Article | Automating Surveillance

Mark Andrejevic

Monash University, Australia
mark.andrejevic@monash.edu

Abstract

This article considers the changing logics of surveillance in the era of automated data collection and processing. It argues that automation results in the emergence of post-disciplinary forms of monitoring that no longer rely on the subject's internalization of the monitoring gaze. Such forms of monitoring do not displace other forms of surveillance but represent a new development made possible by the promise that comprehensive data collection will allow prediction and pre-emption to replace deterrence. In the context of predictive analytics, simulated futures serve as the basis for ongoing processes of intervention that take place in the present. The parsimony of the panopticon, which traded on the uncertainty provided by its partial gaze, is replaced by the tendency toward comprehensive monitoring associated with the proliferation of distributed, embedded, always-on sensing networks. The resulting forms of automated surveillance are characterized by post-representational logics that I describe in terms of operationalism, environmentality, and framelessness.

The World Becomes Alexa

The prognosis for our information environment is clear: interactivity will become functionally synonymous with surveillance, for many purposes. This equation has made its way into popular descriptions of the online economy as a “surveillance economy”—even by the decidedly staid *Wall Street Journal* (Angwin 2012). New forms of convenience coincide with increasingly powerful and comprehensive data collection. At no previous time in human history has so much information about so many been captured, stored, and sorted. Thanks to the rapid development of networked digital platforms, it seems safe to say that this will be true of each subsequent generation for the foreseeable future. We are rapidly headed toward a world in which all aspects of our lives become increasingly dependent upon digital media that, in turn, create comprehensive records of our activities, communications, purchases, and—to the extent that these can be rendered in digital form—our thoughts, hopes, and dreams.

Monitoring at this level requires the development of digital infrastructures and platforms on an increasingly comprehensive scale; above all, it requires automation. There is no other way to amass, make sense of, and put to use such large amounts of data. Even the spaces through which we move are being enfolded within infrastructures of automated data capture. Consider, for example, Google's smart city development in Toronto, which critics have billed as a “city of surveillance” (Kofman 2018). As one commentator put it, “It's one thing to willingly install Alexa in your home...It's another when publicly owned infrastructure—streets, bridges, parks and plazas—is Alexa, so to speak” (Kofman 2018). Private monitoring infrastructures have already thoroughly embedded themselves in the daily lives of many, in the form of smart phones and other portable networked devices, smart speakers, smart cameras, and a growing range of systems that combine the promise of convenience and efficiency with increasingly comprehensive forms of data capture.

Andrejevic, Mark. 2019. Automating Surveillance. *Surveillance & Society* 17(1/2): 7-13.

<https://ojs.library.queensu.ca/index.php/surveillance-and-society/index> | ISSN: 1477-7487

© The author(s), 2019 | Licensed to the Surveillance Studies Network under a [Creative Commons Attribution Non-Commercial No Derivatives license](#)

Data collection on this scale initiates a *cascading* logic of automation. Embedded sensors automate data capture, generating quantities of information that can only be handled by automated data processing and, increasingly, automated response. While it is true that not all forms of information collection qualify as “surveillance,” the development of this sensor-permeated infrastructure enables new logics of surveillance to emerge and take hold. This article explores three characteristic aspects of automated surveillance, based on the premise that profound changes in processes of data capture warrant reconsidering how we think about and understand the implications of mass—and mass-customized—monitoring. Automated surveillance is “operational” in the sense that it privileges intervention over the symbolic power of the monitoring apparatus; it is “environmental” in its mode of governance and “frameless” in scope. These aspects of automation conspire not just to reconfigure the capabilities and applications of surveillance, but, at the limit, to also displace human judgment and, thus, to foreclose the symbolic space for politics. Given the reliance of digital surveillance on media technologies, these developments are in keeping with the broader technological affordances of automated media in the context of what Zuboff (2015) has described as “surveillance capitalism.” As Zuboff put it, in a 2019 interview, “It is no longer enough to automate information flows about us; the goal now is to automate us” (Naughton 2019).

