The Future of Privacy

Valerie Steeves*

On one hand, the future of privacy looks a bit bleak. Big data enthusiasts claim that, once we wire the social world, digital sensors will be able to collect the minutiae of everyday life—from our body temperatures to our test scores to how long we leave our lights on in the evening, to the location of our cars, phones, gloves, spouses and children—and digital assistants will be able to prejudge our needs and preferences based on the patterns in our data. We will also, so the story goes, be able to make better policy decisions, provide cheaper and better education, and identify cures for ailments and diseases that have plagued us for centuries. Even the need for our active consent will recede into the background, as smart houses, office buildings, streets and landscapes begin to passively monitor us for our own good.

As a social scientist, I am also fascinated by the promises of data. But I firmly believe that the complexities of human social interactions cannot be engineered so neatly precisely because people will reintroduce privacy into the social environment in ways that will muddy the big data waters. So the future of privacy is at least a transgressive future, because privacy will continue to challenge corporate and government information infrastructures that seek to colonise the social world for their own purposes.

Take social media, for example. Big data rhetoric assumes that digital sensors can measure human identity and interaction; just as algorithms reduce health to heart rates, weights and blood sugar measurements, social connection (that rich web of family, friends and neighbours that surrounds us all) is reduced to the number of ‘friends’, ‘followers’, and ‘likes’ that we acquire through digital communications. The resulting ‘social graph’ is alleged to provide us with a snapshot of the empirical world that will enable us to more efficiently deliver advertising, health care, education, policing, you name it.

To test this, I recently conducted a qualitative study with Canadian teens between the ages of 13 and 16 about the privacy of the photos they post on social media.¹ Not surprisingly, our research participants’ understanding of privacy had very little to do with non-disclosure. Instead, they sought to protect the privacy of what they disclosed through a complex set of norms designed to give them some control over their audiences.² This is consistent with a stream of research that started with the early advent of the Web that—in spite of every claim about ‘digital natives’ and the death of priva-

DOI: 10.21552/edpl/2017/4/5

* Valerie Steeves, Full Professor in the Department of Criminology at the University of Ottawa, Canada. Her research focuses on the impact of new technologies on human rights. For correspondence: vstevees@uottawa.ca.

¹ Matthew Johnson et al, To Share or Not to Share: How Teens Make Privacy Decisions about Photos on Social Media (MediaSmarts, 2017).

² Valerie Steeves, ‘Privacy, Sociality and the Failure of Regulation: Lessons Learned from Young Canadians’ Online Experiences’ in Beate Roessler and Dorota Mokrosinska (eds), Social Dimensions of Privacy: Interdisciplinary Perspectives. (Cambridge University Press 2013).
cy— has consistently and clearly indicated that young people care about their privacy and take active steps to protect it in online spaces.³

However, what was surprising was the extent to which they protected their privacy by hiding their actual preferences and interests behind a social media ‘personality’ that often had very little to do with them. Rather than voluntarily providing a window into their actual relationships, they posed content that ‘everyone’ would ‘like’. For example, one girl’s Instagram account was covered with pictures of horses, not because she liked horses—she had no particular leaning one way or the other—but because horses ‘make a good Instagram theme’. A boy explained that he would not post any content about baseball even though he was a huge baseball fan because that would be ‘random’ and his ‘followers’ might not find it ‘post worthy’. Another girl went to great lengths to keep any mention of anime off her social media accounts, because that was a ‘personal’ interest. In like vein, our participants took great pains to shield family members, especially younger siblings, from exposure on social media. As one girl summarised:

…family isn’t something that you throw outside there for the whole world to see. It’s kind of something that stays personally to you. … when I have family photos I feel scared of posting them because I care about my family and I don’t want them to feel envied by other people … I really like my family. I really like my brother. I don’t want anyone making fun of my brother.

If the world of the future is structured by surveillance, then privacy will continue to be relevant because it is the social mechanism that enables us to negotiate the boundary between ourselves and others to protect our intimate sphere. The more uncomfortable that boundary becomes, the more we will withdraw behind that boundary, and the fantasy of accurately mapping the social world will recede. To data protection enthusiasts, it will be no surprise that true disclosure in the future will continue to be predicated upon consent, trust, transparency and reciprocity.

But in the best of futures, privacy will not be transgressive, it will be constitutive. Especially because algorithms can unintentionally reproduce discrimination, privacy will be an essential corrective if we are to build a future that enables all of us to participate equally in networked society. Think of the short life of Microsoft’s Tay: within 24 hours, the bot ‘learned’ antisemitism and misogyny from the data stream.⁴ We saw the same potential for discrimination when the Chicago Police used algorithms to identify potential criminals and followed up by placing young, black men with no criminal record under surveillance.⁵

---


If we have learned anything from these examples, it is that numbers, proxies and computations are not neutral and correlations in data streams are not the equivalent of knowledge. Privacy will continue to help us re-learn these lessons as we experiment with artificial intelligence and machine learning in the future, because privacy is not about data, it is about people. It is directly tied to our sense of identity and dignity, and it is the umbrella that enables us to enjoy our other human rights. Privacy is by definition a commitment to the human over the technical. That is why placing privacy at the foundation of the socio-technical systems we create over the next few decades is our surest hope of building a future where people can thrive.