Article

Surveillance Capitalism and Platform Policing: The Surveillant Assemblage-as-a-Service

Thomas Linder

Queens University, Canada
thomas.linder@queensu.ca

Abstract

Based on empirical research on training webinars, interviews, and promotional material from Vigilant Solutions, this paper investigates the surveillance regime enabled by *platform policing*: the implementation of cloud-based platforms, designed and run by private corporations, that provide mass surveillance-driven simulations for a range of police operations, including predictive policing, targeted surveillance, and tactical and strategic governance. Building on Amoore's (2016) work on "cloud geographies," this paper argues that the platform model embodied by Vigilant Solutions involves multivalent processes of de- and reterritorialization in which new technological and datalogical spaces are formed and these erode older societal boundaries of private, public, and state. Specifically, Vigilant Solutions leverages its multi-sided platform business model through the deterritorializing, cloud-based concatenations of surveillant technologies. It then argues that the resultant reterritorialized cloud space, which is accessible through its Vigilant Investigative Centre (VIC) platform, fuses mass surveillance data from diverse private, public, and state sources in a simulated geography. Further, the VIC furnishes to law enforcement an array of data analytics that exploits this cloud geography to enable a boundary-crossing surveillance regime of association analysis and proximal suspicion.

Introduction

Since the early debates on "big data," embodied by the likes of boyd and Crawford (2012) and Mayer-Schönberger and Cukier (2013), investigations around the intersection of policing and surveillance have gained considerably in terms of nuance and complexity. The main thrust of the subsequent discussions centered around "predictive policing," its epistemological validity, and criminological implications (Bennett Moses and Chan 2016; Ferguson 2012, 2015, 2016; Joh 2016; Van Brakel and De Hert 2011; Van Brakel 2016). Others noted that big data had broader effects on policing, that its rationalities for vast data collection and analysis were driving an expansion of digital surveillance technologies, such as automatic license plate recognition (ALPR), biometrics, body-worn cameras, and open source or social media surveillance (OSINT) (Brayne 2017, 2018; Chan and Bennett Moses 2016, 2017; Ferguson 2017). At the same time, the convergence of big data and private corporations, dubbed "surveillance capitalism" (Zuboff 2015, 2019), grew as a crucial area of inquiry. Many of these corporations, such as Google, Uber, Facebook, or Amazon, deployed a different platform-based business model, or "platform capitalism," which combined surveillance capitalism with the renting of their platforms as services (Langley and Leyshon 2017; Lippert and Newell 2016; Pasquale 2016; Srnicek 2017a, 2017b). At the crossroads between platform-based surveillance capitalism and big-data policing lies platform policing: the implementation of cloud-based platforms, built and run by private companies, that provide mass surveillance-driven simulations for a range of police operations, including predictive policing, targeted surveillance, and tactical and strategic governance.

Linder, Thomas. 2019. Surveillance Capitalism and Platform Policing: The Surveillant Assemblage-as-a-Service. *Surveillance & Society* 17(1/2): 76-82.

<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](#)

Beyond this functionality, the platform-policing business models differ considerably with some maintaining ownership over the data; some retaining the data on their own servers; some offering both subscription-based models or outright ownership; some providing the hardware for free; and some selling or leasing the hardware.

This paper examines the case of Vigilant Solutions, whose business model I dub the surveillant assemblage-as-a-service. Drawing on empirical material from sales brochures, interviews, and demos gathered from Vigilant during the 2018 International Association of the Chiefs of Police convention as well as from training webinars Vigilant offers, this study argues that this surveillant assemblage as-a-service platform-policing model involves multivalent processes of de- and reterritorialization in which new technological and datalogical spaces are formed, thereby eroding established societal boundaries of private, state, and public. Specifically, it first argues that Vigilant Solutions leverages its multi-sided platform business model through the deterritorializing, cloud-based concatenation of surveillant technologies. Building on Amoore's (2018) work on "cloud geographies," it then argues that the resultant reterritorialized cloud space, which is accessible through the company's Vigilant Investigative Centre (VIC) platform, fuses mass surveillance data from diverse private, public, and state sources in a simulated geography. Further, the VIC furnishes an array of data analytics to law enforcement, which then exploits this cloud geography to enable a boundary-crossing surveillance regime of association analysis and proximal suspicion.