Since the following arguments draw on some established theories of surveillance, it is worth clarifying the article’s approach to the concept of surveillance. When we speak of surveillance, there is a tendency to invoke associations with the specter of Big Brother and oppressive forms of state control—the secret police and its various appurtenances: wiretaps, closed-circuit cameras, and hidden microphones. The convergence of commercial and state technologies has made it easy to blur whatever distinction there might have been between monitoring and surveillance. As the Snowden leaks revealed, state intelligence agencies piggyback on data that is collected for marketing purposes (Greenwald 2014). Moreover, state surveillance relies on, among other systems, the commercial platforms we increasingly use for entertainment, commerce, and work. In many cases, state surveillance also models its data collection and processing practices on systems the commercial sector has pioneered. The former Chief Technical Officer of the CIA, for example, invoked the inspiration for his “collect everything and hold on to it forever” approach by referencing “the Google Framework” (Ingram 2013). The mainstreaming of “surveillance capitalism” (Zuboff 2015) as an economic model for online platforms and services blurs the line between monitoring and surveillance—not least because market monitoring increasingly shades into manipulation and exploitation. Consider, for example, Facebook’s leaked claim to advertisers that it can profile teenagers to track when they feel “insecure,” “anxious,” and in “need of a confidence boost” (Levin 2017). Tracking the fears and anxieties of young people in order to deploy these as leverage to influence behavior is an activity that approaches the more sinister and authoritarian uses of surveillance power.

Defining foundational terms is always a vexed task. But for the purposes of the following analysis, surveillance is interpreted broadly in order to acknowledge the blurred boundaries between state and consumer surveillance and, thus, between control, convenience, and care. The Surveillance Studies Network’s 2006 Report on The Surveillance Society offers a suitably broad definition, “Where we find purposeful, routine, systematic and focused attention paid to personal details, for the sake of control, entitlement, management, influence or protection, we are looking at surveillance” (Ball and Wood 2006), though we might add profit to the list. When we speak of surveillance, we also typically invoke asymmetrical power relations between watcher and watched, with the former in the dominant position. Thus, we tend to distinguish forms of monitoring as accountability—for example, the monitoring of public officials or corporate leaders by journalists—from the top-down exercise of surveillance power. The emerging logics of automated surveillance described in this article may also apply to monitoring more broadly in the digital era, but the primary focus of this article is on those practices associated with powerful state and economic institutions. The defining characteristics of automated surveillance in these contexts do not completely replace what came before; rather, they emerge alongside more familiar surveillance practices and, in some contexts, displace them.

“Total” Information Capture

It is not hard to gain a sense of the shift wrought by automation in contemporary monitoring and surveillance strategies. We can, perhaps, feel the ongoing reduction of the “slack” once associated with not being subject to constant, ubiquitous monitoring, both in the office and at home, as our computers check online to ensure the software we are using is licensed and our employers have new and increasingly powerful systems for tracking our work practices. In the not-too-distant future, when self-driving cars rule the roads, it seems likely that speeding and running red lights will become a thing of the past. There will be many benefits associated with such developments, but there will also be a consolidation of centralized forms of information collection and control. We realize that this progression is an ongoing one and that we are headed toward a world in which corporate and state entities will have comprehensive profiles of every aspect of our professional, personal, and social lives, thanks in part to the “smart” technologies of the future being applied to our phones, cars, offices, and cities. The technological affordances of digital media make comprehensive data collection seem possible and the prospect of enhanced control make it seem desirable. The welter of data promises to crowd out uncertainty and lack of control.

