International Journal of Communication 11(2017), 879–896 1932–8036/20170005

To Preempt a Thief

MARK ANDREJEVIC
Monash University, Australia
Pomona College, USA

This article explores the implications of recent developments in predictive policing, defined as the use of data-mining tools to predict and preempt criminal activity, for the relationship between citizenship and surveillance. It uses the example of predictive policing to consider the difference between panoptic modes of surveillance and emerging practices of environmental surveillance. The former rely on public awareness of surveillance and the internalization of the monitoring gaze, whereas the latter rely on actuarial modes of prediction. The growing emphasis on strategies for preemption rather than on policies for prevention displace political deliberation with technological expertise and work in the direction of automated decision making about resource allocation and armed response.

Keywords: predictive policing, panopticon, surveillance, preemption, simulation

The transition from the Cold War to the so-called global war on terror marks a shift from logics of symmetrical deterrence to those of asymmetrical preemption. This shift is significant insofar as its effects include the rapid shrinkage of the space and time for deliberation—a diminution heralded by the rise of automated forms of sorting, decision making, and response that promise (or threaten) eventually to subtract the human element altogether. The role of the citizen in such a context is to serve as both pretext and obstacle: that which must be protected and that which serves as potential obstacle to the imperative of securitization. Not just civil rights (e.g., to be free from illegal search) but also civic deliberation threaten the need for immediate response in the face of potentially catastrophic threat. Security then serves as an alibi for, on the one hand, warrantless data collection and, on the other, rapid, preemptive response.

The fantasy of ongoing preemption is enabled by the somewhat fantastical—and yet increasingly familiar—promise of violence without cost enabled by the figure of the drone. The drone represents the possibility of intervening rapidly, at a distance, from a position of invulnerability. If human costs (on the side of those prosecuting the strike) do not figure into the decision-making process, then the logics of tradeoff and negotiation can be dispensed with. If unrest and resistance can be preempted, they do not need to be analyzed or understood. Thus, the specter of "inexplicable" and intransigent violence represented by terrorism complements the "droning" of politics, and, as this article argues, security more generally, which becomes reframed as a form of one-way violence without war.

Mark Andrejevic: Mark.Andrejevic@pomona.edu
Date submitted: 2016–09–05

Delinking violence from the battlefield allows for its indefinite expansion in time and space. This expansion is perhaps best captured by the logic of drone warfare, which subtracts the spatiotemporal limitations of the battlefield from the exercise of violence. If, as Gregoire Chamayou (2015) observes, the goal of defining a battle space geographically was to circumscribe the "licit exercise of violence" (p. 31), drone war envisions the prospect of uncircumscribed violence, which is why, despite his often self-contradictory libertarianism, U.S. Senator Rand Paul gestured toward a kernel of truth when he asked the U.S. attorney general to answer the question of whether the president has the right to use a drone on American citizens in the United States. Perhaps the most interesting aspect of the exchange was Attorney General Holder's qualified reply: "Does the President have the authority to use a weaponized drone to kill an American not engaged in combat on American soil? The answer to that question is no" (Brown, 2013, para. 5). Much hinges on the definition of *combat* invoked by Holder, a term that the war on terror has already expanded beyond its battlefield definition. Once the battlefield is subtracted, the notion of combat (and thus of the combatant) must be redefined to include those who are not directly engaged in armed conflict with an opponent. A combatant can become anyone who at some point in time—past or future—can be configured as a threat.

As in the case of deterrence, the logic of preemption is generalizable, and the technologies of simulation and automation on which it relies can be deployed in a range of scenarios of securitization including *predictive policing*. As in the case of drone warfare, predictive policing models future scenarios to act on them in the present. The shift in emphasis from past to future displaces narratives of causation with the goal of predictive intervention. The result is that preemption does not rely on forms of disciplinary surveillance and its attendant forms of subjectification, but rather on postpanoptic logics of surveillance that substitute total monitoring for selective surveillance and prediction for explanation. The key distinction is that disciplinary systems rely on processes of subjectification whereby the targets of surveillance internalize the imperatives of the monitoring system (to become docile subjects), whereas targets of total surveillance are assumed to be impervious to such processes, and thus in need of perpetual monitoring and ongoing violent intervention. Given that preemption draws on the collection and processing of tremendous amounts of data, it relies increasingly on automated forms of information processing and forms of data mining that are difficult or possible to reverse engineer. The result is decision-making processes that are less open to political processes of deliberation, and it is in this regard that drone logic in policing as in warfare reconfigures the role of citizen, both in terms of rights and responsibilities. Rights are subordinated to the need for total information capture, and responsibilities are delimited by automated decision-making processes that rely on information too voluminous for any individual or group of individuals to comprehend.

Deterrence and Preemption

The militarization of politics becomes a defining tendency of preemption, which takes for granted the defined imperatives of securitization and focuses on operational imperatives of efficiency and effectiveness. Deliberation and intervention at the level of underlying causes are displaced by the imperative of just-in-time response.

Consider, for example, an exchange between news reporter Amy Goodman of DemocracyNow.Org and California Senator Barbara Boxer in response to a United States Senate resolution to authorize the use of military force against the Islamic State of Iraq and the Levant (ISIL). Goodman asked whether, given the apparent failure of military intervention to adequately address the spread of ISIL (and indeed, its contribution to the rise of ISIL), Boxer harbored any reservations about a "more-of-the-same" military approach (DemocracyNow.org, 2015). Boxer's response was immediate, visceral, and, in the era of preemption, increasingly familiar:

> I don't think you sit back with people cutting off the heads of Americans. . . . I think this threat by ISIL is a massive threat and I think it threatens us all. I would never vote to put boots on the ground, but there are ways that we can help others so that they don't have to sit there while their girls have acid thrown in their faces and their heads cut off. I'm just not going to do it. Can't do it. (DemocracyNow.org, 2015, para. 19)

Goodman responded that she was not advocating "doing nothing," but was instead asking whether it might make sense to address the underlying causes behind the rise of groups like ISIL rather than continuing the same military policies that helped bring them into being. Specifically, she suggested that it might be a good time to examine the role of the United States's ally in the region, Saudi Arabia. When Goodman asked, "What about cutting off [ISIL's] support?" Boxer replied: "As far as trying to find out the root causes of why they are the way they are, I'll leave that to you. I'm a Senator and my people are threatened, so I'm going to take action" (DemocracyNow.org, 2015, para. 55).

