“Honestly, We’re Not Spying on Kids”: School Surveillance of Young People’s Social Media

Leslie Regan Shade and Rianka Singh

Abstract
Social media is one of the top activities and sites for young people’s socialization in North America, raising concerns over their social privacy, because of reported instances of cyberbullying and sexting, and their informational privacy, because of commercial data collection. A trend in schools and school districts in the United States is to monitor and track, through third party applications and software, student social media during and after school, in an attempt to prevent or reduce the perceived dissemination of violence, bullying, threats, or hate instigated by students and directed toward other students or entire schools. This article will provide an overview of four of these US companies (Geo Listening, Varsity Monitor, Snaptrends, Digital Fly) and consider the policy and ethical issues of data monitoring with respect to young people’s rights to privacy and their freedom of speech.

Keywords
youth, social media monitoring, big data, surveillance, privacy rights

“Honestly, We’re Not Spying on Kids”

In September 2013, US media reported that the Glendale (California) Unified School District hired the firm Geo Listening for a contract of $40,500 in order to monitor the social media of the 14,000 middle and high school students residing in their District. Approved by the school board as an item in their “consent calendar,” where routine and non-controversial items are presented, it was later revealed that school administrators and board members were trying to conceal the issue from wider public scrutiny. As an editorial in the Los Angeles Times stated, “a public announcement might cause kids to mark all their accounts private, making it difficult for investigators to, well, investigate” (“Editorial,” 2014).

The District’s justification for monitoring social media was to ensure student safety and to confirm that student posts did not violate the school code of conduct. Public posts on social media platforms (including Facebook, Instagram, Twitter, and blogs) were thus monitored to flag any signs of depression, suicidal thoughts, violent threats, hateful statements, and bullying. The District was keen to hire Geo Listening after a pilot project was deemed to be valuable, evidenced by their claim that one potential student suicide was averted and another student admonished for posting an image of a fake gun. Reacting to criticisms of the program, especially related to privacy, Chris Frydrych, CEO of Geo Listening, replied, “Honestly, we’re not spying on kids. Can we focus back on the problem: The problem is we’re not listening effectively . . . and we’re shifting that” (Martinez, 2013). Staff attorney Lee Tien of the digital civil liberties organization, The Electronic Frontier Foundation (EFF), retorted, “This is the government essentially hiring a contractor to stalk the social media of the kids” (Martinez, 2013).

Social media, facilitated by the pervasive use of smartphones, is one of the top activities and sites for young people’s socialization in North America. According to the Pew Research Center, “24% of teens go online almost constantly” (Lenhart, 2015). While young people utilize a wide range of social media apps, Facebook remains the most popular (71%), followed by Instagram (52%), Snapchat (41%), and Twitter (33%). “Confident and enthusiastic” (Steeves, 2014a, p. 3)
characterizes young Canadians’ use of the Internet for sociality, information, and education. MediaSmart’s Young Canadians in a Wired World research project surveyed just over 5,000 Canadian students in Grades 4–11 about their use of the Internet and mobile technologies and found that youth were “highly connected” (Steeves, 2014a), using a variety of platforms to connect online, with 99% having access to the Internet outside of school via tablets, laptops, and smartphones.

Many young people are compelled to be online because of both educational and social imperatives. For instance, an increasing amount of after-school work is only accessible via the Internet (Kang, 2016). Socialization is also mediated by social media; Sarah Heath (2015), in focus groups with young Canadian women, noted how “they felt pressure from friends, community groups, and family members both to actively participate on SNS and to include friends, community group members, and family members in their online communities” (p. 369).

The popularity and prevalence of social media use elicit concerns both over young people’s social privacy, because of reported increases in cyberbullying and sexting, and their informational privacy, due to the business model of commercial data collection by popular platforms. As the Geo Listening example above demonstrates, schools and school districts, particularly in the United States, are grappling with whether and how to manage and monitor social media use by their students, both during and after school, in order to prevent or lessen the perceived propagation of threats, violence, cyberbullying, and hate directed toward other students or entire schools. This has led some school districts to deploy third party applications and software to monitor, control, and track the postings of students, under the guise of securitization and responsibilization.

Capitalizing on what can be described as a new moral panic, school monitoring tools that surveil the social media of young people display a trajectory, from earlier global positioning system (GPS) mobile phone devices and subscription-based social networking sites marketed to parents that normalize and domesticate surveillance technologies (Shade, 2011). From cradle to high school graduation, children and young people are suffused with a vast array of surveillance tools that reconfigure the texture of childhood and parenting, as safety and security concerns heighten disciplinary responses (Marx & Steeves, 2010).

In many ways, these surveillant devices exemplify what Shoshana Zuboff (2015) refers to as “surveillance capitalism,” which she describes as “a new form of informational capitalism [that] aims to predict and modify human behavior as a means to produce revenue and market control” (p. 75). Zuboff further argues that surveillance capitalism personifies “a new social relations and politics that have not been well delineated or theorized” (p. 76). Building on Zuboff’s idea of surveillance capitalism, this article will present an overview of four US companies that provide social media monitoring tools to schools and school districts (Geo Listening, Varsity Monitor, Snaptrends, Digital Fly) and consider the ethical and policy issues of such intense data monitoring with respect to young people’s right to privacy and freedom of speech.

Company Analysis

The four companies chosen for analysis are privately owned American companies. A report in the Christian Science Monitor describes these companies as comprising a “secretive industry that jealously guards its tradecraft, revenue, and even their physical location” (Carollo, 2015). As Dana Priest and William Arkin documented in their Washington Post series (Priest & Arkin, 2012), a network of new firms was surreptitiously created after September 11th in order to ostensibly safeguard America; this security–surveillance industrial complex has a vast and largely unregulated reach. While the social media monitoring companies described in this article are not part of this large apparatus per se, their focus on threat assessment in schools is also privatized and in some instances, clandestinely conducted by school districts. The necessity for social media monitoring given by these companies is couched in positive terms; as Kate Crawford’s (2009) work on the technologies of listening illustrates, the act of listening can involve an ethics of care and custodianship, as well as an instructional role, in ensuring that students are properly using and maintaining a social media profile for school security and their personal safety and future career enhancement. But as this article will argue, this business imperative intensifies ethical issues regarding young people’s rights to privacy and their freedom of speech under a regime of commercial data monitoring.

