OPEN

6
Privacy and Surveillance

Abstract: *In addition to our intended self-representations, our digital traces are being gathered by entities far beyond our control: government agencies, commercial companies, data brokers and possibly criminals. We have little or no access to these representations of us, although the data that shapes them comes from us. Foucault's idea of the panopticon is frequently mentioned in discussions of surveillance, but the practices of surveillance are changing yet again. Employers and insurers are just starting to ask us to willingly agree to constant surveillance of certain aspects of our life: our driving or our health, and in return we are promised discounts if we prove ourselves worthy. How can we create a balance between using our machines to see ourselves and being forced to be seen by machines?*

Rettberg, Jill Walker. *Seeing Ourselves Through Technology: How We Use Selfies, Blogs and Wearable Devices to See and Shape Ourselves.* Basingstoke: Palgrave Macmillan, 2014. DOI: 10.1057/9781137476661.0008.

Most of this book has been about how we as individuals create self-representations of ourselves for our own use and to share with each other, but each of us is also represented by other entities in ways that we cannot fully access. Governments collect data about us, as do many different commercial companies. Data brokers combine information about each of us and sell profiles of us to other companies. Commercial websites like Facebook or Amazon generate representations of me based on my data. We live in a time that is teaching each of us that constantly being monitored is normal and even to our benefit.

In this final chapter I write about the times that photos of us are coerced and used as disciplinary tools. I write about data brokers and how commercial companies are gathering our data and creating their own self-representations of us that we are not allowed to see. Finally, I write about the ways surveillance and tracking are used as tools for power, showing how Foucault's concept of the panopticon is changing as we today often knowingly allow ourselves to be watched.

Forced portraits

One of the most frequent reasons given for enjoying taking selfies is that it allows the subject full control over the photographic process, from deciding to take a photo, to choosing the angle and expression, to editing the image to choosing which photos to share with others. As Susan Sontag (1973) noted, 'photography is power' (8). Sontag writes, 'To photograph is to appropriate the thing photographed. It means putting oneself into a certain relation to the world that feels like knowledge – and, therefore, like power' (3). A few pages later she states, 'There is an aggression implicit in every use of the camera' (6).

Photos are regularly used against the subject's will as a form of discipline: police mugshots, the compulsory photographs non-US citizens undergo when entering the United States, driver's license photographs and photographs taken by the police during riots. Personal photographs can also be co-opted by authorities, for example, in an immigration process when an immigrant may have to prove that a marriage or relationship is authentic by providing personal photographs of the couple together over a period of time. Failing to have the expected photographs means that you are seen as suspicious. Photographs are not only used as weapons or disciplinary tools by authorities, but can also become weap-

DOI: 10.1057/9781137476661.0008

ons that can be turned against authorities or against a peer. A bystander's video of police brutality or a soldier's photo of a man being tortured can lead to widespread condemnation of police actions or of military interrogation practices. A nude photograph taken consensually during a love affair may be used for revenge after a breakup or for blackmail if it falls into the wrong hands.

Governments have kept census records about populations for many centuries. Today's records are far more extensive.

Who the advertisers think I am

Your data is extremely valuable to companies that want to sell you things or to organisations that want to convince you to support their agenda. You can easily see some of the consequences of your data being tracked. For example, when I spent a lot of time reading about activity trackers as research for this book, I started seeing ads for activity trackers on many different sites, including Facebook. In addition to data gathered from your web surfing habits, sites such as Facebook and Google use the demographic information you explicitly give them and information they glean from your status updates, private messages and email to customise your news feed and the ads they show you. If you switch your status to 'Engaged,' you will immediately be shown ads for wedding dresses and caterers. If you are a woman over 40, you will see ads for wrinkle cream and botox. The recently married will see ads about pregnancy and baby products, whereas those who have been married for a year without posting anything about being pregnant will likely see ads for fertility aids.

Just tracking what you buy can tell marketers a lot about you, as we saw in the case reported in 2012 where Target sent a teenager ads for maternity clothes based on what she'd been buying (apparently pregnant women buy more vitamins and lotions in the first two trimesters than an average woman does), in practice announcing the girl's pregnancy to her family before she had told them about it (Hill 2012). Sociologist Janet Vertesi (2014) wrote about how she tried to keep her recent pregnancy completely hidden from data brokers. It was a lot more complicated than you might think. She not only had to never mention the pregnancy on social media, even in private messages (which are also tracked for marketing data), but also couldn't browse baby-related sites online or buy anything baby-related using a credit card. Avoiding being tracked and profiled by data brokers is

DOI: 10.1057/9781137476661.0008

not easy to do. In *Dragnet Nation*, Julia Angwin (2014) writes about how she tries to keep her data private, and she concludes that to not be tracked you have to have very sophisticated technical knowledge or have a lot of money. As Vertesi points out, many of the strategies you might legitimately use to stay private – such as using encryption or using cash instead of credit cards – are also likely to flag you as a potential criminal.