The exchange was a telling one insofar as Goodman's repeated attempts to address questions of politics, diplomacy, and explanation were treated by Boxer as simply "doing nothing"—as if a paradigm in which foreign policy relied on anything other than the direct and immediate application of force had become an anachronism. The need for immediate response in the face of imminent threat postpones indefinitely any engagement with questions of underlying causes and political solutions. Preemption is not politics by other means, but the foreclosure of politics altogether. The displacement of politics is facilitated by the perceived invulnerability of long-range intervention. Boxer emphasizes the "costlessness" of the approach she advocates: Without specifically mentioning drones (perhaps because the U.S. drone program remains officially classified), she repeatedly refers to her reluctance to put "boots on the ground" because she is, after all, a self-described leader of the "peace movement" who emphasizes that war is only a measure of "last resort" (DemocracyNow.org, 2015, para. 55).

Nonwar violence, however, becomes the default mode of response, suggesting that, in the drone era, simulation no longer operates in the register of deterrence. For Baudrillard (1994), writing against the background of the Cold War, simulation invoked the stasis of "mutually assured destruction." Deterrence, on this account, "comes from that fact that even the real atomic clash is precluded—precluded like the eventuality of the real in a system of signs" (Baudrillard, 1994, p. 22). Baudrillard describes this preclusion in terms of the abolition of the distinction "between the passive and the active" (p. 27). In the case of the Cold War, this abolition takes place from the side of passivity in the sense that the frenetic activities of predicting, calculating, and gaming result in the perpetual deferral of the event being modeled. In the so-called global war on terror, however, the abolition of the distinction between activity

and passivity is reconfigured: Simulation results in distributed, ongoing (indefinite), targeted violence. If deterrence relies on symmetry to maintain stasis, preemption mobilizes asymmetry for the purposes of perpetual, one-way violence.

Deterrence is disciplinary in the sense that it entails the internalization of a rational calculus that forestalls any "first strike"; preemption is postdisciplinary in that it dispenses with logics of threat and deterrence altogether, with the goal of always striking first. If the form of stasis envisioned by deterrence is that of nonattack, the version envisioned by preemption is that all future threats are obliterated now. If the temporality of deterrence is that of indefinite postponement, that of preemption is the collapse of the future into the present: the urgent response to all future threat in the present. In the former, all present conflicts are referred to a future event (that is continually deferred); in the latter, all future conflicts are collapsed into the present.

If political deliberation is predicated, in part, on "the intuition that talking is better than fighting" (Chambers, 1996, p. 2), preemption is decidedly postpolitical. The politics of Cold War conflagration privileged threat over actual conflict (at least in theory, if not in practice, given the number of proxy "hot" wars that took place during the Cold War). The urgency of the war on terror privileges one-way attack over two-sided conflict. It preempts asymmetric threat with asymmetric attack. In so doing, it dispenses with the forms of subjectification associated with Cold War logics of disciplinary governance. In this regard, the forms of monitoring that characterize the war on terror are postpanoptic: They rely not on discipline, but on simulation; not on the spectacle of surveillance, but on covert monitoring; not on incomplete or partial surveillance, but on complete coverage. The point is not that disciplinary practices have disappeared, but that other regimes of monitoring with different logics have emerged to structure relations of power and control.

These logics are not only evident in shifting patterns of warfare but also in domestic forms of security and policing. They are thus relevant not just to international relations but also to domestic politics and citizenship. The next section explores the domestic mobilization of preemption to further consider its reconfiguration of practices of control and governance.

Predictive Policing

In the realm of policing, preemption is characterized by increasingly sophisticated technologies and practices for anticipating criminal activity before it happens: the evolution of so-called predictive policing. When police describe predictive policing, the focus tends to be on what might be described as near-term preemption. The standard example, frequently cited in articles about the pioneering use of predictive policing technology in the city of Santa Cruz, California, recounts the case of an officer positioned just in the right place to catch criminals in the act:

> A Santa Cruz beat cop . . . was eating his lunch in his patrol car in a downtown parking lot because it was on that shift's predictive list. He spotted two women trying to break into cars and arrested them. (Baxter, 2013, para. 15)

Preemption, in this context, remains short term—almost instantaneous. As the opening of one article on predictive policing put it, "What if police could detect a crime before it happened? Say they could nab a burglar before he's even broken a window? Or stop a fight before the first punch has even been thrown?" (O'Donoghue, 2016, para. 1). This is not about prevention in the sense of transforming the conditions that contribute to theft or fighting; it is about being in the right place to stop an imminent act before it takes place. The researchers behind the pioneering PredPol predictive policing program in Los Angeles even claim to have measured the amount of preempted crime that results from the computer-assisted allocation of police patrols. In the period and locations covered by the research,

> The mathematical model produced 4.3 fewer crimes per week, a reduction of 7.4 percent, compared with the number of crimes that the police would have expected had officers not patrolled the "red box" areas [i.e., the areas selected by the computer for deploying patrols]. (Wolpert, 2015, para. 11)

By comparison, human selection of patrol areas resulted in a reduction of only "two crimes per week in each division" (Wolpert, 2015, para. 11). In other words, the research compared crime rates under predictive policing with projected crime rates without police presence: crimes that purportedly would otherwise have taken place.

As in the military context, this approach to preemption relies on a significant reformulation of the very notion of threat in ways that increase the role of automated forms of information collection and processing while reducing that of citizen deliberation and accountability. This essay explores the nature of this reformulation, its relation to emerging practices of predictive policing, and the emerging disconnect between conventional public understandings of surveillance and its changing role in the policing process.