Geo Listening

Every day in our schools many children will have social and emotional needs that go unnoticed and unmet. In their searching for someone who understands and that can help, students have most often chosen to post their concerns, thoughts and fears to the public pages of social networks. Make yesterday the last day that you were not able to effectively identify and engage with these students to meet their needs. (“Why Choose Geo Listening?”)

Geo Listening positions themselves as a service that can help mitigate issues of young people who are dealing with emotional or social problems, with schools seen as sites of risk for youth. The goal of Geo Listening is to monitor, analyze, and report to school administrators, on a daily basis, relevant public social media postings made by students aged 13 and older that could be cause for concern. Postings are flagged for negative content: counter to the school code of conduct, evidencing violent threats to other students or the school, cyberbullying, or self-harm. According to Geo Listening CEO Frydrych, the daily reports submitted to the schools
consist of screen captures of flagged posts from social media, “along with details of whether they were made on or off campus, the time and date, the user’s name, if available, and a description of why the post caught the attention of analysts” (Ceasar, 2013). Geo Listening employs a small full-time staff and, says Frydrych, a global team of contract workers who work half-days since “the content they read is so dark and heavy” (Frydrych, quoted in Martinez, 2013).

As described on their website, daily reports account for the frequency and severity of posts, which are categorized for bullying, cyberbullying, despair, hate, harm, crime, vandalism, substance abuse, and truancy. The list of problematic content begins with behavior that might be of harm to students only, but gradually moves toward actions that are harmful to schools themselves, thus displaying a move from an interest in the safety of those being surveilled (youth) to protection of those who are doing the surveilling (the schools and school districts).

Rather than owning any potential ethical issues related to monitoring, Geo Listening places the blame on young people themselves for not properly securing their social media profiles in the interest of gaining popularity. For instance, in their frequently asked questions (FAQ), which asks, “Can you explain privacy and social networks?” the response is

Users of social networks receive a username and password, which gives them a right to publish social commentary and media. Most users below the age of 25 do not utilize the available privacy settings because they are seeking to be recognized for their respective posts. They have chosen to post in the public domain in exchange for popularity and a decreasing ability to communicate effectively face to face.  

By claiming that users “have chosen” to post, can this be read to imply that Geo Listening is arguing that students have opened themselves up to monitoring? Their assumption that “users below the age of 25 do not utilize the available privacy settings” is not reflected in qualitative research on young people’s understanding, management, and negotiation of social media privacy. For instance, the digital literacy organization MediaSmarts found that regarding social privacy, youth pay attention to social expectations around the sharing of information and are aware of how to use privacy settings to manage their interpersonal relationships (Steeves, 2014b). However, with informational and data privacy, MediaSmarts found that youth need to acquire more knowledge on the information collection practices of the corporate sites they use, as many youth erroneously believed that privacy policies implied that a company would not share their personal information with others (Johnson, 2015, p. 347).

Glendale Unified School District reported that in the first year of monitoring by Geo Listening, 1,400 incidents were reported, but when further investigated by school officials, many posts evidenced mere “adolescent humor.” Despite these results, school board members defended the monitoring: “This is not an invasion of privacy . . . this is just taking public information and using it for our students’ well-being” (Corrigan, 2014).

Varsity Monitor

We look for things that could damage the school’s brand and anything related to their eligibility. (Sam Carnahan, CEO of Varsity Monitor, cited in Thamel, 2012)

College athletics are a lucrative business in the United States; as Taylor Branch (2011) writes, “Big-time college sports are fully commercialized. Millions of dollars flow through them each year.” Ensuring the integrity and reputation of athletes, coaches, colleges, and universities in this competitive atmosphere is an ongoing issue for the National Collegiate Athletic Association (NCAA), which also needs to secure its own reputation.

Varsity Monitor is a niche service designed specifically to monitor college and high school athletes who have athletic scholarships and those who may have potential professional sports scholarships or contracts at stake; it is felt that a negative social media presence could jeopardize these opportunities. Created by several former Division 1 collegiate athletes and business partners with experience in social media compliance, the service charges universities between $7,000 and $10,000 per year. The company offers three specific rationales for their business. The first is that athletes and their parents need to be concerned about their online presence as sports recruiters check social media profiles. The second is that schools need to use Varsity Monitor in order to check students’ social media to ensure students are “upholding standards,” whether for personal reputation or related to the terms of their contracts. And third, the company provides educational resources for student athletes to learn what is appropriate to post online.

Varsity Monitor cites several specific benefits of their social media monitoring service for athletic departments, teams, and sports professional organizations. According to promotional material on their website, they claim that their service “only takes minutes per day, with no software administration.” They offer “full image monitoring” of “all images posted by athletes, to ensure complete coverage of all posted content.” They monitor the connections and conversations of friends in order to ensure that “agents, boosters and local business people aren’t communicating with and compromising your student athletes.” This “full 360 degree view into the online behavior” of athletes also monitors third party content about “what is being said about your athletes.” They highlight that positive messaging can be further used for marketing and engaging with fans. Athletic recruits can be evaluated before any scholarship offers are made, with a scan of “4 years of social media history.”

Varsity Monitor states that it “respects student athlete privacy and is compliant with all state legislation.” This is the
only mention of privacy on their site. However, Varsity Monitor’s third party content and their “360 view” of athletes indicate that they monitor not only specific student athletes but also a large spread of their friends and ancillary social media users in their wider network. Troubling enough, other students and friends would not have any indication of this monitoring. The promotional benefits of Varsity Monitor are geared toward monitoring the social performance of students, despite their claims of providing knowledge about the appropriate uses of social media.

Snaptrends

Today’s schools are faced with serious issues on a daily basis. With cyber-bullying, school violence, self-harm and other potential threats, it is important for educational institutions to use any means available to provide a secure environment. (Snaptrends, Social Media for Education)

Snaptrends Inc. is a “social observer system” founded in 2012 with company headquarters in Texas. In 2015, they reported raising $225,015 of a planned $2-million financing (Calnan, 2015). They offer “location-based social intelligence” for many industries, including corporate security, health care, law enforcement, energy and utilities, sports and athletics, and the educational sector. The company uses advanced analytics, custom keywords, and geofencing—providing geolocation information for schools, school athletic venues, and study abroad locations. As their promotional material describes, their service provides

...real-time and historical location-based social media posts inside a user-defined lens, which can be of any shape or size anywhere in the world. You can drop multiple lenses or a single lens in conjunction with social media monitoring outside of the lens. With Snaptrends’ proprietary algorithms and processes, you hear the full spectrum of the social conversation no matter where it takes place.9

The technology grabs and analyzes posts and messages, creating a social media map comprising the keywords posted from the lens-covered locations. Officials can then be “alerted with real-time insights into potential issues so they can make critical decisions to ensure the safety and well-being of their population.”10 The keywords culled from social media posts relate to the prevention of school violence, suicide, cyberbullying, truancy, and illegal drugs sales.

