Part Two
Digital Culture
Surveillance technologies are everywhere. We are now almost constantly photographed, tracked, monitored, recorded, and stored. Often this surveillance is so insidious and surreptitious that we neither realize it is occurring nor attribute any harm to it. George Orwell would shudder at what we submit to. Google Glass and other commercial products with their always-on surveillance cinema potential just deepen this threat. Always shifting between the two rhetorical poles of security and safety, this tracking happens everywhere, in spaces both real and virtual. Surveillance artist Peter J. Cornwell says, “The involuntary traces . . . we leave everywhere on the Internet are . . . more difficult to recognize” than those in the real world, “and almost impossible to recall.”

Many Internet sites that we visit, especially those of technology companies, secretly interrogate our computers: analyzing our habits, reporting the serial numbers of products that we have loaded, and leaving information for later exploitation. One’s information fingerprint is now a persistent and monotonically expanding trace, distributed among countless computers across the globe and in space and independent of any specific surveillance agenda (Cornwell, 2002: 597).

Who knows what about us is impossible to determine. Who they might share it with or how long they might keep it is untraceable. As the potential for the
integration of automated, networked, intelligent technologies that span multiple systems increases, a rhetoric of safety feeds these ever-greater encroachments on our rights to privacy (Cornwell, 2002: 597). There is a revolution coming in information privacy, and ubiquitous intelligent cameras mark the end of privacy as we have known it. Witness, for instance, the Mood Meter created by the MIT Media Lab in 2012. Using real-time facial recognition software to create live displays of how the inhabitants of a room or a building are feeling, Fast Company Design Magazine likens it to how we catch a vibe about a gathering, or how we read the emotional temperature of a room. Javier Hernandez Rivera and M. Ehsan Hoque log smiles with their camera and software. That information is then live-fed back into the room with emoticons in the place of their faces. Dubbed a “mood barometer,” the purpose of this interaction is to gauge whether, in fact, happiness—or at least a smile—is contagious. The software is very effective at prodding people who are unhappy or in a neutral mood to act happier. Simply acting happy is infectious. As many studies have proved, pretending to be happy, or smiling when you are not, does have a real impact on your actual mood. This interactive installation software seeks feedback from participants, unlike many of the new dataveillance techniques: the systematic monitoring of a person’s finances, communications, and digital interactions ask for no feedback, and in fact are nearly invisible to their subjects.

Prior to former NSA contractor Edward Snowden’s whistle-blowing revelations about the activities of the U.S. National Security Agency, we did not know whether or when we were being tracked, or how long the info would be stored, or with whom it might be shared. In a post-Snowden era, we now know that American telephone companies routinely hand metadata over to government offices and that user-friendly digital surveillance systems such as Prism and XKeystroke (XKS) snare vast amounts of unencrypted data. Increasingly smart technologies, especially photographic ones, sift, store, and analyze our data, keeping it (in theory at least) in perpetuity. Viruses hijack our browsers, capturing our search data and preferences. From overt CCTV filming to the seemingly innocuous tracking of our grocery store or online purchases, to the extraction of data from our Web surfing, to the monitoring of Facebook photos, we are rich veins of data to be mined by the networked systems from many different sources. These techniques make the Stasi, the relentless police of the German Democratic Republic’s Ministry for State Security, look like amateurs. The GDR employed a fleet of officers and informants—more than half a million at its peak—and 10,000 of those were employed solely in the business of monitoring
and transcribing conversations (Levin, 2002: 579). Primarily employing auditory technologies, the Stasi’s methods predate the digital information explosion of personal computers and were in decline in the 1980s up until they were disbanded after the fall of the Berlin Wall. Now we have moved into a post-panoptic system, into the realm of automated dataveillance.