The goal of total surveillance does not mean that everyone is a suspect. Rather, it means that the target is not a particular individual, but the population as a whole and the patterns it forms. The population serves as the background against which potential targets emerge. Disciplinary approaches rely on the narrativization of the influences and factors that contribute to the formation of a criminal profile. Preemptive practices do not intervene at the level of subject formation, but at that of the population. They are actuarial in the sense that they assess overall patterns of risk to determine probabilities of the emergence of particular events over time and space. The more comprehensive the data profile, the higher the likelihood of unearthing a relevant or actionable pattern.

The Temporality of the Future-Present

In the most general terms, predictive policing relies on "taking data from disparate sources, analyzing them and then using results to anticipate, prevent and respond more effectively to future crime" (Pearsall, 2010, p. 16). The goal is to cast the data-gathering net as wide as possible to use "the power of big data to isolate patterns in otherwise random acts" (Ferguson, 2012, p. 266). Predictive policing has become a much-hyped model for police departments seeking to allocate resources more efficiently and to embrace the data-mining technologies that are transforming other spheres of social practice.

As the United States's most famous and self-promoting former police commissioner William Bratton put it, somewhat recursively, "Predictive policing used to be the future. . . . Now it is the present" (Black, 2016, para. 1). A dozen cities in the United States are currently using a commercially provided predictive policing platform, and there is research that indicates that the programs have been more effective at predicting and reducing crime than human analysts have (Black, 2016).

This apparent success underwrites the development of a postpanoptic model of surveillance that challenges historical expectations and understandings by displacing (or complementing) disciplinary forms of crime management and prevention with actuarial forms of surveillance directed toward the goal of preemption. Strategies of preemption shift the emphasis away from forms of monitoring associated with logics of causality and comprehension to the automated search for actionable correlations. If prevention invokes political discourses related to the underlying causes of criminality, preemption marks a turn toward statistical models of prediction and related forms of real-time intervention.

This shift has consequences for both policy discussions and the public's understanding of the role of police surveillance in the database era. Whereas once upon a time, those concerned about crime rates might have inquired into the societal and individual causes of violent or criminal behavior, the question now shifts in the direction of "Are there enough data to predict and preempt it?" The deflection is apparent in the pattern of post-9/11 law enforcement funding. The federal Local Law Enforcement Block Grant program, which once provided support for community crime prevention, saw its funding drop precipitously in post-9/11 era and was replaced completely in 2004 to make way for the Federal Justice Assistance Grant program, which focuses on equipment and training (Bauer, 2004). Midnight basketball programs gave way to the database and algorithm (as well as enhanced technologies for surveillance). The emerging emphasis is not so much on governing subjects as on finding ways to predict and preempt eruptions of violent or criminal behavior assumed to take place with some degree of regularity across the population. This shift coincides with a reconfigured role for surveillance.

Revisiting the Panopticon . . . Again

The movie *Minority Report* collided with the TV show *Person of Interest* for 22-year-old Chicagoan Robert McDaniel when a police officer showed up at his door one summer day to warn him not to get into trouble because the police were watching him. The warning was reportedly triggered by a predictive policing program used by the Chicago Police Department, a program that generated a "heat list" of "the roughly 400 people in the city of Chicago supposedly most likely to be involved in violent crime" (Stroud, 2014, para. 2). This heat list was generated by algorithms that incorporated historical crime information used to identify past hotspots of criminal activity as well as lists of everyone in the city who had been arrested for or convicted of a crime and information about the people with whom they were in contact.

The notion of a heat list conserves a familiar logic of policing while projecting it into the future. We might describe this logic as reliant on a targeted model of suspicion and surveillance. The goal is to narrow down a reasonably manageable list of suspects to streamline the surveillance process. As described in the media coverage, the heat list model also conserves what might be described as a

disciplinary model of policing (Foucault, 1979). The surveillance process announces itself to those being watched in the form of a warning: "You are being watched: Behave accordingly."

In this respect, the famous Foucaudian description of the panopticon prison in *Discipline and Punish* bears further examination: "The Panopticon is a machine for dissociating the see/being seen dyad: in the peripheric ring, one is totally seen, without ever seeing; in the central tower, one sees everything without ever being seen" (Foucault, 1979, p. 202). The panopticon refers to a plan for a prison in which a superintendent in a central tower monitors prisoners in individual cells arrayed in a circle around the tower. The tower is set up so that the superintendent can see out (into the prisoners' illuminated cells) while remaining hidden to the inmates. The latter cannot see whether they are being watched or not at any given time. The inmate may not see the superintendent in the central observation tower, but the tower plays the role of a constant reminder: It must be ever-present to the inmate's gaze. Therefore, as Reg Whitaker (2010) observes, the panopticon relies on the power of spectacle—it incorporates both panopticism (the few watching the many) and synopticism (the many observing the spectacle of the [gaze of the] few). It is not hard to generalize this claim in practice: Surveillance technologies that rely on the logic of discipline—the internalization of the monitoring gaze—always incorporate an element of the spectacle, a cue or clue that one is being watched. Small smoked Plexiglas domes scattered across the ceiling of a shopping mall, for example, signify the presence of a monitoring gaze. Agents of discipline have been known to make use of the signifiers of surveillance to replace actual monitoring. For example, an empty police car with a uniformed mannequin can serve as a speed trap to slow traffic (at least for awhile). Signs indicating the presence of surveillance cameras are meant to have the same effect as the cameras themselves. As Simon (2005) puts it, "What is important for Foucault's version of Bentham's plan is that the inmate be aware of the gaze of the supervisor through signs of their presence" (p. 11).

