FOREWORD

MARK ANDREJEVIC

If in the physical environment the pressing issue of the next several de-cades (and beyond) is likely to be the dramatic transformation of the global climate, in the social realm (to the extent that it can be distin-guished from the physical environment), the main issue will be the shift-ing surveillance climate. I don't think this is overstating the case: in the areas of politics, economics, commerce, policing, finance, warfare, and beyond, social practices are being transformed by dramatic develop-ments in information collection, storage, and processing, as well as by various techniques of watching, broadly construed. The occasional anec-dote about the power of new forms of data monitoring and mining—the retail outlet that learned a young woman was pregnant before she told her family, the ability of mobile phone use to predict whether someone is coming down with the flu, the use of license-plate readers to reconstruct people's whereabouts—are only tiny foretastes of the automated, multi-dimensional forms of surveillance to come.

We are at a moment in time when we can start to see the surveillant imaginary expand vertiginously, thanks in part to the new avenues for monitoring opened up by technologies that "interact" with us in a grow-ing variety of ways and involve a wide range of senses and sensors, and

also to the increasingly sophisticated techniques for putting to use the huge amounts of data these devices, applications, and platforms capture and store. Intimations of a megadata world are starting to multiply: Edward Snowden's revelations about blanket U.S. National Security Agency (NSA) surveillance, media coverage of the huge databases being amassed by companies like Facebook and Google, and the proliferation of data centers across the landscape, including the NSA's giant complex in Utah. It is a moment that requires reflection on what is at stake in the seemingly inevitable slide into a monitored, digitally redoubled life. This volume represents a defining moment in that process of reflection—the cultivation of a critical imagination that keeps pace with the technological developments and their associated practices in reach, scope, and depth, but counters the ahistorical rhetoric of the digital sublime (Mosco 2004) with a deep sensitivity to suppressed historical continuities and antecedents.

This book provides several useful explorations of the meaning of the term *surveillance*, but perhaps the most simple and generic is that it is the coupling of information collection and use with power. We are living in a time when information is becoming an increasingly transformative force, and power is never absent. In other words, the information "revolution" (in the ironically depoliticized sense in which it is so often invoked), viewed through the lens of power, is perhaps better reconceptualized as a surveillance one. If late twentieth-century preoccupations with power were atomic and ballistic, those of the twenty-first century are increasingly informatic. Fantasies of jetpacks and passenger trips to the moon have largely (but not entirely) given way to ones about new forms of informatization, representation, and interaction. The threat of "the bomb" is complemented by that of a "cyber-Pearl Harbor" (Bumiller and Shanker 2012). We are becoming more preoccupied with novel ways of giving wings to our surveillance devices, sensors, probes (and "smart" weapons) than to ourselves. A fascination with the industrial-era power of turbines and rocket ships is supplemented by the information-era fantasy of total information awareness.

It is against this background that surveillance emerges as a pressing topic of study for the foreseeable future. And at this point, it is the research object itself that defines the field—not a methodology, not even a theoretical canon or a developed, shared set of terms and concerns. This collection both confirms such an observation and qualifies it, for it works in the direction of defining a particular set of approaches and issues, spe-

cifically bringing to bear methodologies and interests based on intersectional feminist commitments and theories. The study of surveillance is, of necessity, a study of power relations, and while it might be possible to attempt to adopt a disinterested, neutral or "administrative" stance to such an endeavor, the studies presented here suggest the disingenuous or complicit character of any such attempt. As Kevin Walby and Seantel Anais put it in their contribution to this collection, a feminist approach is concerned with getting away from neutral definitions of surveillance and putting critique first in order to continually point out "how ruling relations are enabled by the texts and classifications that make up surveillance" (220). The study of surveillance is also, as this collection points out, a recursive endeavor, at least insofar as research is also a form of monitoring and therefore implicated in the relations of power being examined, as Ummni Khan makes clear in her contribution. As in other instances, what is seen or registered is as important as what is exempted from or obscured by the monitoring gaze.

One of the central themes that emerge from this collection is an engagement with what has been, in one way or another, overlooked or obscured in the emerging formation of surveillance studies. At the most basic level, this includes the wide-ranging scope of what ought to be counted as surveillance, especially those monitoring practices that attempt to exempt themselves from an entanglement with power or to cloak themselves in taken-for-granted imperatives. If technologies like CCTV (closed-circuit television) cameras, drones, and wiretapping lend themselves to an already well-conditioned response to the prospect of state surveillance, the perspectives included in the following pages expand and reconfigure the scope of research to include techniques and technologies that might otherwise fly below the radar of surveillance studies: genetic screening in fertility clinics, photographic evidence of domestic violence, images of babies in the womb, birth certificates, security screening, Twitter practices, and the other seemingly mundane forms of data collection, observation, entertainment, and sorting that increasingly characterize daily life in informated and technologized societies.