The Surveillant Assemblage-as-a-Service

At the heart of Vigilant Solution's business model lies its relationship with its sister company, Digital Recognition Network (DRN). DRN (n.d.) provides "Vehicle Location Data for Auto Lenders, Insurance Carriers and Recovery Professionals" by selling or renting automatic license plate recognition (ALPR)¹ cameras to private entities, such as repossession companies and shopping malls. While the private users can run watchlists against captured license plates, the time-stamped and geolocated recordings all belong to DRN / Vigilant Solutions and are stored in their cloud database called LEARN. In their promotional material, Vigilant Solutions claims that this ALPR database contains over 13 billion detections in the US and grows at a rate of 250 million a month. However, Vigilant Solution's role in this dyad makes this somewhat complicated. Vigilant Solutions is the law-enforcement side of the organization, although they now also market themselves to school security in conjunction with local law enforcement, and they describe themselves as "VaaS: video analytics-as-a-service." They sell, rent, or deliver, for free, ALPR and facial-recognition² cameras; and while the data are uploaded to LEARN, they belong to the law-enforcement agency (EFF 2016b, 2016a). The agency can choose whether to make these data available to other agencies, on a wholesale or individual basis; and according to research done by EFF and MuckRock, this is being done on a vast scale: over 200 agencies upload their data and, on average, they share it with 160 other entities and some with as many as 800 (Lipton and Maass 2018). A number of "open source" databases of mugshots (over 18 million) and license plates come to these data sources, as well as integration with the agency's own databases. Recently, they expanded their range of data sources and, thus, LEARN to include body-worn camera video data and a ballistics analysis tool called GunOps for geo- and time-stamping images of spent cartridge casings and matching the markings against existing records. Vigilant Solution's primary income model function is called the Vigilant Investigations Centre (VIC). A subscription fee provides access to its analytics suite. The VIC is "an AI-driven, investigative platform" to "integrate facial recognition, ALPR, ballistics analysis, crime gun mapping, and video data management into one central database."

Vigilant Solutions / NDR's business model is an almost archetypal exemplar of surveillance capitalism and platform capitalism. Zuboff (2015), in her seminal article, identified a number of key traits of surveillance capitalism; and while Vigilant Solutions is no Google, it certainly embodies the extractive logic of digital

¹ Willis, Koper, and Lum (2018) offer a look at the use of ALPR in law enforcement. For a more critical evaluation, and upon which this article will build, see Brayne (2017, 2018) and Joh (2016).

² For an excellent critical analysis of facial recognition technology, see Gates (2011).

accumulation Zuboff identifies (77). Leveraging its dyadic corporate structure as well as open source opportunities, Vigilant Solutions diverts data flows into its own cloud database and monetizes them. Given the variety of state and private institutions involved in this network of extraction, Vigilant Solutions, too, captures and fuses data from socio-politically different spaces, from schools to shopping malls and police lineups. While not quite as “agnostic” as Google, here, Vigilant Solutions performs the same socially expansive processes of “data, extraction and analysis” (Zuboff 2015: 78) that is driven by both the supply and the demand sides of its operation. In addition, Vigilant Solutions also exhibits many of the hallmarks of platform capitalism (Langley and Leyshon 2017; Pasquale 2016; Srnicek 2017a, 2017b). In keeping with the platform capitalism business model of engaging a multi-sided market and monetizing the resultant data flows, it coordinates “the network effects of ‘connectivity’” (Langley and Leyshon 2017: 13) in triplicate: not just between the economic actors involved but also between law enforcement agencies and within the agencies themselves. It is through this triple act of platform organization that Vigilant Solutions succeeds in building and monetizing a modular and highly flexible mass surveillance network for hire: the surveillant assemblage-as-a-service.

Surveillant Territorialization

Amoore (2018) argues that “the contemporary spaces of cloud computing exceed the territorial geographies of the location of data centres, becoming instead a novel political space of calculative reasoning” (12); it provides “the means to map and to make perceptible the geography of our world in particular ways” (6). She proposes a twofold geography of cloud computing that encompasses both the geopolitical spatiality of the data centers and the epistemology of the analytics these centers enable. Here, I wish to build on this approach by, first, investigating the ways in which Vigilant Solutions’ cloud-driven platform structure effects particular territorial shifts, in the form not of interlinked databases dotted around the globe but of networks of surveillance technologies. While Amoore (2018) speaks of the de- and reterritorialization of the cloud along geopolitical lines (8), Vigilant Solutions’ multi-sided cloud platform enables the concatenation of previously siloed surveillance networks and their extension deeper into new spaces, thereby deterritorializing established societal boundaries and reterritorializing the data on LEARN. The sociotechnical specificities of the networks thus created form the techno-spatial conditions of possibility for the epistemology and analytics provided in the VIC.