Discipline relies on the spectacle of surveillance because it mobilizes processes of internalization and subjectification. The goal of the monitoring apparatus is to compel the subject to work on him- or herself. As Simon (2005) puts it,

> At the very least then, the simple Panopticon presumes a population of rational actors who share a homogenous base of knowledge. . . . Under a purely structural-deterministic model, people who are blind, ignorant or irrational would be immune to the effects of panoptic power. (p. 16)

The panopticon is thus an economizing machine driven by a utilitarian conception of rational choice decision making, which is not surprising given its provenance. But we might push this argument a bit further along the lines traced by Simon (2005): The panopticon relies not simply on a particular conception of the subject but also on a well-functioning process of representation: the efficacy of the spectacle. Even the most rational of utility-maximizers face an impasse when it becomes impossible to derive a coherent message from the welter of available information. Discipline depends on both the ability to recognize the process of surveillance at work and to determine the imperatives represented by the monitoring gaze. In this regard, it postulates a subject who is willing and able to internalize these imperatives.

From *Columbo* to *Cops*

Preemption, by contrast, dispenses with these attributes of the subject, pushing beyond disciplinary models. Consider, for example Elayne Rapping's (2004) exploration of a shift in the televised representation of criminality that exposes the rise of incoherence as a policy. She draws on an analysis of crime dramas, arguing for their ideological role, "in maintaining social stability and the authority of the state" (Rapping, 2004, p. 218). Furthermore, she argues that shifts in representational forms and logics provide insight into changing societal understandings:

> When major shifts in the processes and policies that drive law enforcement systems occur, it is invariably television . . . that plays the most powerful role in "informing" the public of these shifts, and helping it to adjust, culturally and psychologically, to their implications. (Rapping, 2004, p. 220)

Rapping (2004) describes the rise of the reality show *Cops* in terms that invoke the failure of the logic of discipline and its reliance on the spectacle of surveillance. *Cops*, which follows police officers responding to calls in a range of metropolitan police districts in the United States, was the longest running show on the Fox Network (25 seasons). The show has moved to Spike TV, where it is currently in its 28th season. For Rapping, *Cops* marks the shift away from a disciplinary approach to criminality, one in which the figure of the criminal was

> transformed from a figure of essential evil to a subject of study for the new science of criminology, in which a "gentler way of punishment" for "docile bodies"—disciplined from birth to internalize and conform to the norms of society or feel guilt for the failure to do so—could be managed. (p. 221).

Disciplinary policies rely on the generation of knowledge-based reform practices that enlist the vocabulary of "deviance, delinquency, reform, and rehabilitation" (Rapping, 2004, p. 228) embraced by 20th-century discourses of sociology and criminology. By contrast, Rapping (2004) argues that *Cops* portrays a version of criminality that accords with what we might describe as emerging strategies of incoherence. In *Cops*, criminals are "incorrigibly 'other' and 'alien;' incapable of internalizing or abiding by the norms and values of a liberal democracy, for they are far too irrational, uncontrollable, and inscrutable for such measures to be effective" (Rapping, 2004, p. 227). The criminals portrayed on *Cops* are not figures who participate in the rational calculus inspired by the threat of surveillance and the specter of punishment: They come to represent the resurgence of the category of the undisciplinable. The very staging of the show emphasizes the obliviousness of the alleged criminals it portrays to the power of the monitoring gaze. They are on TV, and yet are unable or unwilling to "behave."

The postpanoptic approach to threat and risk becomes increasingly familiar in the post-9/11 era. As Rapping (2004) notes, the paradigmatic representative of a nonnarrativizable, ubiquitous threat is the terrorist:

> Like the terrorist, the criminalized other is an alien, an outsider, who poses a threat because they do not conform to our norms. Terrorists are irrational, inscrutable, and inherently violent. . . . And they cannot be "reformed" or "rehabilitated" according to traditional correctional methods because they neither recognize nor respect the codes to which such measures apply. (p. 225)

They also are not amenable to the disciplinary logic of the panopticon: to the calculus of surveillance and punishment.

The convergence of crime and terror around the presumed logic of an implacable and irrational threat results in lack of purchase of disciplinary approaches and their attendant forms of knowing (e.g., the detailed back story and the causal explanation). In the register of terrorism, for example, it is politically taboo to attempt to explain or to invoke the notion of causality: Such attempts are framed as either weak willed and weak minded or, even more disturbingly, justificatory. When State Department spokeswoman Marie Harf questioned U.S. policies of counterinsurgency by observing that "we cannot kill our way out of this war" while also calling for plans that "go after the root causes that leads people to join these groups" (Benen, 2015, para. 3), she was ridiculed by the political right for advocating "jobs for jihadis" (Gobry, 2015, para. 1). The notion that there might be structural and political explanations for spreading forms of insurgency was dismissed as the sign of a discredited "do-gooder" mentality: the attempt to transpose "liberal" attitudes toward crime and social inequality to the realm of terrorism. The moment was a telling one with respect to contemporary policies of incoherence insofar as the latter rely on the ongoing denigration of strategies of explanation and narratives of causation.

The "Becoming Environmental" of Surveillance

Advances in media technology and practice often migrate from the realms of warfare and security to that of the market, but in the case of predictive policing, the direction has been reversed. Law enforcement's interest in mathematical modeling and data mining migrated from the tech sector to the urban precinct in the first decade of the 21st century. This is not to say that crime data have not been incorporated regularly into policing practice, nor is it to overlook the role that policing played early on in techniques of measurement and pattern analysis (see, e.g., Sekula, 1986). Rather, it is to note a shift in the ways of thinking about and handling information inspired by developments in the tech industry, which developed in a relatively short time huge databases and the techniques and technology for putting these to use. If, once upon a time, the public sector had been the repository for most of the stored data in the world, the advent of the information economy resulted in a dramatic role reversal, one perhaps highlighted by an anecdote in *TIME* magazine about a surprise visitor to Facebook founder Mark Zuckerberg at his corporate headquarters. In the middle of one of Zuckerberg's meetings,

> The door opened, and a distinguished-looking gray-haired man burst in . . . trailed by a couple of deputies. He was both the oldest person in the room by 20 years and the only one wearing a suit. He was in the building, he explained with the delighted air of a man about to secure ironclad bragging rights forever, and he just had to stop in and

> introduce himself to Zuckerberg: Robert Mueller, director of the FBI, pleased to meet you. (Grossman, 2010, para. 3)

It is hard to read the encounter as anything other than a data groupie encounter: The FBI director was genuflecting before the master information aggregator, someone who could amass the most comprehensive profile of the daily life of users on an unprecedented scale by getting those users to do the work of providing the data themselves. Zuckerberg was the Tom Sawyer of data mining, figuring out how to get everyone else to do the work for him on an unprecedented scale. As subsequent revelations indicated, Mueller's fascination may well have been a practical one, given that security agencies have found ways to piggyback on the data collection practices of major players in the tech sector, including Google, Microsoft, and Facebook.