This volume explores the ways in which techniques conventionally relegated to the realm of monitoring and documentation—but not surveillance proper—mask and reinforce the gendered, sexed, raced, and classed exercise of power. The ambit of surveillance studies is thereby reconfigured to move beyond the field's more "traditional" focus and its historical ties to sociology's twentieth-century concern with criminology. Rather, it

sets out to explore the ways in which a concern with forms of governance and regulation extends into those practices that assume the guise of scientific neutrality, bureaucratic record keeping, or the largely unexamined social imperatives of securitization, efficiency, risk management, productivity, and reproductivity. There is no neutral record keeping—all forms of data collection have imperatives built in—and the power of the work assembled here lies in disembedding and exposing these imperatives, the interests they serve, and the uses they enable.

The initiative represented by this volume is a timely one for the formation of surveillance studies, a formation whose object is increasingly engulfed by what might be described, on the one hand, as the alleged neutrality of the machine (or the algorithm) and, on the other, as the various alibis of security, efficiency, entertainment, and convenience. Consider, for example, Google's protest in response to Microsoft's "Scroogled" campaign, which criticizes the search-engine giant's business model of targeting advertising based on (among other things) the content of users' email messages. Google countered Microsoft's accusations of privacy invasion by noting, "No humans read your email or Google account information in order to show you advertisements or related information" (D. Kerr 2013). It is a telling protest insofar as it frames the issue of monitoring quite specifically: what counts as intrusive is not the uses to which information is being put (a topic Google's response dodges), but the prospect of another human poking his or her nose into one's personal correspondence. By contrast, the algorithm carries with it the promise of automated neutrality, a machinic "disinterest" that simply operates in the service of convenience, customization, and efficiency (as well as a hint of blackmail: "Wouldn't you rather see ads relevant to you than be bombarded by those that aren't?"). We are invited to place ourselves and our faith in the indifferent hands of the algorithm. In the face of such an invitation, one pressing task for surveillance studies (understood as a critical engagement with the relationship between power and information collection) is to excavate the various interests, pressures, prejudices, and agendas obscured by the technocratic alibi of the algorithm and its analogs—that is, those forms of control that operate in the name of security, efficiency, risk management, and so on, while simultaneously obscuring the forms of gendered, raced, classed, and sexualized discrimination they advance in the name of an allegedly general interest.

There may be aspects of novelty in the expanding role of the algorithm, but one of the lessons of this collection is that there is also a deep sense

of continuity ranging across those forms of surveillance that take place in the name of information-based rationalization or, perhaps even less extravagantly, those that are portrayed as benign, or as entertaining, or even as activist forms of monitoring. Another lesson that emerges in this volume is the importance of focusing not only on the specter of "abuse" or "misuse" of monitoring technologies and practices, but on their proper use and the implications. The prevailing form of misdirection about the information society mobilized by various pundits, publicists, and flaks is their emphasis on what counts as *abuse* (identity theft, fraud, data breaches, and so on), which works to deflect attention away from concerns about emergent *uses*. Focus on these abuses (as important as they may be) backgrounds the "normal" functioning of data collection and use as taken-for-granted—that is, as non-abusive. The important message that recurs across the essays in this collection is that the sanctioned *uses* of the surveillance technology in question—whether for the express purposes of safety, health, marketing, security, entertainment, or protection—require further investigation and interrogation.

Neutrality is the ruse of the algorithm, which, as some of the contributors here demonstrate, does not emerge full-blown, independent of human intervention, but often incorporates the prejudices of "domain specific" expertise and historical patterns of data collection. Data collection is no more neutral than the algorithm, at least until the (impossible) ideal of a fully recorded life is achieved—and even then, that life must be disaggregated and reassembled if it is to be compared, sorted, and mined. At the same time, the algorithm raises the specter of new and reconfigured forms of discrimination based on the emergent and opaque character of data mining.

