: Putting Technology Theory and Policy Into Dialogue with Girls' and Young Women's Voices*. University of Ottawa Press.

Bennet, C. and Raab, C. 2002. *The Governance of Privacy: Policy Instruments in Global Perspective*. London: Barnes and Noble.

Burkell, J., Steeves, V. and Micheti, A. 2007. *Broken Doors: Strategies for Drafting Privacy Policies Kids Can Understand*. Ottawa: On the Identity Trail.

Contenta, S. 2014. "Dating website apologizes for using Rehtaeh Parsons's picture," *Toronto Star*, August 30.

Draper, N. 2012. "Is your teen at risk? Discourses of adolescent sexting in the United States," *Journal of Children and Media* 6: 223.

Goffman, E. 1959. *The Presentation of Self in Everyday Life*. New York: Anchor Books.

Hill, K. 2010. "Zuckerberg's Right: Young People Don't Care (As Much) About Privacy," *Forbes*, January 10.

Industry Canada and Department of Justice. Task Force on Electronic Commerce. 1998. *Building Canada's Information Economy and Society: The Protection of Personal Information*. Ottawa: Public Works and Government Services Canada.

Lawford, J. 2008. *All in the Data Family: Children's Privacy Online*. Ottawa: Public Interest and Advocacy Centre.

Licoppe, C. 2004. "'Connected presence': the emergence of a new repertoire for managing social relationships in a changing communication technoscape," *Environment and Planning D: Society and Space* 22: 135–56.

Livingstone, S. 2009. *Children and the Internet*. Cambridge: Polity Press.

Mead, G. H. 1934. *Mind, Self and Society*. University of Chicago Press.

Media Awareness Network. 2001. *Young Canadians in a Wired World: The Students' View*. Ottawa: Media Awareness Network.

Media Awareness Network. 2004. *Young Canadians in a Wired World, Phase II: Focus Groups* Ottawa: Media Awareness Network.

MediaSmarts. 2014. *Youth and Digital Skills Symposium: Preparing Young Canadians to Make Social, Economic and Cultural Contributions*. Ottawa: Information and Communications Technology Council.

Peter, J., Valkenburg, P. and Fluckiger, C. 2009. "Adolescents and Social Network Sites: Identity, Friendships and Privacy," in Livingstone, S. and Haddon,

L. (eds.) *Kids Online: Opportunities and Risks for Children*. Bristol: The Policy Press.

Phillips, D. 2009. "Ubiquitous Computing, Spatiality, and the Construction of Identity: Directions for Policy Response," in Kerr, I., Lucock, C. and Steeves, V. (eds.) *Lessons From the Identity Trail: Anonymity, Privacy and Identity in a Networked Society*. New York: Oxford University Press, pp. 303–18.

Shade, L. R. 2011. "Surveilling the Girl via the Third and Networked Screen," in Kearney, M. C. (ed.) *Mediated Girlhoods: New Explorations of Girls' Media Culture*. New York: Peter Lang, pp. 261–76.

Standing Committee on Access to Information, Privacy and Ethics, House of Commons, Canada. 2014. *Privacy and Social Media in the Age of Big Data*, 1st sess., 41st Parliament.

Steeves, V. 2006. "It's not child's play: the online invasion of children's privacy," *University of Ottawa Law and Technology Journal* 3(1): 169–88.

2007. "The watched child: surveillance in three online playgrounds," *Proceedings of the International Conference on the Rights of the Child*: 119–40.

2009. "Reclaiming the Social Value of Privacy," in Kerr, I., Lucock, C. and Steeves, V. (eds.) *Lessons From the Identity Trail: Anonymity, Privacy and Identity in a Networked Society*. New York: Oxford University Press, pp. 191–208.

2012a. *Young Canadians in a Wired World, Phase III: Talking to Youth and Parents About Life Online*. Ottawa: MediaSmarts.

2012b. *Young Canadians in a Wired World, Phase III: Teachers' Perspectives*. Ottawa: MediaSmarts.

2014a. *Young Canadians in a Wired World, Phase III: Experts or Amateurs? Gauging Young Canadians' Digital Literacy Skills*. Ottawa: MediaSmarts.

2014b. *Young Canadians in a Wired World, Phase III: Life Online*. Ottawa: MediaSmarts.

2014c. *Young Canadians in a Wired World, Phase III: Online Privacy, Online Publicity*. Ottawa: MediaSmarts.

2015a (forthcoming). "Now You See Me: Privacy, Technology and Autonomy in the Digital Age," in DiGiacomo, G. (ed.) *Current Issues and Controversies in Human Rights*. Toronto: Oxford University Press.

2015b (forthcoming). "Swimming in the Fishbowl: Young People, Identity and Surveillance in Networked Spaces," in van der Ploeg, I. and Pridmore, J. (eds.) *Digitizing Identities*. London: Routledge.

Steeves, V. and Marx, G. 2014. "Safe School Initiatives and the Shifting Climate of Trust," in Muschert, G., Henry, S., Bracy N. and Peguero, A. (eds.) *Responding to School Violence: Confronting the Columbine Effect*. Boulder: Lynne Rienner Publishers, pp. 71–88.

14

Compliance-limited health privacy laws

ANITA L. ALLEN

Information privacy laws, also termed "data protection" laws, regulate the collection, use, dissemination and retention of personal information. These laws – which in the United States are products of constitutions, statutes and common law – have the social dimensions I call "compliance" and "impact" limitations. Any sort of law regulating conduct can have compliance and impact limitations; they are not unique to privacy law. Nor are compliance and impact limitations unique to *information* privacy law. Indeed, of special relevance here, laws protecting the *physical* privacy of our bodies no less than the confidentiality and security of our data can have these social dimensions.

To start, what are compliance and impact limitations as they relate to information privacy laws? Impact limitations are the adverse distributive consequences of information privacy laws, whereby some population groups benefit more than or at the expense of others. Indeed, information privacy laws that seem on their face and by design to benefit all population groups more or less equally may, in fact, disadvantage some demographic groups relative to others, by virtue of socio-culturally salient differences. The intended beneficial impact of a body of privacy law can be impaired by the societal condition of race prejudice, for example. Consider, in this respect, an illustration borrowed from Lior Strahilevitz of an impact limitation of US privacy laws restricting access to most criminal history data (Strahilevitz 2013: 2018–20). US laws that treat government-held criminal history information as private are intended to benefit ex-offender job applicants equally, but instead make winners of white job applicants and losers of African Americans. As suggested by Strahilevitz, given the familiar disproportionately high rate of African American incarceration, in the absence of reliable criminal history data to the contrary, employers will use visible race as a proxy for criminality. Employers will presume that an African American male seeking work is more likely to have a serious, violent criminal past than his white counterpart. While one must