The Timeline that Facebook introduced in 2011 is an interesting narrativisation of our lives, but it is also a goldmine for harvesting our 'life events', from weddings and births to moving house or getting a new job – or even breaking a leg or having braces removed from our teeth. 'Life events' are valued by data brokers who gather data about us from multiple sources and sell it to marketers. If you can locate the exact people who will be most likely to buy your product, whether that is pregnant women or people who have just bought a new house, and you market directly to them, you are likely to sell more products.

You don't even have to be online to have your data tracked. Companies track your purchases using loyalty cards or simply taking note of the credit card you use to make a purchase. There are companies that drive around taking photos of every car they come across and its license plate, creating a gigantic database of the location of millions of cars. The data is primarily intended for repossession of cars whose owners have not paid their car loans, but can also be used for many other purposes (Angwin 2014, 27). If you have a digital thermostat or smoke detector made by Nest, a company purchased by Google in 2014, Google has access to continuous information about the temperature or CO2 levels in your home, which can for instance be used to track when people are present.

In Europe, privacy legislation limits the ways companies can use and connect personal data, and individuals have the right to see the data collected about them, but in the United States and many other countries commercial data collection is largely unregulated. The boundaries between government and commercial data collection are not always watertight. We know that the NSA gets data about us from commercial sites, and commercial data brokers add public data such as drivers license records or moving records to their data profiles of us. Some data we might think should be non-commercial, like data about children in public schools, is actually collected by private companies that run learning management systems, administer tests or provide educational software. Using this data can help children learn more easily. For instance, software will easily be able to track whether an individual child tends to

DOI: 10.1057/9781137476661.0008

persevere at a challenging task or whether he or she will give up quickly, and so the learning activities can be adjusted to that child's learning style. But the use of this data is unregulated in many parts of the world and could be sold to marketers and data brokers.

When today's six-year-olds finish high school, an astoundingly detailed representation of their lives at school will exist, and we don't yet know who will be able to access it. Depending on which country children live in, they may or may not have the right to see their own records. Information about their test scores, disciplinary issues, absences, tardiness, learning styles, health, home situation and personality from the time they were in preschool until they graduate may or may not be shared with marketers, insurance companies, potential employers, courts of law, the police and college admissions boards.

Dave Eggers imagines this data analysed in real time to produce continuously updated rankings of all students in the United States. Why stop at saying that a six year old is in such and such a percentile for reading? If Ivy League colleges admit 12,000 students a year, wouldn't parents love to know whether or not their child was in the top 12,000 students for their age? 'Once we get full participation from all schools and districts,' the representative from the ubiquitous social network service The Circle enthusiastically explains in Eggers's novel, 'we'll be able to keep daily rankings, with every test, every pop quiz incorporated instantly' (Eggers 2013, 341).

With current EU legislation, the individual has the right to see his or her own records, but not necessarily in a useful format. When I requested my information from my Norwegian cell phone provider they sent me 30 pages of printed times, dates, locations and phone numbers I had called over the previous three months. I assume it was printed rather than digital because it is far less useful to me on paper than in a format I could graph or analyse on a computer. Similarly, when I requested my hospital journals they were sent on paper, and I had to pay a fee for the photocopying. In the United States and many other countries individuals do not have the right to see data collected about them, although some companies will comply to some extent (Angwin 2014, 86–9).

Power and discipline

Foucault's theories of discipline are often referenced both in discussions of surveillance and of selfies and self-representations. In discussions of

DOI: 10.1057/9781137476661.0008

self-representation, theorists are interested in Foucault's ideas about 'technologies of the self,' which Foucault (1988) writes 'permit individuals to effect by their own means or with the help of others a certain number of operations on their own bodies and souls, thoughts, conduct, and way of being, so as to transform themselves in order to attain a certain state of happiness, purity, wisdom, perfection, or immortality' (18). In a study of NSFW (not safe for work) blogs where women and men shared erotic photos they had taken of themselves, Kathrin Tiidenberg (2014) invokes Foucault's self-cultivation, noting how an informant expressed that 'self-shooting gave her a way to care for herself and increase her self-awareness.' Through photographing herself, this woman developed a 'new gaze' that 'taught her to feel sexy in her body, but it also altered her material body-practices in terms of how she held herself, how she dressed and accessorized, whether she used make-up and how long she let her hair grow.' Or as Jodi Dean (2010) glosses Foucault's notion, 'Foucault's technologies of the self rely on the installation of a gaze, of the perspective of another before whom the subject imagines itself' (54).