A 1-year license to Snaptrends costs a school district $14,000. A member of a school district in Florida using the service for students and staff said,

According to Vaas, Snaptrends is part of the Central Florida Intelligence Exchange, the local law enforcement Fusion Center. Fusion centers are information-sharing sites established after September 11th by the US Department of Homeland Security and include local law enforcement entities and private sector security companies (Department of Homeland Security, n.d.).

Digital Fly

We monitor the technologies students use, so that you can focus on keeping your school safe. (Digital Fly website)

Launched in September 2015, Digital Fly (“Your Fly on the Wall”) is a spinoff of Intelligent Product Solutions (Marketwired, 2015). Their Fly Paper Engine can “monitor threats in real-time to help prevent the next incident before it happens.”12 Promotional material positions the provision of security for students and staff in light of recent school shootings in the United States as a major reason for monitoring social media. Other cited reasons are to prevent “bullying, self-harm, gang activity, theft, hate crimes, vandalism, wild parties, substance abuse, and truancy.”13 Using geolocation techniques, Digital Fly claims that it can monitor social media within a 10-mile radius of a school, using keywords selected by the school district. The service is priced based on a per student cost of $1.75 or $3.00 per student, depending on the size of the school.

There are several unique features to Digital Fly. They have a Watch List, where the school district can “Create and manage [their] own watch list using key words, hashtags, users, groups and location”; a Tip Line, which is “An anonymous tip line for people to text. Informers can give warning of an incident without any connection”; and an Incident Rewind, wherein school districts can “Turn back time and search for evidence of malintent leading up to an incident. Look for signs to prevent the behavior in the future.”14 Targeting specific students and creating watch lists with certain users poses a potentially deeper ethical issue in social sorting and discrimination based on race and ethnicity. For instance, on the Digital Fly website, an example is given of a Watch List with keyword searches for Beat Down, Drugs, Drunk, Fight, NYC Alcohol, NYC Bar, NYC Drink, NYC Drug, and so on. An example highlighting “Drunk” is provided, with typing mistakes:

Username: King_Zip
Text: So what we get drunk? So what we smoke weed? Were just having fun We don’t care who sees So what we go out? That’s how its supposed to be
Profile:
Location:
Date Created:
Source: Twitter15
Privacy Policies

Table 1 provides an overview of the privacy policies displayed on the websites for Geo Listening, Varsity Monitor, and Snaptrends. There was no available privacy policy on the Digital Fly website (this may be provided for subscribers only). The table explicates their statements on data collection, data retention, third party access, and compliance to the Children’s Online Privacy Protection Act (COPPA, 1998), which regulates the collection of information for children under the age of 13. The monitoring demographic for these services is generally ages 14–18 for high school students and up to age 25 for college-aged students. Geo Listening was the only company to mention COPPA in their privacy policy.

In terms of data collection, all of the services state that they just target and monitor publicly available social media content, but only Varsity Monitor explicitly states that they may collect information from individual users’ friends and their wider social network. Geo Listening and Snaptrends obscurely explicate the terms of data retention to constitute when the service is no longer under contract or only for potential legal purposes. Geo Listening is clear that for third party access only participating schools and school districts may share information, whereas both Varsity Monitor and Snaptrends provide many caveats about when they may share information.

In terms of the type of data analytics the companies are engaged in, how the data are collected and analyzed, whether they are cross-correlated with other types of student data or deployed for marketing purposes, the privacy policies adopt a standard utterance of what we call “privacy prevarication”: language that hedges potential or future inevitabilities in changes in company ownership or partnerships, and statements that cede control over information disclosure to third parties to the client, customer, or user, on the basis of their consent to the terms of service. Geo Listening remarks that if another company acquires them, data they have collected may be under the purview of the contract or only for potential legal purposes. Geo Listening is clear that for third party access only participating schools and school districts may share information, whereas both Varsity Monitor and Snaptrends provide many caveats about when they may share information.

It is not clear from the privacy policies of these companies what specific types of data analytics are considered, and whether and how this information is cross-referenced with other sorts of educational information and records about the student. It is also not transparent whether data are correlated with social media profiles the student may have on other platforms, including the profiles of friends and students within their wider social media network. This web of captured connections facilitated by the interconnectedness of platforms in this commercial infrastructure is redolent of Haggerty and Ericson’s (2000) conception of the surveillant assemblage, which consists of discrete and multifarious forms of human and technical mechanisms for surveillance governed by state, corporate, and other non-state entities, such as human relationships. A key concern is whether or not parents, guardians, and the students themselves are aware of the social media monitoring and the method of reasonable consent provided by the services.

The Ethics of Monitoring: Whose Privacy Rights?

People say that’s not private: It’s public on Facebook. I say that’s just semantics. The question is what is the school doing? It’s not stumbling into students—like a teacher running across a student on the street. This is the school sending someone to watch them. (EFF Staff Attorney Lee Tien, quoted in Martinez, 2013)

Zuboff’s model of surveillance capitalism describes a “new logic of accumulation” (p. 85) wherein “populations are targets of data extraction” (p. 86). While Zuboff was explicitly referring to the vast power of the Google Corporation to amass huge amounts of personal data from mining, analysis, and monetization, the (albeit) smaller profits of the social media monitoring companies described in this article warrant further scrutiny.

Andrew Hope (2015) details the incursion of the surveillance industry and marketers into schools in the United Kingdom and United States. He refers to David Buckingham’s notion of the educational–technological complex, arguing that we need more scrutiny of the role of the commercial information technology (IT) and data industry in the expansion of a new educational–surveillance complex. As Hope demonstrates, new forms of governmental participation contribute to an actuarial turn in school surveillance and the commercialization of responsibilization by parents and adults, leading to a blurring of the public and private, the school and the home—and perhaps contributing to a culture of complacency when it comes to monitoring (on surveillance in schools, see also Fisk, 2014; McCahill & Finn, 2010; Monahan & Torres, 2009). Likewise, the spread of big data tools into K–12 educational practices and pedagogy raises ethical questions and the need to craft appropriate policy responses in different jurisdictions (Regan, Jesse, & Khwaja, 2016).