Relatively crude forms of red-lining, for example, had the exploitable weakness of being discernible and attributable to established forms of discrimination and prejudice. Data mining offers the prospect of reconfiguring and obscuring these forms of discrimination in ways that are difficult to discern or reverse-engineer. If a particular configuration of variables adds up to a prediction—that someone is a "person of interest," an undesirable employee, a credit risk—that prediction does not necessarily come with any assumed underlying explanation: it passes itself off as free of preconceptions, as simply the numbers speaking for themselves. Thus, the prospect offered up by data mining is that of a reorganized range of categories of discrimination—that is, new proxies for use in sorting and predicting. While it may be illegal to discriminate, for example, on the

basis of protected categories for a particular job, the data mine promises new correlations that can serve as opaque alibis, deflecting attempts to demonstrate the links between employment decisions and ethnicity, sex, race, gender, and class. The data can be queried in more specific terms: what is the probability that a particular job candidate will take an extended leave of paid absence, that a prospective student will become a cash donor on graduation, that someone will default on a loan, or that someone will need to be hospitalized? While such questions might be—and have been—amenable to traditional forms of discrimination, data mining promises to generate predictions based on correlations and patterns that cannot be anticipated. This is not to say that ethnicity, class, sex, gender, race, and sexuality will not be implicated, but rather that their roles will be potentially obscured and reconfigured by the range of variables under consideration and the complexity of the correlations on which the algorithm draws. Put in somewhat different terms, the potential threat of data mining lies in the ability to disaggregate discrimination based on more granular sets of attributes. Rather than being broad categories that generalize about employability, insurability, credit risk, security threat, and so on, data-based categories can be more finely sliced and reconfigured to, on the one hand, obscure connections to historical forms of discrimination and, on the other, to reassemble groups that are subject to sorting, targeting, and exclusion.

Dorothy Roberts's essay in this collection notes the way in which, for example, new regimes of targeting and customization underwrite the trend of race-based targeting of pharmaceuticals. As Roberts points out, such developments threaten to resuscitate debunked theories about the biological character of race. At the same time, however, they point in the direction of the disaggregation and reassembly of target groups: not just black patients, but black patients with a heart condition. One might imagine the addition of further variables, some drawn from historical criteria for exploitation, others representing new forms of targeting and specialization (working-class black patients with heart conditions who live in a particular neighborhood, engage in particular types of activities, and so on).

As in the case of other forms of sorting and discrimination, even as data mining promises to become more granular and targeted, it simultaneously subsumes individuals to population-level claims. As one description of data mining in a commercial context put it, "I can't tell you what one shopper is going to do, but I can tell you with 90 percent accu-

racy what one shopper is going to do if he or she looks exactly like one million other shoppers" (Nolan 2012). The claim of data mining is that these predictions are based purely on statistical correlations and not on underlying preconceptions. In actuality, as Shoshana Amielle Magnet has compellingly illustrated in her work on biometric technologies, biases, preconceptions, and prejudices can be baked into the code, where they continue to operate in opaque ways. Magnet explores how debunked conceptions of race are incorporated into facial recognition technology: "As these scientists label the images according to their understanding of their own biological race and gender identities, preconceptions about gender and race are codified into the biometric scanners from the beginning" (2011, 46). Perhaps one of the giveaways is the difficulty algorithms have in predicting what count as rare and exceptional occurrences—that is to say, historical understandings of what is "to be expected" have a way of working themselves into the algorithm.

A world in which preconceptions, biases, and prejudices are coded into the decision-making infrastructure poses new challenges for attempts to intervene in the network of shared meanings. We might describe this outcome in terms of the autonomization of preconceptions and prejudices: because the symbolic processing power has migrated into the algorithm that effectively shapes the decisions that govern everyday life—who gets hired or approved for a loan, who can cross the border and who cannot, who will be targeted, monitored, included or excluded in a variety of contexts—we are invited to imagine that we have somehow moved beyond the constructed assumptions, prejudices, biases, and "truths" that shape its operation. By the same token, we are invited to adopt an external relationship to the efficacy of such preconceptions: disavowing them in daily life while they continue to do their work behind the screen of the interface.

Consider, for example, the way new technologies promise to "see" for their users. The wearable interface, most recently revived by Google Glass, offers to bring "knowledge" beyond what the viewer already knows to what the viewer sees by, for example, recognizing people for the wearer, accessing information about them and sharing it with the wearer, such that the wearer's gaze is mediated by the information retrieved from the database. The Massachusetts Institute of Technology Media Lab's Sixth-Sense system represents a similar attempt to superimpose wirelessly accessed digital information on the physical world. People can tag particular locations with specific information (reviews for a restaurant or

a movie theater and so on), which can then be accessed by others viewing the same location. The technology provides a suggestive metaphor for the fact that our gaze is never unmediated, innocent, or free of preconceptions, background knowledge, and information. Even without the high-tech interface, the physical world is already overlaid with the information the viewer brings to it. Imagine the ways in which such devices might be used by, say, police: forms of background profiling and threat detection might be incorporated into the system so as to categorize each individual as he or she walks by. The result is the automation of shared "knowledge" and preconceptions. That is, a superimposed assessment becomes the result of forms of data processing that take place behind our backs, somewhere in the "cloud" from which the information we are seeing is accessed.