New technologies make it possible to collect and store huge amounts of data, but they also mark a change in the pragmatics of monitoring. If, once upon a time, intelligence agencies focused on individual targets, the focus has shifted to the population and the pattern. Data mining, as Gus Hunt, former chief technology officer of the Central Intelligence Agency once put it, relies on the collection of as many data as possible before particular suspects or risks are known and then using this information to help predict possible suspects and threats (Sledge, 2012). All data are potentially useful in this framework: "The value of any piece of information is only known when you can connect it with something else that arrives at a future point in time" (Sledge, 2012, para. 3). For Hunt speculative data collection requires comprehensiveness: "Since you can't connect dots you don't have, it drives us into a mode of, we fundamentally try to collect everything and hang on to it forever" (Sledge, 2012, para. 3). Such an approach adopts the logic of counterinsurgency described by Ben Anderson (2011): If threat is dispersed throughout the population, then monitoring must also extend "through life without limit" (p. 218).

Predictive policing, insofar as it relies on increasingly comprehensive forms of data collection, marks the moment when policing becomes "environmental" (Anderson 2011, p. 220). Perhaps one of the telltale precursors of this moment is the work of former Police Commissioner Bratton, who, in 1990s New York City, implemented a policy of zero-tolerance enforcement inspired by the "broken windows" thesis (Wilson & Kelling, 1982). This thesis might be described as *environmental* in the sense that it called for intervention not in the form of the management of particular individuals, but rather in shaping the context in which they operated. This "slippery slope" approach to policing postulated that seemingly minor symptoms of public neglect served as a gateway to more serious forms of neighborhood decline and an attendant rise in the rates of criminal activity (Harcourt, 2009). This "order-maintenance" approach was coupled with increases in funding for beat-walking police officers in an effort to couple the notion of community policing with a crackdown on minor infractions based on the premise that improving the neighborhood would win the support and assistance of its residents. Shortly after bringing this brand of policing to New York City, Bratton developed the prototype for subsequent forms of predictive policing, coupling "zero tolerance with a data-driven approach" called CompStat that uses "data analysis to identify crime hot spots, on the premise that allowing police to focus manpower will reduce crime rates" (Bartosiewicz, 2015, para. 13).

The development of this so-called intelligence-led policing fit with the goal of compensating for

tighter budgets with the promise of technology to assist in the more efficient allocation of resources. When Bratton moved to Los Angeles, he oversaw a collaboration with two University of California Los Angeles professors who had done predictive analytics for the U.S. military. The connection was a defining one insofar as it merged counterinsurgency techniques with policing, a trend that has marked a characteristic form of convergence in the post-9/11 era, when warfare has taken on elements of policing (no longer limited to defined times, spaces, and personnel of warfare) even as policing has adopted the approaches and tools of counterinsurgency (thanks in no small part to the transfer of military equipment from de-escalating combat zones in the Middle East). This convergence has been underwritten in part by the Urban Areas Security Initiative, which helped mobilize urban police for counterterrorism operations to the tune of more than $8 billion (Bartosiewicz, 2015). In this regard, Rapping's (2004) invocation of the figure of the terrorist to describe shifting configurations of criminality in the urban landscape proved prescient.

Such claims serve as the basis for predictive policing's economic model. PredPol is a for-profit initiative that makes its pitch to police departments based on the promise of reduction of crime rates through efficient allocation of resources. The promise adopts the logic of real subsumption: Police can be made more productive simply by informating the policing process more effectively. As Jeff Branthingham, the UCLA anthropology professor who helped develop PredPol, puts it,

> You're helping to optimize the precious time that police forces have . . . if you can take those limited resources and help them be just a little bit more efficient, which is really what this predictive policing and PredPol is all about, you can actually go long way with those small amount of optimizations. (Funnell, 2015, para. 16)

Policing as Counterinsurgency

As suggested by the image of the pin-covered map that served as the basis for intelligence-led policing, the emergence of criminal behavior becomes framed as "punctual" in the sense described by Ben Anderson (2011). He argues that, from the perspective of counterinsurgency, the target "only appears in punctual events of violence before disappearing again" (Anderson, 2011, p. 222), a temporality that suggests a reconfiguration of the civilian–criminal distinction. The risk of the eruption of criminality is seen as distributed probabilistically across the population, such that it might emerge at particular points in time and space with differential likelihoods. Thus, everyone gets a threat level assigned to them and everyone is folded in the pattern of monitoring and data capture. As Anderson puts it, "This means that the time outside of punctual events is not best thought of in terms of 'waiting.' . . . Instead, it is characterized by an intensification of attempts to know the population" (p. 222).

In the era of intelligence-led policing, surveillance becomes environmental, as suggested by the 2016 admission by U.S. National Security Director James Clapper that "In the future, intelligence services might use the [Internet of things] for identification, surveillance, monitoring, location tracking, and targeting for recruitment, or to gain access to networks or user credentials" (Ackerman & Thielman, 2016, para. 5). Shifting models of policing go hand in hand with emerging technological developments: It is the advent of a sensor society, in which the physical world becomes equipped with an interactive overlay that makes possible the extension of surveillance "throughout life without limit" (Anderson, 2011, p. 218). It is

not a coincidence that, at the moment when comprehensive monitoring becomes the goal, we are subjected to ongoing invitations to incorporate always-on information capture devices into our homes and workplaces.