ECHELON is the industrialized West’s answer to the Stasi. It is the surveillance system of the U.S. and the U.K., Canada, Australia, and New Zealand. It was formed in 1947 in a secret agreement between the United States and Britain. Later, other countries, including Denmark, Norway, Germany, and Turkey, became “third party” participants. ECHELON’s existence only became public knowledge in 1988 when it essentially moved to a 2.0 phase with all-new mainframes. It is a system that tags key words and “sniffs” all data traffic between civilians and the military, routinely tagging any of its so-called dictionary terms, names, and phrases (Levin, 2002: 579). Something that enabled greater access for ECHELON systems was the conversion of the ISDN (short for the Integrated Services Digital Network protocol) to an all-digital global format in the 1990s. This change was fueled by the arrival of the World Wide Web, and these upgrades in turn transformed the dial-up market and made high-speed Internet access possible. The ISDN protocol, established by the United Nations, ensures that global telecommunications systems can handshake. This system is why it is possible to make a phone call to India or Nigeria, for instance, despite radically different phone companies and systems. ISDN systems are now on the wane, and soon to be eclipsed by broadband. What is unique about ISDN systems, though, is what has enabled the NSA’s vast spy network—they provide easy access for dataveillance: “ISDN protocol are not only optimized to deliver data to ECHELON like sniffer systems, but also allow one to take any phone ‘off the hook’ without it ringing in order to listen in to any domestic or office space” (Levin, 2002: 580).

It is known that these ECHELON-like systems had astronomical capacities for storing data back in the 1990s; we can only speculate as to how much of our personal data they hold now. The Guardian reports, “In 2012, there were at least 41 billion total records collected and stored in XKeyscore for a single 30-day period” (Greenwald, 2013).

In the two decades since, other technologies have come thick and fast. The Danish stroboscopic camera, Jai, was released in 2011. It is said to be able to detect any conversation behind a closed window within visual range, which is about a kilometer away. A laser version by PK Electronick can take hundreds of pictures in a matter of seconds and individually photograph all the participants
in a crowd (Levin, 2002: 579). The Q-Tel molecular scans that are being released in 2013 for airport security are even scarier: “the machine can sniff out a lot more than just explosives, chemicals and bioweapons” (NAC, 2012). The manufacturer, Genia Phototonics, says it can “penetrate clothing and many other organic materials and offers spectroscopic information especially for materials that impact safety such as explosives and pharmacological substances” (NAC, 2012). In other words, it will know what you had for breakfast and what molecular tags you have, such as whether you are predisposed for a particular type of cancer. It is small, portable, and can be operated anywhere within fifty meters of subjects without anyone ever knowing (NAC, 2012). It gives governments the means to sample populations, record their molecular data, and move “well beyond eavesdropping” (NAC, 2012).

Within consumer culture, data is gold too. Self-surveillance—the act of submitting your own data to corporate interests such as Amazon, TiVo, or Facebook—becomes a revolutionary gesture of participation (Andrejevic, 2007: 15) . . . or so corporations would have us believe. With the advent of social media, we now log our own data in the service of multinationals as we seemingly embrace the arrival of a technological Big Brother as participatory surveillors (Batchler, 2012: 92–99; Turner, 2012: 8). A number of digital media artists and groups, however, have turned the tables—or, more exactly, the camera—on themselves by using digital media and self-surveillance as a means of writing their own digital narratives outside of the parameters of social media control. Exploring the ubiquitous potential of surveillance technologies as a medium of self-expression, guerrilla methods by artists are producing site-specific works that use these tactics to repossess all-seeing cameras for aesthetic ends. Social activists also use the potentialities of self-surveillance to reveal and to disguise, to network and to disconnect as a way of both communicating and avoiding detection.

The Occupy Movement uses a blend of social media, self-surveillance, and both official and unofficial media footage to keep their politics in the public consciousness, while also keeping themselves out of the public eye. To succeed, the Occupy Movement must be present and situated, but anonymous and dynamic. Embracing the philosophy that the revolution will not be televised (because once it is, it is subsumed within what Guy Debord called the “Society of the Spectacle”), #OCCUPY offers new nonvisual data-based strategies for networked organizing, collaborative creation, and collective aesthetic acts. Leading thinkers in the situationist movement, Guy Debord (in The Society of
the Spectacle) and Raoul Vaneigem (in The Revolution of Everyday Life) advocated against the transactional nature of capitalism in favour of living every moment consciously as a way of constantly reinventing life, reality, and society. Through transforming one’s self, they argued, one altered one’s relation to power structures and to the world. Using rhetorical strategies (including the dérive, détournement, and psychogeographic exploration) as an anti-aesthetic that has been very influential to the #OCCUPY Movement, the situationists called for local acts to replace both mediated spectacle and highbrow art in order to create “a new genre of creation” (Situationists International Texts). #OCCUPY is certainly a genre of that ilk. Self-surveillance rethinks aesthetic approaches to creative practice in provocative ways.