Jessica Fahlquist (2015) prompts us to consider ethical questions when we monitor children, including privacy and free speech. In the case of the social media monitoring companies described in this article, it is important to note that their services monitor the social media of students when they are both inside and outside of school. This poses free speech implications if young people are punished for material they made outside of school. The legality of these practices in the
| **Table 1. Privacy Policies for Geo Listening, Varsity Monitor, and Snaptrends.** |
|---|---|---|
| **Data collection** | Geo Listening collects and compiles public content from social media sites (Twitter, Facebook, Instagram, Vine, ask.fm, YouTube, and Google+) school/school districts. Information collected can include username, date and timestamp, geolocation data, and full contents of public posts. | Varsity Monitor collects information and content made visible to “everyone” on Facebook and information that Facebook deems to be publicly available information. Users are asked to grant access to limited, additional Facebook information “(1) posted by user; (2) posted or tagged to user’s account by other Facebook users; or (3) associated with user’s account by Facebook.” Other information collected includes “contact information, ‘liked’ items, profile information, posts in newsfeed, photos and videos uploaded to Facebook, calendar of events, custom friend lists, online presence, ‘check-ins,’ family members and relationship details and status, information about friends.” “Even if not explicitly allowed access to Facebook Information, subject to Facebook settings, Varsity Monitor may collect information about user to the extent it is posted to, or associated with the Facebook accounts of user’s friends who have authorized Varsity Monitor to collect their information.” Snaptrends collects content derived from websites and social networking sites that are “publicly available and accessible via standard search engine technology and methods.” Use of web crawlers may be deployed to obtain content through publicly available APIs, according to the terms and protocols of the websites, “including without limitation any robots.txt protocols.” Snaptrend’s policy is to “never circumvent technical controls, such as usernames and passwords, to obtain Content, nor do we seek to thwart CAPTCHA technology.” Web crawling is limited to public information made available by the website operator. |
| **Data retention** | Geo Listening retains the information only “for as long as necessary to accomplish the purposes of the Monitoring Service described above, or as long as permitted by law.” They do not retain the collected information for purposes other than providing the monitoring information to school and school districts. Collected information is destroyed “when it no longer furthers the purposes stated in this Privacy Policy or the contract term has expired without a continuing contract.” | Varsity Monitor collects information and content made visible to “everyone” on Facebook and information that Facebook deems to be publicly available information. Users are asked to grant access to limited, additional Facebook information “(1) posted by user; (2) posted or tagged to user’s account by other Facebook users; or (3) associated with user’s account by Facebook.” Other information collected includes “contact information, ‘liked’ items, profile information, posts in newsfeed, photos and videos uploaded to Facebook, calendar of events, custom friend lists, online presence, ‘check-ins,’ family members and relationship details and status, information about friends.” “Even if not explicitly allowed access to Facebook Information, subject to Facebook settings, Varsity Monitor may collect information about user to the extent it is posted to, or associated with the Facebook accounts of user’s friends who have authorized Varsity Monitor to collect their information.” Snaptrend’s policy is to “never circumvent technical controls, such as usernames and passwords, to obtain Content, nor do we seek to thwart CAPTCHA technology.” Web crawling is limited to public information made available by the website operator. |
Table 1. (Continued)

| Third party access | Geo Listening (https://geolistening.com/privacy-policy/) | Varsity Monitor (http://varsymonitor.com/privacy-policy.php) | Snaptrends (http://snaptrends.com/social-content-policy/and http://snaptrends.com/privacy-policy/) |
|--------------------|---------------------------------------------------------|-------------------------------------------------------------|--------------------------------------------------------------------------------------------------|
| Geo Listening shares information it collects with participating school/school districts "solely to assist school districts in ensuring student safety, as identified throughout this Privacy Policy."
"Only the information our Monitoring Service collects for a particular participating school or school district is shared with that particular school or school district." | Shares information it collects with participating schools.
It may share information if there is a "good faith belief" that it is necessary to detect, prevent, and address fraud and other illegal activity and to prevent death or imminent bodily harm. It may share information with other third parties, with consent, and if the company sells or trades assets. Information will not be provided to third parties "for any other purposes, including for marketing their products or services."
| May share data about customers with contracted service providers.
Will not share, sell, rent, or trade information with third parties for promotional purposes.
"From time to time, we may partner with other companies to jointly offer products or services. If you purchase or specifically express interest in a jointly-offered product or service, we may share data collected in connection with such purchase or expression of interest with our partner(s)."
| COPPA | Monitoring Service is fully compliant with the Children’s Online Privacy Protection Act (COPPA).
If personal information from a child under 13 is collected without authorization of parental or guardian consent, “Geo Listening will notify the participating school district representatives and delete any personal information associated with that child as quickly as possible.” They will take “reasonable steps to identify and delete any records that do not comply with COPPA.” | "You may stop the Company from collecting and using Your Information at any time by (i) uninstalling the VM Application and setting your Facebook privacy settings to prevent the VM Application from accessing Your Information through your friends or (ii) by deleting your Facebook account.” | "If we hold Content about you, or you think we hold such Content, you may have the legal right, upon written request, to access such Content (subject to certain exceptions), and request that such information be corrected or deleted, as the case may be, if it is incomplete or inaccurate, or if we have obtained it in violation of applicable law.” |
| Other notable details | N/A | | |

API: application programming interface.
United States has been examined by Catherine Mendola (2015), who remarks that because there are no legal precedents by the Supreme Court concerning off-campus Internet speech to date, “it is unclear whether schools may legally surveil students’ Internet posts in order to protect the school population from a substantial disruption to its educational goals” (p. 171). Furthermore, in considering whether it is appropriate to conduct Internet surveillance, the issue of ensuring (or chilling) free speech is paramount, “as students would know that their posts were monitored and consequently could choose not to express their thoughts on the Internet” (pp. 178–179).