The convergence between anticriminality and counterinsurgency is highlighted by Chamayou's (2015) description of the advent of post-9/11 militarism: "Antiterrorism, which is both moralizing and Manichean, abandons any real analysis of the roots of hostility and its own effects upon it" (p. 69). Perhaps the most tellingly familiar aspect of this observation comes in the latter half of the formulation: the refusal of allegedly preemptive responses to recognize their own complicity in reproducing the forms of violence to which they are ostensibly opposed. The issue is not simply that the "long-term" effects of preemptive strategy are not taken into consideration, but rather that any such debate is displaced by the immediacy of response called for by the imminence of the threat. Recall Barbara Boxer's allegiance—in the name of urgency—to policies that created the very threat they promise to manage. For Chamayou, one of the political casualties of the preemptive frame is politics. Whereas any alternative to pure preemption "implies (apart from brute force) compromise, diplomatic action, pressure, and agreements . . . antiterrorism excludes any political impact upon the conflict. 'We do not negotiate with terrorists' is the key phrase in radically nonstrategic thought" (Chamayou, 2015, p. 22). The hallmark of such an approach is the desubjectivization of the opponent that calls for the automation of response.

If the model of disciplinary power is the confessional, the space within which the subject provides an account of him- or herself, the icon of preemptive power is the smart city that dispenses with the "active" or subjectified aspect of interactivity (data monitoring becomes ubiquitous and passive). If the disciplinary goal is the spectacle of surveillance, the preemptive one is its disappearance through ubiquity. If surveillance is everywhere, it is no longer a discrete process, but the medium through which we move. Disciplinary surveillance can be partial, but must be known (to its targets). Postdisciplinary surveillance can be covert, but it must be comprehensive. This is not to say that postdisciplinary surveillance does not have disciplinary effects (surely, awareness of comprehensive monitoring could lead to the internalization of a monitoring gaze in some quarters), but rather to note that these effects are not its defining purpose. Such forms of monitoring are targeted precisely on those who are assumed to be impervious to disciplinary norms (terrorists and implacable, irrational criminality).

Similarly, if the object of disciplinary power is distinctly human in terms of its narrativized subjectivity, that of preemptive power can be assimilated to a range of "natural" forces. PredPol notoriously draws on earthquake-modeling techniques to predict recurring patterns of criminality. As PredPol's chief scientist puts it,

> Some of the models we use at PredPol are self-exciting point processes that were originally developed for modeling earthquake aftershock distributions. . . . The fact that these point process models fit earthquake and crime event data quite well is, by itself, a cool result. (Mohler, 2015, para. 5)

Other approaches to predicting street crime analogize gang activity to wolf pack behavior (Smith, Bertozzi, Brantingham, Tita & Valasik, 2012), further naturalizing and desubjectivizing the specter of criminality.

Such approaches highlight the disparity between disciplinary surveillance and environmental power. An earthquake cannot participate in ongoing logics of self-definition and self-disclosure; it remains foreign to processes of subjectification, as do the members of the wolf pack. In both cases, the most that can be done is to redouble nature so as to simulate its activities in ways that yield actionable knowledge. As Jeff Brantingham of PredPol puts it in his description of the mathematics of preemption,

> The naysayers want you to believe that humans are too complex and too random—that this sort of math can't be done . . . but humans are not nearly as random as we think. . . . In a sense, crime is just a physical process (quoted in Rubin, 2010, p. 10).

This formulation is a telling one: It highlights the physicality of crime in contradistinction to what? Its sociality or, perhaps, its subjectivity? From the perspective of the data mine, criminality as billiard-ball–like predictability, despite the conscious nature of the balls in question.

The promise of perfect preemption relies on what William Bogard (1996) describes as "the simulation of surveillance," the goal of which is not simply to map the environment, but to redouble it in the form of the model: "The imaginary—the impossible—of surveillance is perfect exposure. The imaginary of simulation is the perfect double. Finally, the imaginary of the simulation of surveillance is the perfect doubling of exposure" (p. 47). This progression is another way of describing a postsubjective realm in which the inconsistency or gap introduced by subjectivity is preempted through the "filling in" made possible by the totalization of environmental surveillance. The goal is an impossible one, but it is prefigured by the image of the "broken window" through which the advent of predictive policing traces its lineage.

Although predictive policing models tend to rely largely on historical patterns of crime data—and, in some cases, on scraping social media and other readily available personal data—the tendency that it traces pushes toward the inclusion of as broad a spectrum of information as possible. Surely, environmental factors might figure into criminological calculations (e.g., weather patterns and barometric pressure) but also biometric ones (discerned through the implementation of emerging forms of sensors, such as the Department of Homeland Security's pioneering efforts in the detection of "malintent" via the monitoring of body temperature, facial expression, pulse rate, and other signals) as well, of course, as genetic factors and eventually all available and imaginable forms of data collection and modeling. Research conducted in Finland, for example, discovered that people with two particular genes were "13 times more likely to have a history of repeated violent behavior" (Hogenboom, 2014, para. 3) than those who did not have the genes. Based on their sample, the researchers said that "at least 5–10% of all violent crime in Finland could be attributed to individuals with these genotypes" (Hogenboom, 2014, para. 3).

Researchers responding to these findings suggested that genetic makeup is just one factor among many to consider in anticipating criminal behavior. As one academic put it, although environmental influences are crucial, "it is worthwhile to look for biological contributions to criminal or antisocial behavior as their impact on individuals, communities and society in general is sizeable" (Hogenboom, 2014, para. 28). Genetics becomes one more factor in the "becoming environmental" of data collection, prediction,

and intervention. For example, a platform called HunchLab is expanding the reach of typical predictive policing programs to include, in addition to data on past criminal activity, factors such as "population density; census data; the locations of bars, churches, schools, and transportation hubs; schedules for home games—even moon phases" (Chammah, 2016, para. 7). According to one description of the application, whereas some correlations are to be expected, "Others are more mysterious: rates of aggravated assault in Chicago have decreased on windier days, while cars in Philadelphia were stolen more often when parked near schools" (Chammah, 2016, para. 7).