Participation in public space has the potential to challenge the installed public cameras and formal systems of control precisely by using the politics of location to speak against official discourses. Returning collective action and public narrative to town squares, these groups and artists are reinventing narrative for a digital culture generation. The spontaneous uprising of collective, multilinear narratives in global public space has rendered the Square the new center of participatory art, and these actions are a roadmap to where future technologies might take us.

Guerrilla use of public technologies is one version of what German artist Joseph Beuys called social sculpture. Beuys defined social sculpture as a cultural reflection on and an active intervention into a community or environment for the purpose of creating a space for unexpected interactions and situational participation. Social sculpture, by design, explores the relationship between aesthetics, social processes, and ecosystems through performance, environmentalism, and political engagement. In the early days of the Web, when networked computer technology was still fairly primitive by our current standards, Mexican-American performance artist Guillermo Gomez-Peña and collaborator Roberto Sifuentes launched a high-tech event called “Naftaztec: Pirate Cyber-TV for AD 2000.” As Latinos, he and Sifuentes had been stung by the libertarian rhetoric that maintained cyberspace was a politically neutral space of equal access, a space allegedly free from the barriers of race, gender, and class. For Gomez-Peña, this was a cop-out that denied the crises of social and racial inequality that engulfed and continues to engulf the United States (Gomez-Peña, 2000: 295–308).

The pair actively played with the stereotypes of Mexicans as techno-illiterates and illegal aliens, and hijacked cable television in 1994. These Pirates, critiquing American culture, interrupted evening news broadcasting in 3.5 million American
homes. This was not a hack. It was an experimental satellite broadcast in multilingual television; they purchased the airtime and transmitted this alleged pirate intervention to hundreds of community cable outlets. In total they were on air for ninety minutes. They were promoting an altered view of reality. Part of the broadcast included The Chicano Virtual Reality Machine, which could videotape personal and collective memories, and a Virtual Reality Bandanna, which would allow Americans “to experience first hand the psychological sensation of racism” (Gomez-Peña, 2000: 39). They renamed the Internet the Chicano Interneta and surfers were allowed to post written and visual comments at their website. The broadcast won the prize as best experimental video at the San Antonio Cine Festival in 1994.

Another performance troupe that seized the eyes of the law to repurpose these official cameras for their own ends was the Surveillance Camera Players. From 1996 until 2006, the Players set out to remake what they called the “tools of social control,” that are used both to enslave them within consumer culture and police them against shoplifting, stealing from employers, sabotaging, or vandalizing goods or property that belong to others. Making explicit the connection between the eye of the lens and the hand of the law through their pro-privacy acts, the Surveillance Camera Players set out to make use of these cameras that they claimed had lowered crime rates so profoundly that, they said, they left security guards without anything to watch. Seen as a kind of programming, the troupe used the surveillance cameras as an audience of their own productions, which could happen at a surprise location at the same time (Tuesdays at 8:30, for instance) as a sort of regular guerrilla programming with performances that started out as one-time productions of plays, like the staging of a silent version of Waiting for Godot. Some cameras they used were monitored live and others recorded to tape, so productions were tailored specifically to the venue. They say, as guerrillas, we must ensure that we do not relish the camera. Surveillance is not passive and it is not our friend. We must not mistake the subversive possibilities offered by the abundance of equipment meant to curtail, monitor, and control our desires with a neat new device provided for us by the spectacle. We don’t need this garbage to have a good time, any more than we need TV, but if the enemy is going to clutter our landscape with watchful eyes, we should look into those eyes and let them know how silly we think they are. Guerrilla programming is production of an action, not consumption of a product. It may be that the surveillance camera can give us a focus point on the street.
Fast-forward to the days of the Occupy Movement, and the notion of entertaining, amusing, and morally edifying “the surveilling members of the law enforcement community” no longer seems so amusing (Surveillance Camera Players). One group, the Institute for Applied Autonomy, has created an app that repurposes the data collected by the Surveillance Camera Players. The troupe had produced a map of all of the CCTV locations in public space in New York City. The Institute took this data and created a “path of least surveillance” (Institute for Applied Autonomy): a web-based app called iSee that helps individuals plan a route that avoids detection. Events in Tiananmen Square had demonstrated in a gruesomely dramatic fashion how easily the ubiquitous surveillance camera could be repurposed by hostile police and army should the occasion arise. In the wake of the September 11th attacks on New York, the Institute wanted to be sure that protesters were safe. By clicking on the iSee “map, a user indicates points of origin and destination” (Institute for Applied Autonomy) and can then safely navigate through un surveilled urban space.