The fantasy of total surveillance accompanies the increasingly disconcerting drive to displace social relations with technological ones (for example, as in the case of new forms of data-driven automated decision-making that characterize job recruiting, parole decisions, risk assessment, and a growing range of social practices). This is not a new fantasy. Rather, it addresses a deep-seated social anxiety: that we all fundamentally depend on forms of trust that can be abused and disappointed. These socially necessary forms of trust are built into the rhythms of our daily lives, and our dependence upon them has come to seem more and more like a vector of vulnerability, especially when viewed against the background of the myriad threats they enable. At every “stop” sign on the traffic grid, for example, we find ourselves at the mercy of each other’s willingness to follow the rules of the road. We continually confront our fragility when this willingness is suspended, sometimes deliberately, as in the case of automotive attacks in France, Australia, Canada, and elsewhere. In Australia, the simple but diabolical act of sticking needles in strawberries demonstrated how easy it is to sabotage the food supply and thus how vulnerable we are in the face of the deliberate abuse of the trust that underwrites daily life (Cohen and Lewis 2018). How else to combat such vulnerabilities than by monitoring everything all the time? The prospect of total surveillance offers to relieve us of the social burden of having to trust one another at a time when it is becoming harder than ever to do so, thanks to the automated dissemination of polarizing content and the related mobilization of the distrust of “fake news” as a political strategy.

Much the same can be said of a range of automated technologies that have a surveillance dimension to them, from always-on smart cameras to smart supermarkets. The (impossible) promise of total surveillance coincides with the (equally impossible) promise of freedom in the form of total autonomy: the attempt to subtract ourselves from experiencing one of the defining anxieties of the social, which is that our trust might be misplaced and abused because our vulnerability is in the hands of others.

Symbolic Surveillance

Automated surveillance emerges at the intersection of this anxiety with the emerging technological capacity to imagine the possibility of total data capture. We can start to see how the promise of comprehensive surveillance differentiates itself from the operation of the defining figure of modern surveillance: Jeremy Bentham’s panopticon prison design, in which every prisoner is visible to a superintendent hidden in a central tower (Bentham 2011). As Michel Foucault (2012) famously argued, panoptic power relies upon discipline, and discipline depends, in turn, on the symbolic efficiency of the spectacle of surveillance. Crucial to the functioning of the panopticon is not just the fact that the inspector in the prison’s central tower can see into the surrounding cells but also that the tower itself dominates the visual horizon of the inmates as testimony to the fact that they could be subject to the monitoring gaze at any time. The tower—and not, significantly, the inspector (who is carefully hidden from the inmates’ gaze)—serves as the visible symbol of surveillance. The actual (as opposed to symbolic) surveillance Bentham imagined might eventually be

dispensed with as long as the tower retained its efficiency: this was the promise and power of the panopticon. In keeping with Bentham's utilitarianism, the panopticon he envisioned operated on the principle of parsimony: the least actual surveillance, the least punishment, and the fewest overseers could achieve the greatest impact through an innovative use of design and symbolism.

Automated surveillance, by contrast, operates according to a principal that might be described as the opposite of parsimony: the prospect of comprehensive, always-on ubiquitous monitoring, and the implicit understanding that there is always the need for more. If a risk is missed, a prediction flawed, then the proposed solution is always more thorough, accurate monitoring—never less. In this model, symbolic surveillance—and its attendant logic of uncertainty—is displaced by actual surveillance. If the tower symbolized the omniscient gaze, then the advent of digital technology makes it real. Within the panoptic system, as Foucault put it, being watched all the time is “at once too much and too little” for the purposes of disciplinary control of the monitored subject: “too little, for what matters is that he knows himself to be observed; too much, because he has no need in fact of being so” (Bentham 2011: 201). In the automatic system, by contrast, panoptic surveillance is also too much and too little, but for different reasons. It is too much because the target need not be aware of being monitored; too little because monitoring must be as comprehensive as possible. If, in the disciplinary model, awareness of surveillance ensures the internalization of the priorities of the monitoring gaze, then, in the automated model, the goal is to capture the undisciplined activity of those being monitored so as to more accurately categorize, sort, and anticipate these activities.

Thus, if the disciplinary model relies upon deterrence, then automated one relies upon pre-emption. The former is internalized control, whereas the latter envisions the continual exercise of external force. As Rapping (1999) argues in her groundbreaking work on the *Cops* TV format, the figure of the post-disciplinary subject is the irrational, implacable, a-subjective figure of the criminal as terrorist. Such a figure cannot be reached by the symbolic power of the spectacle of surveillance: being watched does not result in the internalization of the monitoring gaze and its imperatives. For automated surveillance, the operational question becomes whether observation can detect in time to pre-empt.