The shared information then comes to serve as a kind of prosthetic collective unconscious—although the process that generates it remains unavailable to viewers, this information nevertheless helps to shape their understanding of the surrounding world. This logic is not dissimilar to that of search engines like Google, which shape the user's experience of the informational world online. When people embark on a search, they see results that are generated by algorithmic logics that remain opaque to them: the results look almost "natural"—the obvious response to a particular search term or query. However, the algorithms that shape the information available to users are developed with a particular set of imperatives in mind, including the goals of attracting and retaining users in an environment conducive to Google's commercial interests.

In some contexts the workings of the algorithm are made partially transparent to users—as in the case of Amazon.com's book recommendations, which allow users to see which past purchases or searches have resulted in a particular book being suggested. For the most part, however, the workings of the algorithm are opaque and are likely to become increasingly so for two reasons. First, the advent of mining "big data"— the unprecedented size of contemporary databases and the emerging techniques for making sense of them (Andrejevic and Gates 2014, 186)—results in algorithms whose results defy explanation or render it superfluous. Someone who buys a particular model of car may be highly likely to be politically conservative, but there is no clear underlying or causal explanation—the pattern is purely correlational. Second, those who control the database and the algorithm have little incentive to make the basis of algorithmic decision making available, not least because this

would entail revealing the increasingly powerful forms of monitoring and surveillance on which they are based.

The development of digital monitoring demonstrates the generalization of the logic unpacked in this volume: unacknowledged biases that underwrite dominant power relations work their way into myriad forms of monitoring and documentation. Thus, the direction in which surveillance is headed will require resources that draw on an intersectional exploration of the ways in which forms of exclusion, discrimination, and sorting are built into the taken-for-granted norms that guide the monitoring process. Suppressed or overlooked histories of surveillance practices provide crucial guides for navigating this unfolding surveillance-scape, in which all forms of monitoring are encompassed by the embrace of power. It is the attention to these norms and the suppressed forms of exclusion and coercion they incorporate that provides crucial avenues for debunking the neutrality of the algorithm and the "completeness" of the database. Similarly, the excavation of suppressed histories helps shed light on what has become all too easy to overlook in the contemporary exercise of surveillance.

Additionally, this collection interrogates and undermines the invocation of the notion of an abstract "we" in the face of surveillance technologies that disaggregate, reconfigure, and sort populations according to a growing range of variables. The obliviousness embedded in this invocation finds its expression in the notorious response of Google CEO Eric Schmidt to concerns about the surveillant character of his company's business: "If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place" (Metz 2009). The formulation seeks to defuse concerns by conflating random strangers ("anyone") with the real cause of concern: entities both public and private with the power to intervene in ways that affect the life chances of "you," who is likely to be someone other than Schmidt, a fabulously wealthy, straight, white, male, U.S. citizen who can imagine he has the luxury of being blithely unconcerned about the monitoring practices he describes (and benefits from). The charge of "something to hide" transfers the blame for the threat of discrimination, exclusion, and exploitation faced by those differently situated than Schmidt onto the victims: what happens to them is a result of something nefarious they must be hiding. Or, tautologically, if they suffer adverse effects, these must be directly attributable to something about them that is wrong, underhanded, or otherwise deviant. Schmidt's public embrace of willing submission to comprehensive

monitoring drives home Rachel Hall's observation in this collection that transparency is effectively the new white.

Google, obviously, is not some diary-invading kid brother or a nosy neighbor, but one of the planet's most powerful private corporations and subject to the subpoena powers of one of its most powerful states — a state which has embarked on widespread monitoring of the population and asserted its right to summarily execute its own citizens in certain circumstances. This is not to say that Schmidt should be concerned himself, but rather that his facile generalization does not take into account the concerns of those differently situated, of those who bear the brunt of the approved uses of surveillance (and not the "abuses" about which Schmidt is certainly as concerned as the next corporate executive). More pointedly, it is to highlight that the temptation to "convince ourselves that vulnerability is equally distributed" (Smith 2010, 8) is limited to those in Schmidt's privileged position. Something similar might be said of the temptation to write in terms of an assumed "we" who are subject to the monitoring gaze, a temptation that itself defines a particular position with regard to emerging surveillance practices. This collection provides a potent reminder of the fact that such a "we" is not to be taken for granted, but rather to be understood as the site of ongoing political struggle.

In developing a feminist set of methodologies and concerns, the pieces in this collection provide a crucial contemporary critical perspective on what counts *for* surveillance and what counts *as* surveillance. It turns out that in both cases the answer is much broader than has been sufficiently addressed by either contemporary debates or academic research. This collection goes a long way toward remedying such omissions and will serve as an important turning point in the critical study of one of the defining practices of the digital age.