When interactive media artist Hasan M. Elahi’s name was mistakenly added to the watch list by the CIA, he turned the camera on himself to practice protective self-surveillance in Tracking Transience: The Orwell Project. A case of mistaken identity for the Bangladeshi-American artist led to six months of interrogation and investigation. It was ultimately Elahi’s use of social media that saved him from a stint in Guantanamo because he was able to call up Google calendar and demonstrate that he could not have done what he was being accused of. As a response to those months of trauma, Elahi preempted any further incidents by wiring himself with a GPS and relentlessly documenting his own movements, his meals, and his activities. This means that he is always trackable in real time by the FBI or anyone else. His website documents all of these activities, often to the tune of more than 100 photos per day. Others, too, practice this kind of art, as lifecamming and live blogging become more and more popular for twenty-first century Proustians.

According to digital media theorist Christiane Paul, streamed experience is the closest thing to live experience in our mediated age (Paul, 2008: 18). Live experience in a mediated age is elusive. Capture or streaming is becoming the default
mode for life-like experiences. Capture can be simple, like Noah Kalina Everyday (see Kalina). This was a six-year experiment in which the artist photographed himself every day and then compressed these images into a time-lapsed film that he posted on YouTube. Or capture can be complex. Witness Manu Luksch’s fifty-five-minute feature film *Faceless* (Luksch, 2007), for instance, which stars Tilda Swinton and was created through capture with CCTV cameras over many months.

Using the British Data Protection Act of 1998 and other privacy legislation to reclaim data records and surveillance footage for her own ends, Luksch gains access to her publicly viewed data and images. The use of CCTV is strictly controlled in some countries, such as Denmark and Germany. In the U.K., however, they are extremely densely deployed. Penning a “Manifesto for CCTV Filmmakers,” Luksch declares a set of rules, establishes effective procedures, and identifies further issues for filmmakers using pre-existing CCTV (surveillance) systems as a medium in the U.K. The filmmaker’s standard equipment is thus redundant; indeed, its use is prohibited. The manifesto, according to Luksch, can easily be adapted for different jurisdictions (Luksch, 2006).

Calling her works ambientTV, Luksch advocates not introducing any new cameras or lighting into the scenes. The data subject (or protagonist) must be featured in all key scenes, with the documented activity counting as sensitive or personal data. In addition, all third parties must be rendered unidentifiable; since surveillance cameras don’t record sound, filmmakers must determine their own parameters for sounds; and finally, since the footage is subject to such complex copyright and privacy issues, any filmmaker should employ a lawyer before trying to show their finished work (Luksch, 2006).

*Faceless* explores a futuristic era of calendar reform in which the past and the future have been eliminated from people’s lives. We could call Luksch’s approach Postcinematic Surveillance—a whole new genre. Following the protocol of her own “Manifesto,” Luksch uses these captured images, which anyone can request of themselves, to construct a surreal, choreographed world where everyone’s face is obliterated (as required by the privacy law). Luksch posits the guerrilla filmmaker as a viral agent and a “symbiont.” She says that the most prolific documentarists are no longer to be found in film schools and TV stations. In some European and American cities, every streetcorner is under constant surveillance using recording closed-circuit TV (CCTV) cameras. Such cameras are typically operated by local government, police, private security firms, large corporations and small businesses, and private individuals, and may be automatic or controlled (zoomed and panned) from a remote control room. Filmmakers,
and in particular documentarists of all flavours, should reflect on this constant gaze, she says. Why bring in additional cameras, when much private and public urban space is already covered from numerous angles? (Luksch, 2006). In the act of hijacking these technologies, lighting and cameras become not just unnecessary but forbidden. The hack is complete once Big Brother’s eye is used for aesthetic effect.