In a webinar ambiguously aimed at both law enforcement and school security officials, Vigilant Solutions pushed for the expansion of school security to include both an outer perimeter of ALPR cameras outside school grounds and an internal perimeter of facial-recognition cameras at “choke points” in buildings. In this design they display a multivalent de- and reterritorialization of school security space. Eerily reminiscent of “rings of steel” security architecture in which concentric rings of CCTV, material fortifications, patrols, and checkpoints were erected around the City of London in response to Provisional IRA bombings in the 1990s (Coaffee 2004; Coaffee and Wood 2006; Coaffee, Fussey, and Moore 2011), this penetration goes beyond “the border is everywhere” security scape thinking (Johnson et al. 2011) by leveraging the affordances of the cloud to not only concatenate facial recognition and ALPR technologies but also school security, the public area surrounding the school, and law enforcement in a single cloud space operated by Vigilant Solutions.

Vigilant Solutions’ “surveillant assemblage” (Haggerty and Ericson 2000)—their cloud-based platform that consists of heterogenous surveillance technologies, networked systems, databases, and users—expands by incorporating new territories and new assemblages. This dynamic of territorialization is driven by the watchlist rationality of 100% coverage and effectivity, an impossible goal that nonetheless demands constant expansion and integration with other assemblages and databases. Such an over-riding imperative, when coupled with the asymmetric knowledge involved in platform business models in which the various partners like schools and precincts are only dimly aware of each other, finally serves to occlude questions of the total spatial coverage and access of the whole Vigilant Solutions system itself. While issues of privacy and jurisdiction arise as well, the de- and reterritorialization implemented here create a new surveillant techno-space to which both Vigilant Solutions and the law enforcement agency involved gain epistemic

access, in this instance by piggybacking off school security needs. Vigilant Solutions and NDR intentionally feed these platform dynamics on scales far larger than a school. The demos of its investigative platform (VIC) indicate the collation of ALPR, facial recognition, as well as gunshot and ballistics data from both private, public, and state sources all across the United States. Through its platform business model of providing the surveillance technologies at low or zero cost and charging a subscription fee for access to LEARN and the VIC, it is rapidly expanding the surveillant techno-spaces from public roads to the private school grounds to which it has access. Indeed, the surveillant assemblage-as-a-service model induces further integration as expansion and sharing are sold as the logical consequence of its functionality, in which each subsequent addition is but an extra plug-in to the modular system. These overlapping logics of network effect drive the rhizomatic distension of the surveillant assemblage described by Haggerty and Ericson (2000). As they foresaw, platform policing enables the convergence of once discrete systems, thereby extracting data flows and rendering life digitally legible (606). However, this assemblage is not the horizontalizing, deterritorialized product of the omnidirectional surveillant desire they thought it might be. Instead, the surveillant techno-space is reterritorialized with new centers of hierarchical power from which highly differential relationships of access and control are determined. Although individual law enforcement agencies choose their levels of cooperation through their contracts, the surveillant assemblage-as-a-service reduces law enforcement to users; platform policing is then also one more front in the neo-liberalization of policing in which the boundaries of police power are also deterritorialized as their infrastructure is hollowed out and privatized. While the erasure of societal silos undoubtedly constitutes an expansion in police reach, it comes at the cost of the ostensible state monopoly over (surveillant) force.