Helen Nissenbaum’s (2010) notion of “contextual integrity”—the various informational contexts that govern or habituate privacy norms—is also key in considering students’ informational privacy, especially with the context collapse of in-school and after-school communication on social media. Following Nissenbaum’s characterization of privacy as contextual integrity, control over personal information—the ability to determine what information gets collected, how it is used in certain contexts, and for how long it is retained—is essential for upholding privacy as a fundamental right of citizenship. For many young people, unaware of how their social media usage affects their personal privacy, the conditions of social media monitoring by schools, which may or may not be overt, draw attention to a shifting privacy–information rights dichotomy, which complicates reasonable expectations of privacy within and outside of school.

Another ethical issue is access and use of publicly available social media content; recent research on the ethical challenges of big data content is illustrative here. Not only does big data, referring to the collection, aggregation, manipulation, and dissemination of large data sets for corporate and government information practices, increase the risk of accumulating personal information without the user’s awareness or consent, it also lends itself to what Kate Crawford and Jason Schultz (2014) describe as “predictive privacy harms” (p. 95): the collection and use of information that draws attention to a person’s data behaviors. This is particularly troubling when publicly available social media content is used, or misconstrued, in unforeseen ways. Grappling with the ethics of privacy, consent, and anonymity in social media (Zimmer, 2010) and big data (Metcalf & Crawford, 2016; Zwitter, 2014) is not only a concern for academic researchers but also a growing recognition in the big data industry itself, where data stewardship practices are becoming more common (Martin, 2015).

A host of other questions arise from social media monitoring. Are parents and guardians apprised of the monitoring? Can parents and guardians and students opt out of monitoring? What are parental attitudes about their children’s online privacy in the domestic environment, and do they construe surveillance via monitoring as a protective or disciplinary measure (Clark, 2012)? What are the provisions for data access and retention, especially when young people leave a school district or graduate? As Kathryn Montgomery (2015a) remarks, given the proliferation of digital monitoring, data collection, and big data analytics into the educational and domestic sector, we need to remain cognizant of “the specter of ‘digital dossiers’ that could follow young people into adulthood, affecting their access to education, employment, health care, and financial services” (p. 268).

**Public Interest and Policy Responses**

Instigated by the commercial abundance of the Ed-Tech industry and profuse social media use by students, legislation and campaigns about student privacy are increasing in the US. FERPA (Family Educational Rights and Privacy Act), is an earlier federal law enforced by the Department of Education to protect the privacy of children’s educational records (report cards, transcripts, disciplinary records, contact and family information, and class schedules) and student information for online activities that use school-issued devices (US Department of Education, 2007). However, much student data collected by schools and private companies in the era of big data and education are not covered by FERPA. Recognizing this, the Future of Privacy Forum and the Software & Information Industry Association (SIIA) created a Student Privacy Pledge to safeguard student privacy. The pledge aims to limit the collection, use, and sharing of student personal data to authorized educational institutions, not to sell student data, or to use and disclose data for behavioral targeting of advertisements to students (Future of Privacy Forum and the SIIA, 2016).

The Electronic Privacy Information Center (EPIC) created a Student Privacy Bill of Rights that “puts students back in control of their data and provides the privacy, security, and due process protections that students deserve” (Strauss, 2014). The Student Privacy Bill of Rights provides principles for access and amendment of student data, focused collection of data, respect for the context of how students provided the data, security through responsible data practices, transparency around clear and accessible privacy and security practices, and accountability by schools and private companies over the management of their data (EPIC, 2014).

The EFF campaign, *Spying on Students: School-Issued Devices and Internet Privacy*, focuses on the privacy risks of school-supplied electronic devices and software and the privacy rights of students and their parents/guardians in the United States (EFF, 2015). EFF is especially concerned with the implications of the widespread use of Google Apps for Education (GAFE) and other cloud-based services.

The State of California introduced three bills in 2014–2016 to strengthen the privacy rights of students. Assembly Bill 1584 mandates what information must be included in contracts with third party educational software and digital record providers (State of California, Assembly Bill 1584,
2014), while Assembly Bill 1177 applies to companies that provide online services for K-12 students (State of California, Assembly Bill 1177, 2014). Both pieces of legislation contain provisions on ensuring the confidentiality and security of student data and prohibit the targeting of behavioral marketing to students. Assembly Bill 1442 provides mechanisms and redress specifically for social media monitoring. It requires notification to students, parents, and guardians when schools and school districts are considering the adoption of social media monitoring; requires notification to parents and guardians about monitoring programs; provides restrictions on monitoring to encompass only content and information relevant to student or school safety; allows students to see what information has been collected about them; provides mechanisms to redress incorrect information, or to request the removal of information; and mandates the destruction of all student information when students turn 18 and/or leave the school or school district (State of California, Assembly Bill 1442, 2014). In July 2015, a Glendale Unified School District official responded that they were compliant with the new law (Corrigan, 2015).

The political economy of big data, the commercial structure of social media, and the nuances of behavioral advertising create a preponderance of privacy concerns for students and young adults that California legislation and public interest advocacy are addressing. The efficacy of such legislation by corporations and schools will need to be assessed with regard to compliance amid the attendant preponderance of big data and diffuse algorithmic structures that constitute Zuboff’s conceptualization of surveillance capitalism. These responses also highlight the importance of citizenship-based media education to align around privacy rights.

Taking Back the Monitoring?

Surveillance has become a normalized facet of young people’s online lives. Many recognize this and while they don’t really like it, they recognize that this is the literal price of “free” social media. This is the paradoxical nature of social media; their convenience factor—used intensely by many youth (and adults!) for mundane activities, communication, community building, research, news, education, entertainment, and employment—is offset by their architecture of participation and terms of use (Werbin, 2014). Of concern is that this normalization of surveillance in social and mobile media will “undoubtedly shape the way they construct their identities, communication, and social and civic practices in unforeseeable ways” (Vickery, 2014, p. 399). Surveillance of young people can erode their trust in parents, authority figures, schools, and the state; it can stifle the development of autonomy, resilience, and agency; it can further impact moral development (Office of the Privacy Commissioner of Canada [OPC], 2012). Surveillance in schools undermines the values of education and the democratic nature of citizen engagement (Hope, 2016). It is a tactic of disciplinary governance wherein responsibilization, as Wendy Brown (2015, p. 133) argues, operates as a “regime” to organize, measure, and reorient individuals.