Media theorist Marshall McLuhan said, “technologies begin to perform the function of art in making us aware of the psychic and social consequences of technology” (McLuhan, 1964: 14). These artistic endeavors invert internalized psychic and social events to make them visible as art. As our technology more and more stands as an interface and a boundary object between us and a world where everything is mediated, these surveillance art efforts have been, until now, largely hardware-driven. With the rise of the smart phone and mobile technologies, self-surveillance, participation, and public space are transformed.

We live in dangerous times. Merely by placing a phone call to the phone company, police departments can “clone” a mobile and download text messages even while it is turned off (Lichtblau, 2012). This is not legal in the U.S., but, regardless, phone companies comply in the interest of public safety. During the Arab Spring many protesters and activists worked with “media-savvy video journalists” to devise new methods of organizing outside of the all-seeing eye of the police, while the latter, in turn, would use similar methods to monitor communication. These journalists are “dubbed vee-jays” and they implement a variety of “dissemination strategies”: “Photos and videos are shared across multiple platforms, alongside additional text, context, or transcripts, and often have metadata such as time, date, and location stamps” (Ulbricht, 2012). Content is uploaded live or at regular intervals through an assortment of social media sites and livestream portals, including Bambuser, by satellite connection. When Internet or cellular access gets shut down or disrupted, “footage is collected and distributed via agile alternatives such as runners—[known as] the old-fashioned ‘sneaker net’” (Ulbricht, 2012).

During the student protests in London in January 2011, police started corralling students who had taken to the streets. The police used a tactic called “kettling,” which traps protesters between their frontline and a cordoned-off area. Protesters are then either herded by police out of the area or are trapped within the enclosure. In many instances, the protesters are then denied access to food, water, and bathroom facilities for long periods of time. In response to this, a group of students and volunteers banded together to create Sukey. This is an

Carolyn Guertin 117

10.15215/aupress/9781771991292.01
app designed to inform protesters of police movements, giving the users directions to avoid being trapped within a cordon. The info travels in real time via any social media platform to and from mobile phones. The source is people monitoring the news and other protesters and observers in the area. “Since many people rely on the authenticity of this information, identification of sources is crucial” (Malevé, 2012: 15).

Sukey searches for messages on Facebook, Twitter, Tumblr, and other social networks using the hashtag #Sukey. The results are then filtered using what one of the programmers calls “a kind of algorithmic reputation management.” The use of Sukey has proved very useful for “escap[ing] kettling. But it has also raised many questions regarding [its reliance] on external platforms to establish the reliability and trustworthiness of its sources, in a context where trust is essential” (Malevé, 2012, 15–16).

Sukey taps into the power of social networks “to aggregate and spread information and map out relationships, and used this power to distribute strategic information to protesters. But in doing so, it also fed the data hungry machines of social networks with sensitive information about protesters and their circles of friends” (Malevé, 2012: 15–16). In other words, using Sukey could just as easily trap you as save you. It is designed to work in real space, but it makes apparent how easy it will be for the police to start using digital cordons (Malevé, 2012: 16). And it is equally clear that it is just a matter of time before they will. Social media service providers have been no friends to protesters under NSA and other regulations, and they have the right “to not only ‘contribute to prevent’ but also to ‘terminate’ infringements” of usage (Malevé, 2012: 17). We already have seen how easily the dotcom boom wiped out independent providers and “put large, well financed, corporations back in the driving seat” with Web 2.0 (Malevé, 2012: 17–18). While we do the work of social media, “the mission of 2.0,” Nicolas Malevé says, “is to destroy the P2P aspect of the Internet: To make you, your computer, and your Internet connection dependent on connecting to a centralized service that controls your ability to communicate” (Malevé, 2012: 18).