Cartographies of Contact

Through this multi-party spatial creep, Vigilant Solution's platform-policing assemblage also enables the generation of new epistemological geographies of proximal suspicion. The modular, penetrating, and peripatetic network of ballistics cameras, facial-recognition cameras, and ALPR cameras timestamp and geolocate all data points and allow their mapping on Geographic Information System (GIS) interfaces in simulations of proximal suspicion. Demonstrating its claim that these data reveal "patterns, trends and associations," a representative at the International Association of the Chiefs of Police (IACP) conference provided the following hypothetical scenario. A gunshot is investigated, and the cartridge is found and geotagged in LEARN. ALPR cameras had recorded all vehicles in the vicinity at the time of the shooting, these are linked to the cartridge, thereby creating a suspicious pool of vehicles. Another shooting occurs, the ballistics match and a second pool of suspicious vehicles is created. A reoccurring vehicle is identified, and VIC draws on LEARN's historical ALPR database and calculates the most probable locations for the vehicle to be found. As some of the recent work on big data and policing (Brayne 2017, 2018; Chan and Bennett Moses 2017) has begun to indicate, the big data "myth" (boyd and Crawford 2012) of purely inductive, atheoretical, immanent, or correlational knowledge production (Amoore 2018; Aradau and Blanke 2015, 2016) has not manifested. Vigilant Solutions's system is exemplary in this respect: while it does provide preemptive surveillance and a partly correlational epistemology, the investigative practices the VIC offers are actually suspicion driven, using proximity in the surveillance-based GIS simulation (Graham 1998, 2013) as a measure by which to reduce the data load and enable further investigative work.

On the face of it, such inductive and deductive practices are not that dissimilar from older, pre-mass-surveillance methods. As Chan and Bennett Moses (2017: 303) have noted, new technologies tend not to cause major breaks in policing styles, and this case appears to be no different. The crucial difference, however, lies in the simulation: the GIS system that goes beyond basic mapping to not only include suspicions and projections about behavior, relationships, and spaces but also provides a virtual geographic interface through which analysts can operate and act upon the world.³ According to their brochures and training webinars, the VIC offers a whole suite of association analysis tools for generating suspicious

³ It is not surprising that a few days before the submission deadline, Vigilant Solutions was acquired by Motorola, another company at the forefront of platform policing surveillance simulations with their CommandCentral Aware technology.

connections between gunshots, vehicles, faces, locations, times, and cases. Analytics like “locate analysis,” “associate analysis,” or “common plate analysis” use the data pool in LEARN to retrospectively compute suspicious proximities to locations, people, and vehicles. Additional analytics like “virtual stakeout” and “mobile hit hunter” enable the same surveillance antecedently, tasking the simulation with a variety of trigger warnings for future proximities. In order for analytics of proximity and acts of induction and deduction to be possible, the data for the simulation must be preemptively collected. Thus, while the officer’s actions may be considered targeted surveillance, the platform itself requires mass, unwarranted surveillance. As Brayne (2017: 992-93) points out, two of the effects of big-data practices in policing are the lowering of thresholds for inclusion in databases and the increased incorporation of non-policing databases. This is the key change that platform policing ushers in: a vast background system of mass surveillance to generate GIS simulations for a posteriori targeted action—and it does so insidiously by partially out-sourcing the task of mass surveillance to a private company, which then offers the targeted access as a service in return.

The epistemic power of this surveillance regime relies on the mission-, function- and spatial creep of the network, dynamics which are further exacerbated by the multi-sided platform model. Vigilant Solutions / DRN have aggressively acquired new assemblages, integrating the GunOps ballistics surveillance and VideoBadge body-worn cameras in the last few months as well as collaborating with ParkMobile to further extend its civilian ALPR network. The geographic spread and data diversity directly condition the depth of the simulation, and the platform model is uniquely capable of acquiring new sources and repurposing them. Both the data and the technologies are rendered multivalent by the platform, serving different purposes, depending on the user. Vigilant Solutions capitalizes on the deterritorialization of technology and the reterritorialization of data in their cloud geography by leveraging this multivalence and exploiting the technological and datalogical network effects each user differentially experiences. As Srnicek (2017a: 45) argues, platform capitalism “has data extraction built into its DNA, as a model that enables other services and goods and technologies to be built on top of it, as a model that demands more users in order to gain network effects.” Vigilant Solutions is no different; the growth of the platform itself must logically take higher priority than the surveillance desires of law enforcement, and this introduces a critical dynamic into the structure and function of the surveillance apparatus. The GIS simulation LEARN and the VIC can generate, as well as the analytics of proximal suspicion they provide, are products of this surveillant assemblage-as-a-service. They not only draw their surveillance power from the platform-fueled creep but are also fundamentally shaped by it. This form of privatization not only affects the technological architecture but it also has epistemological ramifications for what is known. As critics of ALPR technology put it, “‘No Cost’ License Plate Readers Are Turning Texas Police into Mobile Debt Collectors and Data Miners” (Maass 2016). In this case, function (creep) could follow form, and platform policing is running the risk of entangling police and business to a novel degree.