Such an approach takes on the speculative character of other data-driven strategies: Put in as much information as possible and see what types of correlations emerge. Because the goal is preemption and not explanation, there is no need to interpret the findings (e.g., by asking why assaults decrease when the wind increases): Simply allocate resources accordingly. As the CIA's chief technological officer might have put it, the goal is to collect as many dots as possible to see how they might be connected.

Conclusion: Pure Imminence

Common-sense understandings of monitoring practices have not necessarily kept pace with these postdisciplinary shifts. For example, one of the more intriguing aspects of the public debate triggered by the FBI's attempt to get the Apple Corporation to help it access data stored on the iPhone of one of the San Bernardino shooters was that it seemed to generate a more robust public response than Edward Snowden's revelations about the government's widespread monitoring of U.S. citizens. As *The New York Times* put it, "The Apple case already seems to have garnered more public attention than the Snowden revelations about 'metadata collection' and programs with code names like Prism and XKeyscore" (Shear, Sanger, & Benner, 2016, para. 20). Why might the public be more concerned about the attempt of law enforcement to access the phone of a known mass murderer than wholesale spying on the populace? The *Times* article speculated that "Because the issue now centers on a device most Americans carry in their pockets, it is concrete and personal in a way that surveillance by the National Security Agency never was" (Shear et al., 2016, para. 4). As Lee Rainie of the Pew Research Center put it, "It's an in-your-face proposition for lots more Americans than the Snowden revelation was" (quoted in Shear et al., 2016, para. 22). It is not entirely clear why the FBI accessing someone else's phone might be more "in your face" than the NSA accessing data about your phone and everyone else whom you have called. Perhaps more "in your face" refers to the fact that a team of investigators was surely getting ready to read and analyze everything they could find on the phone. This case was not one of impersonal machines scanning and sorting large quantities of data, but something more personalized: government agents reading through data otherwise accessible only to the phone's owner.

The public might in some ways still be more attuned to a disciplinary model of surveillance based on the compulsion of self-disclosure. This type of investigation looks more familiar and personal: the 21st-century version of investigators shaking down someone's home, rifling through their files, breaking down their doors, and sifting through their personal effects. People think of phones as their own, whereas they have come to understand circulating data as something already beyond their control, not so much something they own as something they provide.

However, there may be something more at work in the differential reception of these two apparently disparate types of state surveillance: a disconnect between the ways in which data miners and those who supply the data think about how they can be put to use. Data miners think in terms of pattern and correlation, whereas the "minees" think in terms of specific human audiences and their own life stories: who might be interested in the details of their lives and why. In this respect the differential reception of the two forms of monitoring represents the emerging disconnect between the scope and depth of different types of monitoring: the focused targeting of particular suspects versus the wholesale monitoring of an entire population associated with "environmental" forms of surveillance and preemption.

The advent of predictive policing marks one realm in which postpanoptic logics take shape, and thus serves as a useful site for considering the political consequences of the shift from discipline to preemption. The postpanoptic model of "total"—or environmental—surveillance envisions the possibility of capturing and processing tremendous amounts of data at speeds approaching real time (as events unfold). The goal of preemption, repeatedly invoked in discussions of predictive policing, is thus to intervene at the moment of (or immediately prior to) the eruption of criminal behavior. The fantasized perfection of prediction licenses compresses the timeframe for intervention: Long-term preventative measures are displaced by immediate preemption (immediate in the sense of coming just before the act). This shift in temporality has social and policy implications that flow from the tendency toward automation. The goal of ubiquitous, always-on surveillance emerges against the background of the failure of the disciplining power of the monitoring gaze (associated with the reframing of the figure of the terrorist/criminal from that of the knowable subject to that of the inscrutable force of nature). If subjects cannot be relied on to discipline themselves, then surveillance must become as comprehensive as possible. However, this level of monitoring requires automation of both data collection and data processing (and, eventually, of response).

The imperative of automation is also underwritten by the imminence of the threat, or rather by the reframing of any predicted risk as an imminent one: If it can be known, that is enough to render it actionable. This logic of pure imminence—whereby a growing range of future threats is collapsed into the present so as to be acted on immediately—is enabled by the fantasy of invulnerability associated with the figure of the drone. Absent invulnerability, acting on future threats requires a political calculus of risk. However, the combination of generalized imminence with automation diminishes the role for politics and diplomacy: The delay of deliberation is ruled out in the face of the imminent threat. At the same time, the competence of experts and everyday citizens is challenged by the generation of information so copious that it cannot be processed by any individual or group of individuals.

The concern raised by this essay is thus threefold: that the shift to predictive policing leads to a self-reinforcing spiral of preemption in which the failure to address underlying causes ever more comprehensive forms of surveillance, that the rhetoric of imminence combined with the goal of automation reduces the time and space for deliberation and causal analyses, and that public understanding has not yet caught up with the implications and consequences of these new forms of monitoring and surveillance. Postdisciplinary logics of monitoring have the somewhat ominous consequence of replacing the negotiation of competing causal claims with the direct, asymmetric, and ongoing application of preemption and its attendant forms of violence.

References

Ackerman, S., & Thielman, S. (2016, February 9). U.S. intelligence chief: We might use the Internet of things to spy on you. *The Guardian*. Retrieved from http://www.theguardian.com/technology/2016/feb/09/internet-of-things-smart-home-devices-government-surveillance-james-clapper

Anderson, B. (2011). Facing the future enemy: U.S. counterinsurgency doctrine and the pre-insurgent. *Theory, Culture & Society, 28*(7/8), 216–240.

Bartosiewicz, P. (2015). Beyond the broken window. *Harpers*. Retrieved from http://harpers.org/archive/2015/05/beyond-the-broken-window/

Baudrillard, J. (1994). *Simulacra and simulation*. Ann Arbor, MI: University of Michigan press.

Bauer, L. (2004). Local Law Enforcement Block Grant Program, 1996–2004 (Technical report). Washington, DC: Bureau of Justice Statistics.

