Smart Security Cameras: The Corporatization of the Surveillant Assemblage

Yasmin McDowell

Abstract

Using a political economy approach, this paper considers how home smart security cameras function as part of the surveillance-industrial complex and strengthen the relationship between law enforcement agencies and multinational technology companies for the benefit of private interests. This dynamic is maintained by the surveilled citizens themselves, who finance the smart security camera industry and participate in a culture of surveillance. The concepts of *surveillant assemblage* and *panoptic surveillance* will be used to ground these claims. This paper will reference scholarly articles and news pieces about Amazon Inc.'s Ring doorbell to illustrate two important consequences of the proliferation of smart security cameras: the outsourcing of policing and the shaping of consumer behavior.

Keywords: surveillance, political economy, smart security cameras, policing, Big Tech

Introduction

In the past decade, smart security cameras have gone from being a novel invention to a household staple in millions of homes around the world. This paper argues that their proliferation empowers multinational companies by strengthening their relationship with law enforcement agencies and streamlining their ability to influence and police citizens in a manner that aligns with corporate interests. Smart security cameras thus do not function for the benefit of the citizens they ostensibly protect. Instead, the latter are led to purchase the very devices that allow them to be policed for private profit.

This paper will draw on the concepts of *surveillant assemblage* and *panoptic surveillance* to build a theoretical framework within which to understand the distribution of smart security cameras. Scholarly articles will be used to illustrate two important consequences of their distribution: the outsourcing of policing and the shaping of consumer behaviour. This paper will make frequent reference to Amazon Inc. due to their well-documented expansive commercial interests and the popularity of their smart security camera, the Ring Doorbell. Finally, we will consider how machine learning methods used on smart security camera data may further disadvantage marginalized groups.

Definitions

Until recently, “security cameras” and “closed-circuit television cameras” were used interchangeably. Closed-circuit television cameras (CCTV) refer to recording devices that transmit footage to defined locations as opposed to broadcast on air. They may be installed on private or public property, and can have visual, audio, or thermal recording capabilities (Caught on Camera, 2019). Mass CCTV networks have been used by property owners and law enforcement agencies since the late 1980s and can be considered precursors to today’s “smart” security camera systems (Goold, 2004, p. 2). This paper will draw on scholarship about CCTV to inform our understanding of smart security cameras, which have only been widely used since the early 2010s.

A camera is considered “smart” if it can connect and interact with its user and other smart devices, typically through a wireless internet connection. Popular smart security cameras include the Ring Doorbell (owned by Amazon), the Nest Hello (owned by Google’s parent company Alphabet), and the Arlo Pro (owned by Arlo Technologies). These inconspicuous cameras allow homeowners to communicate with and record visitors remotely via synchronized devices such as smartphones, tablets, or laptops.

Throughout this paper, we will be commenting on the relationship between commercial entities and law enforcement. The term “law enforcement agency” will broadly refer to any police department, sheriff’s department, district attorney, transit authority, university or college

campus police, and the Department of Justice (California State Legislature, 2019). Accordingly, “law enforcement officer” will refer to an officer, deputy, employee, or agent of a law enforcement agency.

Finally, the term surveillance is broadly understood to mean “the careful watching of someone” (Collins, 2019). This understanding stems from the direct translation of the French verb “surveiller” which means “to watch”. Today, surveillance is a nebulous term loaded with cultural specificity. In this paper, we will borrow from the work of surveillance scholar Christian Fuchs, whose article “How Can Surveillance Be Defined?” describes surveillance as “the collection of data on individuals or groups that are used so that control and discipline of behaviour can be exercised by the threat of being targeted by violence” (Fuchs, 2010, p. 11). This violence can be psychological, structural, or physical (Fuchs, 2010, p. 12). Other scholars may choose a more neutral definition of the term; however, we have selected this one since it accurately depicts how smart security cameras have been utilized in recent years.