Surveillance scholars on the other hand rarely fail to mention Foucault's theories of another aspect of power, a more direct gaze, or as Foucault (1988) writes: 'technologies of power, which determine the conduct of individuals and submit them to certain ends or domination, an objectivizing of the subject' (18).

Foucault wrote about Bentham's design for a wheel-shaped prison building where the gaolers would sit in the middle and be able to see each prisoner in his individual cell around the perimeter of the circle. The prisoners would not be able to see each other and would always know that they *might* be being watched. That knowledge would keep them disciplined, always behaving as the gaolers required.

> All that is needed, then, is to place a supervisor in a central tower and to shut up in each cell a madman, a patient, a condemned man, a worker or a schoolboy. By the effect of backlighting, one can observe from the tower, standing out precisely against the light, the small captive shadows in the cells of the periphery. They are like so many cages, so many small theatres, in which each actor is alone, perfectly individualized and constantly visible. The panoptic mechanism arranges spatial unities that make it possible to see constantly and to recognize immediately. In short, it reverses the principle of the dungeon; or rather of its three functions – to enclose, to deprive of light and to hide – it preserves only the first and eliminates the other two. Full lighting and the eye of a supervisor capture better than darkness, which ultimately protected. Visibility is a trap. (Foucault 1995, 200)

DOI: 10.1057/9781137476661.0008

This *panopticon* is also an image of our modern society, Foucault argued. Our government watches us, and in general, we don't commit crimes because we know we could be caught. It is important that we know that we might be watched at any time, but that we can never know for sure whether we are watched now. 'Power should be visible and unverifiable,' Foucault wrote, 'the inmate must never know whether he is being looked at at any one moment, but he must be sure that he may always be so' (201). George Orwell's novel *Nineteen Eighty-Four* (1949) describes this kind of intensely surveilled state perfectly.

In the decades since Foucault wrote about the panopticon, the nature of surveillance has changed greatly. We are watched to a far greater degree than when Foucault was alive, with surveillance cameras on every street corner and the NSA and many other entities able to access our emails or phone calls. It's not clear that today's surveillance functions in the regulatory way Foucault described, disciplining us to be well-behaved citizens. Surveillance has become complicated in the digital age. Even the word has been altered. Roger Clarke defined dataveillance (1988) as 'the systematic monitoring of people's actions or communications through the application of information technology'. Steve Mann and collaborators coined other variations. Sousveillance plays upon the French word *sous,* meaning 'under', in contrast to *sur* which means 'over', and it refers to ordinary citizens watching authorities, for instance using wearable cameras. Coveillance is peers watching each other (Mann, Nolan, and Wellman 2003).

In his book *The Googlization of Everything*, Siva Vaidhyanathan argues that we need a new term to describe today's surveillance, as it is fundamentally different from the panopticon Foucault described. Vaidhyanathan proposes the term *cryptopticon.* The most important thing about today's cryptopticon, Vaidhyanathan (2011) writes, is that 'we don't know all the ways in which we are being watched or profiled – we simply know that we are. And we don't regulate our behavior under the gaze of surveillance. Instead, we don't seem to care' (112). According to Vaidhyanathan, we don't know all the ways in which we are being watched, but we know that they are extensive, and that we are watched by many different entities: governments, corporations and criminals.

In the years after Vaidhyanathan coined the term cryptopticon we have debated the Snowden leaks and had ongoing discussions of how Facebook and other web services track us, and we actually know quite a lot more about how we are being watched. In many cases we know exactly

DOI: 10.1057/9781137476661.0008

how we are being watched. For instance, several companies are now offering discounts on health insurance to employees who agree to wear a Fitbit activity tracker (Olson and Tilley 2014, Olson 2014). Progressive, a US car insurance company, offers its customers a device they call the Snapshot that will track their driving for 30 days, and promise a discount to drivers the Snapshot device finds drive less than average, in safer ways and at safer times of the day (Huffman 2013; Progressive 2014). Wildflower Health is a company that offers a pregnancy tracker, Due Date Plus, that is marketed to insurance companies and large employers. Due Date Plus is already offered to all women in Wyoming who are covered by Medicaid, and it seems very similar to many other pregnancy tracking apps available, letting you track weight and other measurements. There are some added benefits for users such as access to calling a nurse at any time of the day or night, but most importantly for the health care provider, the app 'uses self-reported data to identify high-risk pregnancies and drive interventions' (DeGheest 2013). Maternity and newborn care are a major expense in health care, so if high-risk pregnancies can be caught early on, better care can be provided and a lot of money, and possibly lives, can be saved.