Balancing social media privacy for young people with the need to ensure their safety and security does not mean that we sacrifice their privacy rights nor jeopardize their rights to free speech and participatory communication. The rights of children and young people are intertwined with their use of digital media. This is a pressing concern for Internet governance, as currently one in three Internet users globally is under the age of 18 (Livingstone, Carr, & Byrne, 2016).

Gry Hasselbalch Lapenta and Rikke Frank Jørgensen (2015) raise important questions for public policy to consider regarding youth, privacy, and social media. The first is to reframe privacy rights to consider and distinguish between social privacy (among family, friends, peers) and informational privacy (personal information collection by commercial and corporate entities). The second is to consider the role that commercial and corporate entities play in shaping the nature of our privacy; what rights do we cede with their terms of service, and how have they become so pervasive that they constitute a new public infrastructure? Third, how can we reshape the business model and the structural affordances of commercial social media platforms to allow for personal control?

This nexus of social media, youth, and privacy points to a heightened form of “panoptic sort” as theorized by Oscar Gandy (1993) almost 25 years ago. In his study on the political economy of personal privacy, Gandy argued that the panoptic sort was a discriminatory technology characterized by its ability to socially sort people into categories ascribed by economic value. To class we can add race, gender, and sexuality. Surveillance ethics thus need to be considered from an intersectional perspective. Software that monitors social media to detect content that suggests terrorist radicalization or recruitment of young people could lead to the undue surveillance of minority and Muslim youth; data discrimination can be both overtly and covertly racialized (Gangadharan, 2014; Khadaroo, 2015). Jacqueline Vickery’s (2015) research on how non-dominant youth manage and negotiate social and mobile privacy leads her to argue that “the consequences of surveillance . . . necessitate critical inquiry into the complicated relationship between performance, surveillance, privacy, and exploitation” (p. 294).

Youth have learned how to subvert surveillance from parents or school authorities by a variety of means. danah boyd (2014) refers to the practice of young people deploying social steganography “or hiding messages in plain sight by leveraging shared knowledge and cues embedded in particular social contexts” (p. 65) as one way to achieve privacy. The use of in-group references, slang, falsified information, and limiting information are other modes of resistance (Media Literacy Week, 2012).
Montgomery (2015b) argues that with the encroachment of big data into the educational and leisure realms of young people, robust privacy laws and consumer protection must be developed in tandem with the creation of a new social movement that includes advocacy organizations, academics, parents, and youth. Promoting digital policy literacy, which provides a framework for young people to comprehend policy processes, the political economy of social media, and the socio-technical infrastructures of social media platforms (Shade, 2015; Shade & Shepherd, 2013), can also contribute to an empowerment approach to privacy for youth, which provides agency to youth in the management and negotiation of their privacy (Regan & Steeves, 2010). For it is indeed the voices of youth that are missing in these debates, as the EPIC Student Privacy Bill of Rights recognized. Responding to the Glendale Unified School District’s monitoring of social media in the Los Angeles Times, Young Cho, a 16-year-old high school, stated that while she supported the practice to keep students safe, social media is not a private place, not really a safe place . . . it’s not the same as being in school. It’s students’ expression of their own thoughts and feelings to their friends. For the school to intrude in that area—I understand they can do it, but I don’t think it’s right. (Caesar, 2013)

Declaration of Conflicting Interests
The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding
The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: The research for this article was funded by the eQuality Partnership Grant from the Social Sciences and Humanities Research Council of Canada (SSHRC). For information, see: http://www.equalityproject.ca/

Notes
1. On social media monitoring in the United States, see Sengupta (2013), Stephens (2014), Simon (2015), and Farivar (2013). Social media monitoring in Canadian schools, and monitoring services and school district responses, is the subject of a CBC article: Hamilton (2016).
2. “Why Choose Geo Listening.” https://geolistening.com/
3. See https://geolistening.com/why-choose-us/
4. See https://geolistening.com/faq/
5. See http://varsitymonitor.com/benefits.php
6. See Note 5.
7. See http://snaptrends.com/social-media-for/education
8. See http://www.bloomberg.com/research/stocks/private/snapshot.asp?privcapId=214710959
9. See http://snaptrends.com/social-media-software/geofencing/
10. See Note 9.
11. See http://www.digitalfly.net/
12. See Note 11.
13. See http://www.digitalfly.net/#!products-and-services/c14un
14. See Note 13.
15. See Note 14.
16. See Geo Listening Privacy Policy at http://geolistening.com/privacy-policy; Varsity Monitor at http://www.varsitymonitor.com/privacy-policy.php; and Snaptrends at http://snaptrends.com/privacy-policy/

References
boyd, d. (2014). It’s complicated: The social lives of networked teens. New Haven, CT: Yale University Press.
Branch, T. (2011, October). The shame of college sports. The Atlantic. Retrieved from http://www.theatlantic.com/magazine/archive/2011/10/the-shame-of-college-sports/308643/
Brown, W. (2015). Undoing the demos: Neoliberalism’s stealth revolution. New York, NY: Verso Books.
Calnan, C. (2015, May 29). Snap Trends raises portion of $2M funding. Austin Business Journal. Retrieved from http://www.bizjournals.com/austin/blog/techflash/2015/05/snap-trends-raises-portion-of-2m-funding.html
Carollo, M. (2015, November 16). The secretive industry of social media monitoring. Christian Science Monitor. Retrieved from http://www.csmonitor.com/World/Passcode/2015/1116/The-secretive-industry-of-social-media-monitoring
Cesari, S. (2013, September 14). Glendale district says social media monitoring is for student safety. Los Angeles Times. Retrieved from http://www.latimes.com/local/la-me-glendale-social-media-20130915-story.html
Children’s Online Privacy Protection Act. (1998). Washington, DC: Federal Trade Commission. Retrieved from https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule
Clark, L. S. (2012). The parent app: Understanding families in the digital age. New York, NY: Oxford University Press.
Corrigan, K. (2014, August 14). GUSD continues to monitor students’ social media posts. Los Angeles Times. Retrieved from http://www.latimes.com/tn-gnp-me-0814-geolistening-monitoring-to-continue-20140814-story.html
Corrigan, K. (2015, July 22). Glendale Unified renews online monitoring policy. Los Angeles Times. Retrieved from http://www.latimes.com/tn-gnp-glendale-unified-renews-online-monitoring-policy-20150722-story.html
Crawford, K. (2009). Following you: Disciplines of listening in social media. Continuum: Journal of Media & Cultural Studies, 23, 525–535.
Crawford, K., & Schultz, J. (2014). Big data and due process: Toward a framework to redress predictive privacy harms. Boston College Law Review, 55, 93–128.
Department of Homeland Security. (n.d.). Fusion center locations and contact information. Retrieved from https://www.dhs.gov/fusion-center-locations-and-contact-information
Editorial: Geo listening in the light, finally. (2014, August 16). Los Angeles Times. Retrieved from http://www.latimes.com/tn-gnp-me-0816-editorial-geo-listening-in-the-light-finally-20140816-story.html
Electronic Frontier Foundation. (2015). Spying on students: School-issued devices and student privacy. Retrieved from https://www.eff.org/issues/student-privacy
Electronic Privacy Information Center. (2014). Student bill of rights. Retrieved from https://epic.org/privacy/student/bill-of-rights.html
Fahlquist, J. N. (2015). Responsibility and privacy: Ethical aspects of using GPS to track children. *Children & Society, 29*, 38–47.