Operationalism

If, as Foucault argues, the panoptic apparatus is remarkable for its “lightness” (once discipline is internalized, surveillance and punishment become superfluous), then the automated version is characterized by its weight: the surveillance apparatus must become increasingly powerful, data processing ever more sophisticated, and the process of intervention ongoing. There will always be another eruption of criminality to be predicted and acted upon. If the logic of the panopticon was industrial—securing the productivity of the target through ensuring its docility—then that of automated surveillance is not directed toward maximizing the productivity of the workforce with an eye to displacing it, but simply taming it. Since docility is increasingly called into question (reliant as it is on disciplinable subjects), ongoing external intervention becomes the constant accompaniment of automated surveillance. This is the logic of the drone strike, of predictive policing, and, suggestively, of the libertarian paternalism of “nudge” economics, which relies on experiment and observation to pre-empt undesirable behavior. From the perspective of the “choice architects” of the nudge economy (Thaler and Sunstein 2012), discipline is irrelevant: what they require is observational data that predicts how people will respond to changes in their decision-making context or environment. In automated surveillance systems, the homogeneity of the disciplinary model is replaced by continual processes of experimentation and environmental modulation calculated to generate more data and thus anticipate and foreclose through intervention.

With these contrasts in mind, we can elaborate three defining characteristics of automated surveillance: operationalism, environmentality, and framelessness. Such an account supplements Deleuze's (1992) influential formulation of “control societies” by directing attention to the post-representational character of automated surveillance. If panoptic power is symbolic in the sense that it relies on the efficacy of the spectacle of surveillance, automated surveillance is operational in that it acts instead of displays or warns.

The surveillance camera works to encourage the target to internalize the lessons of surveillance, whereas the automated system triggers the ongoing application of external force: police are dispatched by a predictive algorithm to catch criminals “in the act” and drones are deployed to assassinate insurgents before they can act. This shift accords with an environment in which surveillance is no longer exceptional but constant, no longer targeted but ubiquitous. It reflects the erosion or inefficacy of the symbolic power of surveillance in certain contexts as well as the dramatic reduction in the cost of comprehensive surveillance associated with networked digital media.

Environmentality

Although impossible as an actual endpoint, the goal of total information capture remains the guiding theme of automated surveillance. This is evidenced by the recurring response to the many critics of its failures in practice: always what is needed is more and better data. If targeted ads get it wrong, if police surveillance fails to accurately predict criminal activity, then these outcomes are repeatedly attributed to incomplete or inaccurate information: the system just needs to know everyone better. This is an imperative that neatly parallels the proliferation of interactive systems that do just that by promising to capture more detailed information about the rhythms of our daily lives. The enduring symbolic/disciplinary power of surveillance, in this reconfigured context, is to impress upon the populace the importance of submission to the imperative of comprehensive information capture—in the name of security, efficiency, and convenience. As Dawar (2018) suggests in an article in the *Harvard Business Review*, accurate marketing relies on a comprehensive monitoring infrastructure: “A platform serves consumers by constantly anticipating their needs. To do that it must collect granular data on their purchasing patterns and product use and try to understand their goals” (Dawar 2018). To “understand” here is to predict future behavior and responses. Pre-empting behavior, whether an act of destruction or consumption, relies on comprehensive monitoring not just of individuals but also of populations and environments. This is why post-panoptic intervention is “heavy” in the sense that it requires information capture and processing at a heretofore-incomprehensible scale—one only imaginable in a context of automation. The ubiquitous “smartening” of our environment envisions its redoubling in the form of a sensor. Putting this information to use simultaneously pushes in the direction of the environment—whether smart space, office, or car—as a medium of response: these smart surroundings do not simply collect information, they also reconfigure themselves cybernetically to act upon their constituent elements and inhabitants. We are already familiar with this dynamic online: advertisers experiment with user response so as to change ad design in real time; ads and newsfeeds reconfigure themselves in response to our online activity. Dynamic infrastructures like networks of self-driving cars would operate similarly. Even physical spaces can reconfigure themselves in response to sensor activity: changing billboards, information, and ad displays in real time and, perhaps, even modulating the physical environment to canalize our activity and movements.