As Mae thinks in *The Circle*, 'what had always caused her anxiety, or stress, or worry, was not any one force, nothing independent and external – it wasn't danger to herself or the constant calamity of other people and their problems. It was internal: it was subjective, it was *not knowing*' (Eggers 2013, 194).

The fantasy of absolute self-knowledge through technology, backed up with the knowledge that the software will call in experts (doctors, nurses, hospitals) is very seductive. If my data shows me (and my insurer) that I am a safe driver, that I am doing a great job looking after my baby, or that I am walking 10,000 steps a day and doing my best to stay healthy, I will feel good about myself. If I can look at graphs showing that my weight gain during pregnancy is normal and that the baby is growing well I'll feel safe. I might feel differently if I wasn't able to keep up the 10,000 steps my employer required or if I started admitting to my pregnancy tracker that I wasn't getting enough sleep or was eating nothing but ice cream.

These apps are only the beginning. The technology is here, and we are just starting to find ways to use it. Remember the smart onesies and baby monitors I wrote about in the last chapter? Imagine if Wyoming Medicaid starts offering smart onesies to newborns that track breathing, sleep,

DOI: 10.1057/9781137476661.0008

heart rate, temperature, feeding and more. Imagine if you start getting visits from child services if your baby doesn't get enough sleep or there are other risk indicators. That might also save lives, but imagine parenting under constant government surveillance. These transactions – our data for a discount or for health care – will quite likely save lives, but it is very easy to see how they can be abused. And this technology is already here.

Seeing ourselves

When we willingly share data from an activity tracker, a safe driving monitor or a health app with our employer or insurer, we willingly trade our personal data in return for lower costs or better services. Sometimes we might appreciate being 'seen,' whether we feel that we are seen by the technology or by our health care providers or insurers. But, importantly, these apps allow us to see ourselves. As I discussed in chapter 5, studies have found that people develop 'affective ties' to the data they track (Oxlund 2012, 50; Ruckenstein 2014; Rooksby et al. 2014), just as our diaries, blogs, selfies and family photo albums are meaningful to us.

Apps which allow us to see our own data allow us to see ourselves. We look at our data doubles as we gazed into the mirror as teenagers wondering who we were and who we might be. We look at our data in much the same ways as you might flick through your selfies to find the one that shows you the way you want to be seen.

When Parmigianino painted his *Self-Portrait in a Convex Mirror* in 1524, he painted himself exactly as he saw himself, using the best technology available to him. His image is distorted due to the convex shape of the mirror he used. Our self-representations are always distorted in some way. The data doubles that are generated by our health trackers or productivity apps are not complete or even entirely accurate likenesses any more than Parmigianino's self-portrait was, although it may be harder for us to see how they are distorted.

Parmigianino's self-portrait hangs in an art gallery nearly half a millennium after he painted it. Millions of people must have seen his self-portrait or a photograph of it over the years. But unlike our contemporary self-representations, it was not analysed by data brokers, search engines, marketers and governments. The audience for our self-representations is no longer, as a few decades ago, ourselves and each other. Our audience today includes machines. The machines parse the

DOI: 10.1057/9781137476661.0008

data we provide, running selfies through facial recognition software, our status updates through sentiment analysis software, our health data through risk indication analyses, and send the results on to marketers, employers, insurers or governments. Machines helped us create those self-representations in the first place.

And yet, we continue to express ourselves. We are humans, after all. 'Photography is power,' Susan Sontag wrote (1973, 8). Selfies and other self-representations can be seen as a way of taking back this power, just as UPS drivers track their supervisors and protestors turn cameras on the police.

In practice, for now, we don't think too much about our machine audiences. We are too busy learning more about ourselves and each other by taking selfies, writing blogs, talking together on Facebook or Tumblr. We no longer need to rely on others to represent us. We represent ourselves.

DOI: 10.1057/9781137476661.0008