Farivar, C. (2013, September 16). California school district hires online monitoring firm to watch 13,000 students. *ArsTechnica*. Retrieved from http://arstechnica.com/tech-policy/2013/09/california-school-district-hires-online-monitoring-firm-to-watch-13000-students

Fisk, N. (2014). “. . . When no one is hearing them swear”: Youth safety and the pedagogy of surveillance. *Surveillance & Society, 12*, 566–580. Retrieved from http://www.surveillance-and-society.org

Future of Privacy Forum and the Software & Information Industry Association (SIIA). (2016). *Student privacy pledge*. Retrieved from https://studentprivacypledge.org/

Gandy, O. H. (1993). *The panoptic sort: A political economy of personal information*. New York, NY: Westview Press.

Gangadharan, S. P. (Ed.). (2014). *Data and discrimination: Collected essays*. Washington, DC: Open Technology Institute, New America Foundation. Retrieved from https://www.newamerica.org/oti/data-and-discrimination/

Haggerty, K. D., & Ericson, R. V. (2000). The surveillant assemblage. *British Journal of Sociology, 51*, 605–622.

Hamilton, B. (2016, March 19). Safety in schools: Will social media monitoring help keep schools safe? *CBC News*. Retrieved from http://www.cbc.ca/news/canada/canadian-school-safety-social-media-monitoring-1.3479718

Heath, S. (2015). Security and insecurity online: Perspectives from girls and young women. In J. Bailey & V. Steeves (Eds.), *eGirls, eCitizens* (pp. 361–383). Ottawa, Ontario, Canada: University of Ottawa Press.

Hope, A. (2015). Governmentality and the “selling” of school surveillance devices. *The Sociological Review, 63*, 840–857.

Hope, A. (2016). Biopower and school surveillance technologies 2.0. *British Journal of Sociology of Education, 37*, 885–904.

Johnson, M. (2015). Digital literacy and digital citizenship: Approaches to girls’ online experiences. In J. Bailey & V. Steeves (Eds.), *eGirls, eCitizens* (pp. 339–360). Ottawa, Ontario, Canada: University of Ottawa Press.

Kang, C. (2016, February 22). Bridging a digital divide that leaves schoolchildren behind. *The New York Times*. Retrieved from http://www.nytimes.com/2016/02/23/technology/fcc-internet-access-school.html

Khadoroo, S. T. (2015, July 24). Could school computers be a tool in preventing ISIS from recruiting teens? *Christian Science Monitor*. Retrieved from http://www.csmonitor.com/USA/Education/2015/0724/Could-school-computers-be-a-tool-in-preventing-ISIS-from-recruiting-teens

Lapenta, G. H., & Jørgensen, R. F. (2015). Youth, privacy and online media: Framing the right to privacy in public policymaking. *First Monday, 20*, Retrieved from http://firstmonday.org/ojs/index.php/fm/article/view/5568/4373

Lenhart, A. (2015). *Teens, social media & technology overview 2015*. Pew Research Centre. Retrieved from http://www.pewinternet.org/2015/04/09/teens-social-media-technology-2015/

Livingstone, S., Carr, J., & Byrne, J. (2016). *One in three: Internet governance and children’s rights* (Office of Research-Innocent, Discussion Paper 2016-01). Florence, Italy: UNICEF Office of Research. Retrieved from https://www.cigonline.org/sites/default/files/no22_2.pdf

Marketwire. (2015, September 10). *Digital fly launches real time social media monitoring and alert service for schools*. Retrieved from http://www.marketwired.com/press-release/digital-fly-launches-real-time-social-media-monitoring-and-alert-service-for-schools-2054501.htm

Martin, K. (2015). Ethical issues in the big data industry. *MIS Quarterly Executive, 14*, 67–85.

Martinez, M. (2013, September 18). California school district hires firm to monitor students’ social media. *CNN*. Retrieved from http://www.cnn.com/2013/09/14/us/california-schools-monitor-social-media/

Marx, G., & Steeves, V. (2010). From the beginning: Children as subjects and agents of surveillance. *Surveillance & Society, 7*, 192–230. Retrieved from http://www.surveillance-and-society.org

McCahill, M., & Finn, R. (2010). The social impact of surveillance in three UK schools: Angels, devils, and teen mums. *Surveillance & Society, 7*, 273–289. Retrieved from http://www.surveillance-and-society.org

Media Literacy Week. (2012). *Constant surveillance: Youth privacy in a digital age*. Retrieved from http://www.medialiteracyweek.ca/2012/08/constant-surveillance-youth-privacy-in-a-digital-age/

Mendola, C. E. (2015). Big brother as parent: Using surveillance to patrol students’ internet speech. *Boston College Journal of Law & Social Justice, 35*, 153–192. Retrieved from http://lawdigitalcommons.bc.edu/jlsj/vol35/iss1/7

Metzalf, J., & Crawford, K. (2016, January–June). Where are human subjects in big data research? The emerging ethics divide. *Big Data & Society, 1–14*. doi:10.1177/2053951716650211. Retrieved from http://bds.sagepub.com/content/3/1/2053951716650211.full.pdf+html

Monahan, T., & Torres, R. D. (Eds.). (2009). *Schools under surveillance: Cultures of control in public education*. New Brunswick, NJ: Rutgers University Press.