Conclusion

This article set out to show that the emergence of cloud-based, privately developed and operated mass surveillance policing platforms has unleashed a set of structural dynamics that fundamentally affect the socio-politics of police surveillance. The Vigilant Solutions / DRN business model of the surveillant assemblage-as-a-service aggressively collects and integrates data across established societal boundaries. Its cloud-based corporate platform enables the concatenation of surveillance networks from distinct societal spaces and the aggregation of the data in LEARN. In so doing, it is deterritorializing institutional knowledge silos and reterritorializing them in the form of a privately developed surveillant simulation. The GIS simulation and the particular suite of association analytics available in the VIC generate a cloud geography of proximal suspicion that is based on the unwarranted preemptive mass collection and collation of data. Platform policing thus represents a problematic merger of big-data techniques with practices of targeted suspicion in which form, function, and access are primarily controlled by a corporate platform. Such a surveillant simulation as a key interface between police and public raises crucial epistemological and political questions about relations of power. It is not, I would argue, that the simulation risks losing contact

with the real, as Baudrillard suspected but rather the inverse: that life will start to conform to the desires and strictures of the simulation.

References

- Amoore, Louise. 2018. Cloud Geographies: Computing, Data, Sovereignty. *Progress in Human Geography* 42 (1): 4–24.
- Aradau, Claudia, and Tobias Blanke. 2015. The (Big) Data-Security Assemblage: Knowledge and Critique. *Big Data & Society* 2 <http://bds.sagepub.com/content/2/2/2053951715609066>.
- Aradau, Claudia, and Tobias Blanke. 2016. Politics of Prediction: Security and the Time/space of Governmentality in the Age of Big Data. *European Journal of Social Theory* 20 (3): 373–91.
- Bennett Moses, Lyria, and Janet Chan. 2016. Algorithmic Prediction in Policing: Assumptions, Evaluation, and Accountability. *Policing and Society* 28 (7): 806–22.
- boyd, danah, and Kate Crawford. 2012. Critical Questions for Big Data: Provocations for a Cultural, Technological, and Scholarly Phenomenon. *Information, Communication & Society* 15 (5): 662–79.
- Brayne, Sarah. 2017. Big Data Surveillance: The Case of Policing. *American Sociological Review* 82 (5): 977–1008.
- Brayne, Sarah. 2018. The Criminal Law and Law Enforcement Implications of Big Data. *Annual Review of Law and Social Science* 14 (1): 293–308.
- Chan, Janet, and Lyria Bennett Moses. 2016. Is Big Data Challenging Criminology? *Theoretical Criminology* 20 (1): 21–39.
- Chan, Janet, and Lyria Bennett Moses. 2017. Making Sense of Big Data for Security. *The British Journal of Criminology* 57 (2): 299–319.
- Coaffee, Jon. 2004. Rings of Steel, Rings of Concrete and Rings of Confidence: Designing Out Terrorism in Central London Pre and Post September 11th. *International Journal of Urban and Regional Research* 28 (1): 201–11.
- Coaffee, Jon, Pete Fussey, and Cerwyn Moore. 2011. Laminated Security for London 2012: Enhancing Security Infrastructures to Defend Mega Sporting Events. *Urban Studies* 48 (15): 3311–27.
- Coaffee, Jon, and David Murakami Wood. 2006. Security is Coming Home: Rethinking Scale and Constructing Resilience in the Global Urban Response to Terrorist Risk. *International Relations* 20 (4): 503–17.
- DRN. DRN Data License Plate Recognition Technology. <https://drndata.com/> [accessed November 12, 2018].
- EFF. 2016a. Vigilant Solutions Mou With City of Kyle. *Electronic Frontier Foundation*. <https://www.eff.org/document/vigilant-solutions-mou-city-kyle> [accessed November 20, 2018].
- EFF. 2016b. Vigilant Learn User Agreement. *Electronic Frontier Foundation*. <https://www.eff.org/document/vigilant-learn-user-agreement> [accessed November 20, 2018].