Baxter, S. (2013, August 14). Santa Cruz predictive policing adds tool for cops, neighbors. *Santa Cruz Sentinel*. Retrieved from http://www.santacruzsentinel.com/article/zz/20130814/NEWS/130817547

Benen, S. (2015). We cannot kill our way out of this war. *MSNBC*. Retrieved from http://www.msnbc.com/rachel-maddow-show/we-cannot-kill-our-way-out-war

Black, D. (2016, March 18). Predictive policing is here now, but at what cost? *The Dallas Morning News*. Retrieved from http://www.dallasnews.com/opinion/sunday-commentary/20160226-david-black-predictive-policing-is-here-now.ece

Bogard, W. (1996). *The simulation of surveillance: Hypercontrol in telematic societies*. Cambridge, UK: Cambridge University Press.

Brown, H. (2013, May 8). Attorney general responds to Paul on drone strikes. Retrieved from https://thinkprogress.org/attorney-general-responds-to-paul-on-drone-strikes-1a0573e1d9e#.js4yxesom

Chamayou, G. (2015). *A theory of the drone*. New York, NY: New Press.

Chambers, S. (1996). *Reasonable democracy: Jürgen Habermas and the politics of discourse*, *Vol. 11*. Ithaca, NY: Cornell University Press.

Chammah, M. (2016). Policing the future. *The Verge*. Retrieved from http://www.theverge.com/2016/2/3/10895804/st-louis-police-hunchlab-predictive-policing-marshall-project

DemocracyNow.org. (2015, January 28). Sen. Barbara Boxer on campus rape bill, climate skeptics and why she supports Obama's war on ISIS. Retrieved from https://www.democracynow.org/2015/1/28/sen_barbara_boxer_on_campus_rape

Ferguson, A. (2012). Predictive policing and reasonable suspicion. *Emory Law Journal*. Retrieved from http://law.emory.edu/elj/_documents/volumes/62/2/articles/ferguson.pdf

Foucault, M. (1979). *Discipline and punish: The birth of the prison*. New York, NY: Vintage Books.

Funnell, A. (2015, August 23). Predictive policing: Putting data on the beat. *Future Tense* [Radio show]. Ultimo, Australia: ABC Radio National. Retrieved from http://www.abc.net.au/radionational/programs/futuretense/predictive-policing3a-putting-data-on-the-beat/6702640#transcript

Gobry, P. (2015, February 20). In partial defense of "jobs for jihadis" State Dept spokeswoman Marie Harf. *Forbes*. Retrieved from http://www.forbes.com/sites/pascalemmanuelgobry/2015/02/20/in-partial-defense-of-jobs-for-jihadis-state-dept-spokeswoman-marie-harf/#a96e39d34807

Grossman, L. (2010, December 8). Mark Zuckerberg. *TIME*. Retrieved from http://content.time.com/time/specials/packages/article/0,28804,2036683_2037183_2037185,00.html

Harcourt, B. (2009). *Illusion of order: The false promise of broken windows policing*. Cambridge, MA: Harvard University Press.

Hogenboom, M. (2014, May 15). Two genes linked with violent crime. *BBC News Online*. Retrieved from http://www.bbc.com/news/science-environment-29760212

Mohler, G. (2015). Predictive policing. *Data Science Weekly*. Retrieved from http://www.datascienceweekly.org/data-scientist-interviews/predictive-policing-george-mohler-interview

O'Donoghue, R. (2016, April 5). Is Kent's Predictive Policing project the future of crime prevention? *Kent Online*. Retrieved from http://www.kentonline.co.uk/sheerness/news/what-if-police-could-detect-93715

Pearsall, B. (2010). Predictive policing: The future of law enforcement? *National Institute of Justice Journal*, *266*, 8–19

Rapping, E. (2004). Aliens, nomads, mad dogs, and road warriors: The changing face of criminal violence on TV. In S. Murray & L. Ouellette (Eds.), *Reality TV: Remaking television culture* (pp. 214–230). New York: New York University Press.

Rubin, J. (2010, August 21). Stopping crime before it starts. *Los Angeles Times*. Retrieved from http://articles.latimes.com/2010/aug/21/local/la-me-predictcrime-20100427-1

Sekula, A. (1986). The body and the archive. *October*, 39 (Winter), 3–64.

Shear, M., Sanger, D., & Benner, K. (2016, March 13). In the Apple case, a debate over data hits home. *The New York Times*. Retrieved from http://www.nytimes.com/2016/03/14/technology/in-the-apple-case-a-debate-over-data-hits-home.html?_r=0

Simon, B. (2005). The return of panopticism: Supervision, subjection and the new surveillance. *Surveillance & Society*, *3*(1), 1–20.

Sledge, M. (2013, March 21). CIA's Gus Hunt on big data: We 'try to collect everything and hang on to it forever.' *The Huffington Post.* Retrieved from http://www.huffingtonpost.com/2013/03/20/cia-gus-hunt-big-data_n_2917842.html

Smith, L., Bertozzi, A., Brantingham, P., Tita, G., & Valasik, M. (2012). Adaptation of an ecological territorial model to street gang spatial patterns in Los Angeles. *Discrete and Continuous Dynamical Systems*, *32*(9), 3223–3244.

Stroud, M. (2014, February 19). The minority report: Chicago's new police computer predicts crimes, but is it racist? *The Verge*. Retrieved from http://www.theverge.com/2014/2/19/5419854/the-minority-report-this-computer-predicts-crime-but-is-it-racist

Whitaker, R. (1999). *The end of privacy: How total surveillance is becoming a reality.* New York, NY: The New Press.

Wilson, J. Q., & Kelling, G. L. (1982). Broken windows. In R. G. Dunham & G. P. Alpert (Eds.),,Critical issues in policing: Contemporary readings (pp. 395–407). Prospect Heights, IL: Waveland Press,

Wolpert, S. (2015, October 7). Predictive policing substantially reduces crime in Los Angeles during months-long test. *UCLA Newsroom*. Retrieved from http://newsroom.ucla.edu/releases/predictive-policing-substantially-reduces-crime-in-los-angeles-during-months-long-test