Because social media users inevitably use the large providers like Facebook and Twitter, the providers make deals and move further and further from net neutrality. “The infrastructure built for surveillance can thus be recycled in order to develop a commercial model of bandwidth discrimination” (Malevé, 2012: 19). The Occupy Movement and other protesters have created some alternatives that enable you to once again control, monitor, and even alter your social data and location. Open Street Map project (osm) is one such option. It deals more
intelligently with user data and demonstrates how a community designs, maintains, and interprets its own data within a unique framework. OSM is essentially “a Wikipedia for maps,” but it reinvents Web 2.0 in some specific ways: it is open about data, metadata, and logged behaviour: rather than merely using the data, users are encouraged to think critically about it (Malevé, 2012: 21). You can also decide what to do with your own logs once you have used them—archive, edit, or delete them?—because it gives you the ability to modify your data. Users formalize their participation through OSM, in order to safeguard the fundamental motives behind their participation and to ensure that no uninvited eyeballs are watching their movements.

Cell phone providers are another weak link in the communication chain and render the DIY cell phones impractical for leading the protest charge; Occupy here is a better system. An open-source local area network or personal Internet, it establishes “a peer-to-peer network of virtual spaces (autonomous from the Internet) for open political discussions. Anyone within range of an Occupy here WiFi router with a web-capable smartphone or laptop can join the network ‘OCCUPY.HERE,’ load the locally hosted website http://occupy.here/ and use the message board to connect with other users nearby.” Another app, Serval Rhizome Retriever, “allows news, information, software updates, files, maps etc to be disseminated without any supporting Internet access”; similarly Geolocation, enables geolocation-based chatrooms for protesters on the move because “public” is a space and a group constantly subject to renegotiation.

The camera and camera-enabled technologies have been a major source of resistance and information dissemination for the Occupy Movement. Cop Recorder masks your location and Vibe inhibits access to your location. Cop Recorder is “a network-enabled authority recorder” (occupy-here) that allows for secret audio recording when you have an encounter with an enforcer. It then facilitates an easy anonymous upload to its own OpenWatch.net server. Vibe is a major social media innovation in the #occupywallstreet protest (Nouveau 2011). A microblogging software similar to Twitter, it is anonymous, temporal, and location-based. Created by Hazem Sayed, the Vibe app is revolutionary because it creates a temporal tether for the dissemination of a message. Time frames can be as short as fifteen minutes or as long as thirty days. Similarly, the distance of transmission can be as small as 160 feet and as expansive as the whole world. As a protest tool, it enables mobility. It fosters a fluid ability to hide, dodge, and circumvent real-time police monitoring of social media networks. It is also local, and at its best targets a particular need in a particular place at a particular time.
The first massive decentralized social network in the history of the Internet is called TheGlobalSquare (Roos, 2011). Designed as a tool against censorship and oppression, it works on the Libertarian premise that information should be free. Repurposing peer-to-peer approaches, the creator, fNf, and others “are revisiting older tech such as HAM or CB radio based packet radio systems as stand-alone systems or as nodes in a newly emerging alternative internet” (Nocturnals-Anonymous). The Free Network Foundation (fNf), Project Mesh Net, and Open-mesh.org use Freedom Towers and unregistered routers to create their own independent networks. These three groups are “developing a ‘mesh’ approach to the internet which, theoretically, would be free, ubiquitous and anonymous” (Nocturnals-Anonymous) and as peer-to-peer networks would eliminate all intermediaries. Their goal, according to Brian Anderson, director of the documentary Free the Network: Hackers Take Back the Internet, is to create an uncensorable internet—a network free from government or corporate manipulation and regulation. Together all of these many alternative approaches are starting to coalesce into real opposition to outside control. Since they are not operating in secret, it will be a challenge to defeat official opposition. The fNf speculates:

If such a “meshnet” does come into existence, we can expect a vigorous reaction by governments the world over. However, where there is no “there” there to regulate, where the transactions are anonymous and essentially untraceable, it remains unclear what steps will be available to a government to assert control over such a system, but we can certainly expect them to try. (Nocturnals-Anonymous)