In keeping with this logic of environmental modulation, Gabrys (2014) has drawn on Foucault’s conception of environmentality to describe the mode of governance associated with monitoring in smart environments. Building on a series of remarks in Foucault’s late lectures, Gabrys marks the shift from discipline to environmentality (which modulates the milieu or context of action): “he suggests the subject or population may be less relevant for understanding the exercise of biopolitical techniques, since alterations of environmental conditions may become a new way to implement regulation” (2014: 35). This formulation neatly captures the shift from discipline to prediction—from internalized forms of prevention to externalized modes of pre-emption, from the symbolic role of the camera to the operational one of automated systems. As Massumi (2009) puts it, “environmentality must work through the ‘regulation of effects’ rather than of causes” (154). The work of control takes place not on the inside—through processes of individual training and discipline—but from the outside, via an environment that serves as sensor, probe, and, when necessary, agent.

Framelessness

When the environment becomes a sensor there is no clear delimitation on what is to be collected, sorted, and processed—a result in keeping with the emergent and speculative character of data mining. Limiting the scope of data collection would run counter to the goal of unearthing unanticipated correlations. It is not surprising that the deployment of monitoring devices favors always-on data capture, which is enabled by the expansion of networked interactivity. Automated data collection might then be described as “frameless” in several senses. It can dispense with a conceptual selection framework—a frame for deciding in advance what information is relevant. Similarly, since there are no pre-selection criteria, we can expect that the data collection infrastructure will continue to expand indefinitely: interactive devices will accumulate new and more sophisticated sensors to capture ever-expanding categories of information (biometrics, mood, etc.). Finally, there are no spatial or functional grounds for delineating between monitored and non-monitored spaces. In the disciplinary model of industrial control, surveillance focused on the workspace (and other designated sites of regulation: schools and prisons, for example). Here, monitoring helped delineate spaces of production from those of leisure or domesticity, which were not subject to the most concentrated regimes of oversight and control. In the digital era, by contrast, networked interactivity de-differentiates the monitoring process: data capture comes to permeate a growing range of spaces and activities.

Taken to its limit, the endpoint of data-driven decision-making is the automation of judgment. This endpoint represents the attempt to overcome the limitation of the human frame: that of the subject, for it is the figure of the subject that limits how much information can be absorbed and processed. One of the reasons machines invite fantasies of neutrality or objectivity is that they promise to be able to transcend the partiality—in both senses of the word—of subjectivity. If human subjects are limited, necessarily, to a situated viewpoint because their knowledge of the world can only ever be incomplete, then the prospect of total information capture coincides with a vantage point that can, finally, encompass the full picture. The more we remind ourselves of the fallacy of machinic neutrality—because of incomplete, inaccurate, or biased data, or the fact algorithms are crafted by humans and incorporate their own limitations—the more we invoke the imperative to attempt to clean the data, make it accurate, and turn the development of automated systems over to the machines themselves. What needs to be contested is the very notion of completeness as a condition for judgment, or, by the same token, the notion that finitude or partiality is a hindrance rather than a condition of possibility. In practical terms, the goal of automation is to develop systems that replace societal decisions governing life, liberty, and opportunity.

In this ambition there is a deep-rooted antipathy to the political for conceding the inevitability of finitude. In this respect automation partakes of what the philosopher Slavoj Žižek describes as “the dream of a language which no longer acts upon the subject merely through the intermediate sphere of meaning, but has direct effects in the real” (1996: 196). This is the promise of machine language, which differs from human language precisely because it is non-representational and therefore collapses the space between saying and doing. The peril posed by automated surveillance is not that it will be perfected but that we will act as if it could be, thereby developing increasingly comprehensive sensing networks to feed into automated sorting and decision-making systems, displacing the language of politics with the efficacy of the operation.