- Ferguson, Andrew Guthrie. 2012. Predictive Policing and Reasonable Suspicion. *Emory Law Journal* 62: 259–326.
- Ferguson, Andrew Guthrie. 2015. Big Data and Predictive Reasonable Suspicion. *University of Pennsylvania Law Review* 163 (2): 327–410.
- Ferguson, Andrew Guthrie. 2016. Policing Predictive Policing. *Washington University Law Review* 94 (5) : 1109–1189.
- Ferguson, Andrew Guthrie. 2017. *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement*. New York: NYU Press.
- Gates, Kelly A. 2011. *Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance*. New York: NYU Press.
- Graham, Stephen. 1998. Spaces of Surveillant Simulation: New Technologies, Digital Representations, and Material Geographies. *Environment and Planning D: Society and Space* 16 (4): 483–504.
- Graham, Stephen. 2013. Geographies of Surveillant Simulation. In *Virtual Geographies: Bodies, Space, and Relations*, edited by Mike Crang, Phil Crang, and Jon May, 140–57. New York: Routledge.
- Haggerty, Kevin D., and Richard V. Ericson. 2000. The Surveillant Assemblage. *The British Journal of Sociology* 51 (4): 605–22.
- Joh, Elizabeth E. 2016. The New Surveillance Discretion: Automated Suspicion, Big Data, and Policing. *Harvard Law & Policy Review* 10: 15–34.
- Johnson, Corey, Reece Jones, Anssi Paasi, and Louise Amoore. 2011. Interventions on Rethinking ‘the Border’ in Border Studies. *Political Geography* 30 (2): 61–69.
- Langley, Paul, and Andrew Leyshon. 2017. Platform Capitalism: The Intermediation and Capitalisation of Digital Economic Circulation. *Finance and Society* 3 (1): 11–31.
- Lippert, Randy K., and Bryce Clayton Newell. 2016. Introduction: The Privacy and Surveillance Implications of Police Body Cameras. *Surveillance & Society* 14 (1): 113.
- Lipton, Beryl, and Dave Maass. 2018. EFF and Muckrock Release Records and Data From 200 Law Enforcement Agencies’ Automated License Plate Reader Programs. <https://www.eff.org/pt-br/deeplinks/2018/11/eff-and-muckrock-release-records-and-data-200-law-enforcement-agencies-automated/Users/Tom/Zotero/storage/CP63CHWK/eff-and-muckrock-release-records-and-data-200-law-enforcement-agencies-automated.html>
- Maass, Dave. 2016. “No Cost” License Plate Readers Are Turning Texas Police into Mobile Debt Collectors and Data Miners. <https://www.eff.org/pt-br/deeplinks/2016/01/no-cost-license-plate-readers-are-turning-texas-police-mobile-debt-collectors-and/Users/Tom/Zotero/storage/TNC6P3SC/no-cost-license-plate-readers-are-turning-texas-police-mobile-debt-collectors-and.html>.
- Mayer-Schönberger, Viktor, and Kenneth Cukier. 2013. *Big Data: A Revolution That Will Transform How We Live, Work, and Think*. London: Houghton Mifflin Harcourt.
- Pasquale, Frank. 2016. Two Narratives of Platform Capitalism. *Yale Law & Policy Review* 35 (1): 309–318.
- Smicek, Nick. 2017a. *Platform Capitalism*. New York: John Wiley & Sons.

- Srnicek, Nick. 2017b. The Challenges of Platform Capitalism: Understanding the Logic of a New Business Model. *Juncture* 23 (4): 254–57.
- Van Brakel, Rosamunde. 2016. Pre-Emptive Big Data Surveillance and Its (Dis) Empowering Consequences: The Case of Predictive Policing. In *Exploring the Boundaries of Big Data*, edited by Bart van der Sloot, Dennis Broeders, and Erik Schrijvers, 117–41. Amsterdam: Amsterdam University Press.
- Van Brakel, Rosamunde, and Paul De Hert. 2011. Policing, Surveillance and Law in a Pre-Crime Society: Understanding the Consequences of Technology Based Strategies. *Technology-Led Policing* 20: 165–92.
- Willis, James J., Christopher Koper, and Cynthia Lum. 2018. The Adaptation of License-Plate Readers for Investigative Purposes: Police Technology and Innovation Re-Invention. *Justice Quarterly* 35 (4): 614–38.
- Zuboff, Shoshana. 2015. Big Other: Surveillance Capitalism and the Prospects of an Information Civilization. *Journal of Information Technology* 30 75–89.
- Zuboff, Shoshana. 2019. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: Public Affairs.