As Professor Xavier says in The X-Men, “anonymity is the first line of defense” (Güres, 2012: 54). To continue to enable protest and reform, it is crucial that protesters need to be able to do so as anonymous subjects and with anonymous data. “Always a means, never an end in itself” (55), Seda Gürses says that anonymity is generally perceived as a crime, but in fact it is a necessary strategy under oppressive regimes where people’s movements are closely controlled. Anonymity as a strategy enables us to strip messages of any useable or traceable information. This is particularly important in the United States and Canada where data is increasingly inaccessible. Under the European Data Protection Directive, anonymous data is free. Anyone can access it, mine it, use it, or even repurpose it. In North America, the reverse is true: we are locked out of access even to anonymous data, and the big brother of social media mercilessly catalogues our own data. Instead,
we might well imagine a world such as Karen Mancel and Herman Maat’s interactive wearable work, Tele_Trust. Maat says that all communication is “based on trust” (Mancel and Maat, 2009). We can read religious significance into the veil-like wearable technology, but it could also be a high-tech suit that plugs the user into a mode of transmission. Proximity creates a network of bodies and enables communication, as touch triggers snippets of conversation about trust issues. The transmissions that are received are excerpts from interviews with people around the issues of safety, and the dichotomy of public/private space. These messages are transmitted to interactors who touch the wearer, to plug in to that person’s personal network. Karen Mancel asks: “Is it necessary to touch somebody to be able to trust him?” (Mancel and Maat, 2009)

In conclusion, I would ask: Where lies the future of public space? If our rights to our personal data, our rights to assemble, and our rights to our molecular autonomy are being stolen from us, then are we forced to adopt an Orwellian kind of doublethink in order to survive? Or is it possible, as the Occupy Movement and a variety of media artists maintain, for us to preserve a space for autonomy? Dataveillance threatens to suck up not just our data, but to anticipate our needs and desires as well. In fact, a study conducted in 2013 by Cambridge University Press (and funded by Microsoft and Boeing), says just that—confirming what Facebook knew all along: given enough data, you can start to make predictions about people’s lifestyle and likes and dislikes. Some of the headlines about their report read:

- Your Facebook Likes can predict your sexual orientation with 88 percent accuracy.
- Liking Harley Davidson . . . is predictive of low intelligence, whereas Liking Curly Fries is predictive of high intelligence.
- If you’ve Liked Hello Kitty, you’re more likely to be creative, but not very conscientious. (Marsden, 2013)

The report, called “Private traits and attributes are predictable from digital records of human behavior,” has spawned a free online personality test called youarewhatyoulike.com, and clearly the lifestyle choices that it predicts with such accuracy have immediate applications for corporations with products to sell. However, to read that as the whole truth about the study is to miss the most interesting part. As Paul Marsden says in his assessment of the report, Facebook does have a cunning accuracy when it comes to predicting issues with binary
or dichotomous structures. What he does not say is that Facebook is modeling dichotomies. It is the opinions, actions, complexities, and contradictions that fall outside of those simple yes/no choices that do not find their way into the study.

Similarly, Jill Magid, a Dutch artist who uses CCTV as a performance medium, says:

Surveillance cameras create stages, or fixed, monitored platforms. Under their gaze there is a potential for me to act, and a potential to save this act as a recorded event. By watching an area rather than an individual, the camera in its static position seems to favor its context over the pedestrians passing through it. It seems to say: The city is permanent, the civilian ephemeral. In a positive sense, this technology offers me a way to place myself, to become visible (and potentially permanent) within the city, through a medium bigger than myself. It is thus a creative field in which I choose to play. In terms of its political position (as maintaining security or, conversely, invading privacy) I see these positions as qualities of the technology itself—criteria of the tool that simply makes its use, in my way, more loaded. (Lovink, 2004)

So, perhaps, it is ultimately not the body-as-subject, but rather the site-as-subject, where the gaze of surveillance falls, that matters. For, as so many of these artists and programmers have demonstrated, it is the restrictions themselves that fuel innovation. Perhaps it is the struggle against oppression that matters most. As long as we continue to struggle for the right to be anonymous, then we may well find a way to preserve our freedoms and to regain so many of the rights to privacy that we have lost.

REFERENCES

Cornwell, Peter J. 2002. “Surveillance ofAssailants and Face[value].” In CTRL [SPACE]: Rhetorics of Surveillance from Bentham to Big Brother, ed. Thomas Y.


The Free Network Foundation: http://thefnf.org