References

- Angwin, Julia. 2012. The Surveillance Economy. *The Wall Street Journal*, September 29. <https://www.wsj.com/articles/SB10000872396390443389604578026473954094366> [accessed November 15, 2018].
- Ball, Kirstie, and David Murakami Wood (eds). 2006. A Report on The Surveillance Society. A report by the Surveillance Studies Network. September. <https://ico.org.uk/media/about-the-ico/documents/1042391/surveillance-societysummary-06.pdf> [accessed January 5, 2019]
- Bentham, Jeremy. 2011. *The Panopticon Writings*, edited by Miran Bozovic. London, UK: Verso.

- Cohen, Hagar, and David Lewis. 2018. Food Terrorism and Other Possible Culprits Behind the Strawberry Contamination Scare. *ABC News*, October 18. <https://www.abc.net.au/news/2018-10-20/three-reasons-needles-could-have-ended-up-in-strawberries/10396822> [accessed November 15, 2018].
- Dawar, Niraj. 2018. Marketing in the Age of Alexa. *Harvard Business Review*, May-June. <https://hbr.org/2018/05/marketing-in-the-age-of-alexa> [accessed November 15, 2018].
- Deleuze, Gilles. 1992. Postscript on Societies of Control. *October* 59: 3-7.
- Foucault, Michel. 2012. *Discipline and Punish: The Birth of the Prison*. London, UK: Vintage.
- Gabrys, Jennifer. 2014. Programming Environments: Environmentality and Citizen Sensing in the Smart City. *Environment and Planning D: Society and Space* 32 (1): 30-48.
- Greenwald, Glenn. (2014). *No Place to Hide: Edward Snowden, the NSA, and the US Surveillance State*. New York: Macmillan.
- Ingram, Matthew. 2013. Even the CIA is Struggling to Deal With The Volume of Real-Time Social Data. *Gigaom.com* March 20. <https://gigaom.com/2013/03/20/even-the-cia-is-struggling-to-deal-with-the-volume-of-real-time-social-data/2/> [accessed November 15, 2018].
- Kofman, Ava. 2018. Google's "Smart City of Surveillance" Faces New Resistance in Toronto. *The Intercept*, November 14. <https://theintercept.com/2018/11/13/google-quayside-toronto-smart-city/> [accessed November 15, 2018].
- Levin, Sam. 2017. Facebook told advertisers it can identify teens feeling 'insecure' and 'worthless'. *The Guardian*, May 2. <https://www.theguardian.com/technology/2017/may/01/facebook-advertising-data-insecure-teens> [accessed November 15, 2018].
- Massumi, Brian. 2009. National Enterprise Emergency: Steps Toward an Ecology of Powers. *Theory, Culture & Society* 26 (6):153-185.
- Naughton, John. 2019. The Goal Is to Automate Us: Welcome to The Age of Surveillance Capitalism. *The Guardian*, January 20. <https://www.theguardian.com/technology/2019/jan/20/shoshana-zuboff-age-of-surveillance-capitalism-google-facebook> [accessed, January 24, 2019].
- Rapping, Elayne. 1999. Aliens, Nomads, Mad Dogs, and Road Warriors: Tabloid TV and the New Face of Criminal Violence. In *Mythologies of Violence in Postmodern Media*, edited by Christopher Sharrett and Barry Keith Grant. Detroit, MI: Wayne State University Press.
- Thaler, Richard, and Cass R. Sunstein. 2012. *Nudge: Improving Decisions About Health, Wealth, and Happiness*. London: Penguin.
- Žižek, Slavoj. 1996. *The Indivisible Remainder: An Essay on Schelling and Related Matters*. London: Verso.
- Zuboff, Shoshana. 2015. Big Other: Surveillance Capitalism and the Prospects of an Information Civilization. *Journal of Information Technology* 30 (1): 75-89.