Montgomery, K. (2015a). Children’s media culture in a big data world. *Journal of Children and Media, 9*, 266–271.

Montgomery, K. (2015b). Youth and surveillance in the Facebook era: Policy interventions and social implications. *Telecommunications Policy*, 39, 771–786.

Nissenbaum, H. (2010). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford, CA: Stanford University Press.

Office of the Privacy Commissioner of Canada. (2012). *Surveillance technologies and children: Report prepared by the research group of the OPC*. Gatineau, QC: Author. Retrieved from https://www.priv.gc.ca/information/researchrecherche/2012/opc_201210_e.asp

Priest, D., & Arkin, W. M. (2012). *Top secret America: The rise of the new American security state* (Also a Washington Post investigation). New York, NY: Back Bay Books. Retrieved from http://projects.washingtonpost.com/top-secret-america/

Regan, P. M., Jesse, J., & Khwaja, E. T. (2016, March). *Big data in education: Developing policy for ethical implementation in the US and Canada*. Paper prepared for presentation at the American Society for Public Administration Annual Conference, Seattle, WA.

Regan, P. M., & Steeves, V. (2010). *Kids r us: Online social networking and the potential for empowerment*. *Surveillance & Society, 8*, 151–165.
Sengupta, S. (2013, October 28). Warily, schools watch students on the internet. *The New York Times*. Retrieved from http://www.nytimes.com/2013/10/29/technology/some-schools-extend-surveillance-of-students-beyond-campus.html

Shade, L. R. (2011). Surveilling the girl via the third and networked screen. In M. C. Kearney (Ed.), *Mediated girlhoods: New explorations of girls’ media cultures* (pp. 261–275). New York, NY: Peter Lang Publishing.

Shade, L. R. (2015). I want my Internet! Young women on the politics of usage-based billing. In J. Bailey & V. Steeves (Eds.), *eGirls, eCitizens* (pp. 411–434). Ottawa, Ontario, Canada: University of Ottawa Press.

Shade, L. R., & Shepherd, T. (2013). Youth and mobile privacy: Applying a model of digital policy literacy. *First Monday, 18*(12). Retrieved from http://firstmonday.org/ojs/index.php/fm/article/view/4807/3798

Simon, S. (2015, March 21). Cyber snoops track students’ identity. *Politico*. Retrieved from http://www.politico.com/story/2015/03/cyber-snoops-track-students-116276

State of California, Assembly Bill 1584, Pupil Records: Privacy: 3rd-Party Contracts: Digital Storage Services and Digital Educational Software. Chapter 800: An Act to Add Section 49073.1 to the Education Code, Relating to Pupil Records, Approved by Governor September 29, 2014. Retrieved from https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140AB1442

State of California, Assembly Bill 1177, Student Online Personal Information Protection Act, Chapter 839, An Act to Add Section 49073.6 to the Education Code, Relating to Pupil Records, Approved by Governor September 29, 2014. Retrieved from http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140AB1177

Stevees, V. (2014a). *Young Canadians in a wired world, phase III: Life online*. Ottawa, Ontario, Canada: MediaSmarts. Retrieved from http://mediasmarts.ca/ycww/life-online

Stevees, V. (2014b). *Young Canadians in a wired world, phase III: Online privacy, (online publicity)*. Ottawa, Ontario, Canada: MediaSmarts. Retrieved from http://mediasmarts.ca/ycww/online-privacy-online-publicity

Stephens, C. (2014, September 14). Huntsville schools say call from NSA led to monitoring students online. *al.com*. Retrieved from http://www.al.com/news/index.ssf/2014/09/after_warning_from_nsa_huntsvi.html

Strauss, V. (2014, March 6). Why a “student privacy bill of rights” is desperately needed. *The Washington Post*. Retrieved from https://www.washingtonpost.com/news/answer-sheet/wp/2014/03/06/why-a-student-privacy-bill-of-rights-is-desperately-needed/

Thamel, P. (2012, March 30). Tracking Twitter, raising red flags. *The New York Times*. Retrieved from http://www.nytimes.com/2012/03/31/sports/universities-track-athletes-online-raising-legal-concerns.html?_r=0

US Department of Education. (2007, October). *Parents’ guide to the Family Educational Rights and Privacy Act: Rights regarding children’s education records*. Retrieved from http://www2.ed.gov/policy/gen/guid/fpco/brochures/parents.html

Vaas, L. (2015, July 31). How one school district is monitoring social media of students and teachers. *Naked Security*. Retrieved from https://nakedsecurity.sophos.com/2015/07/31/how-one-school-district-is-monitoring-social-media-of-students-and-teachers/

Vickery, J. R. (2014). Talk whenever, wherever: How the US mobile phone industry commodifies talk, genders youth mobile practices, and domesticates surveillance. *Journal of Children and Media, 8*, 387–403.

Vickery, J. R. (2015). “I don’t have anything to hide, but . . . ”: The challenges and negotiations of social and mobile media privacy for non-dominant youth. *Information, Communication & Society, 18*, 281–294.

Werbin, K. (2014). Social media, commodification, and surveillance. In L. R. Shade (Ed.), *Mediascapes: New patterns in Canadian communication* (4th ed., pp. 258–277). Toronto, Ontario, Canada: Nelson Education.

Zimmer, M. (2010). “But the data is already public”: On the ethics of research in Facebook. *Ethics and Information Technology, 12*, 313–325.

Zuboff, S. (2015). Big other: Surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology, 30*, 75–89.

Zwitter, A. (2014, July-December). *Big data ethics*. *Ethics and Information Technology, 17*, 387–403.

Zwitter, A. (2015, July 31). How one school district is monitoring social media of students and teachers. *Naked Security*. Retrieved from https://nakedsecurity.sophos.com/2015/07/31/how-one-school-district-is-monitoring-social-media-of-students-and-teachers/

Zwitter, A. (2014, July-December). *Big data ethics*. *Big Data & Society, 1–6*. doi:10.1177/2053951714559253

**Author Biographies**

Leslie Regan Shade (PhD, McGill University) is a Professor at the University of Toronto’s Faculty of Information. Her research interests include the social and policy aspects of social media, with particular attention to gender, youth, and political economy.

Rianka Singh (MA, McMaster University) is a PhD student at the University of Toronto’s Faculty of Information. Her research interests include gender and digital activism.