Theoretical Framework

While potentially outdated, Michel Foucault’s interpretation of Jeremy Bentham’s panopticon model helps us understand surveillance as a tool for self-discipline. In the late 18th century, Bentham designed a prison where cells would face inward towards a central dark guard tower (McMullan, 2015). A light would shine out at the cells in order to maximize the visibility of inmates. Since prisoners would be unable to determine whether they were being watched, the expectation was that they would behave properly at all times. This structure would theoretically train prisoners to internalize lawful behaviour indefinitely and become good citizens when they returned to society. Writing in the 20th century, Foucault argued that this model of surveillance exists outside the prison in other disciplinary institutions such as factories, hospitals, militaries, and schools (Haggerty & Ericson, 2000, p. 607).

While panoptic surveillance was a useful model for understanding 18th and 19th century institutions, surveillance scholars Kevin Haggerty and Richard Ericson argue that digital surveillance is better understood through the ontological framework of *assemblage*. Gilles Deleuze and Felix Guattari (1980) originally conceived of the theory of assemblage to describe the world as a multiplicity of heterogeneous objects that flow and function together (Haggerty & Ericson, 2000, p. 608). These discrete flows may involve people, signs, knowledge, and institutions. An important distinction between the assemblage and panopticon models are that the latter is a top-down model within a closed system, whereas the former is composed of entities that are emergent and unstable (Haggerty & Ericson, 2000, p. 609). Since the surveillant assemblage does not have fixed boundaries, traditional political strategies cannot simply prohibit one “particularly unpalatable technology” without creating a ripple effect to other components within the assemblage (Haggerty & Ericson, 2000, p. 609). Further, these flows allow law enforcement agencies to increase their surveillance capacity by integrating computer

systems and databases across state and non-state institutions (Haggerty & Ericson, 2000, p. 610). Taking another metaphor from Deleuze and Guattari, Haggerty and Ericson (2000) argue that within the surveillant assemblage there is a *rhizomatic* leveling of the hierarchy which means “groups which were once previously exempt from routine surveillance are now increasingly being monitored” (p. 606).

Today there is not one guard tower that looks out onto a defined group of criminals, but millions of smart security cameras that look out onto any number of citizens. Whereas inmates knew they were being watched, pedestrians are not always aware that they are passing through a camera's frame of vision. As people discover the ubiquity of smart security cameras, they may begin to assume hidden watchmen in their midst; surveillance is thus extended from homes to the general public.

Outsourcing Policing

The intended purpose of security cameras is to prevent or provide evidence of theft, assault, and vagrancy (Goold, 2004, p. 3). While traditionally the tools of big banks and shopping mall owners, security cameras are now available for use by the average homeowner and storekeeper. *Smart* security cameras are particularly useful as they allow for two-way communication: property managers can monitor their premises from a smartphone to welcome or threaten anyone trying to enter. Two smart security devices dominate the North American market: Google's Nest and Amazon's Ring. Nest Cams can be synchronized with other Google products, allowing users to “scare off intruders or have a conversation with [their] family” (Google, 2019). Ring products are generally cheaper, ranging from \$59-199, and include smart cameras, doorbells, lighting, and accessories to “cover every corner. Inside or out” (Ring, 2019b).

Website pitches aside, Lauren Smiley (2019) offers a useful case study on how these devices are used and by whom. In an article for *The Atlantic*, Smiley describes how a Nest Cam caught an African American woman stealing an Amazon package in Potrero Hill, San Francisco. A neighbour then posted a “wanted-style” picture of her on the app Nextdoor, and soon every wealthy Nest owner in her community began monitoring her. Over the course of the following year, she was drawn into a “vortex of smart-cam clips, Nextdoor rants, and cellphone surveillance that would tug at the complexities of race and class relations in a liberal, gentrifying city” (Smiley, 2019). The subject eventually ended up losing custody of her daughter and was sentenced to rehab. While this dramatic outcome is not solely a result of the Nest footage, it is an example of how these high-tech devices only target one type of perpetrator: those who are desperate enough to commit a crime in the open (Smiley, 2019). Smart security cameras do not combat costly white-collar crime, but petty crime by people dealing with poverty who live alongside the wealthy (i.e. who live in gentrified neighbourhoods). In an assessment of the crime-reduction capabilities of public CCTV cameras, Hille Koskela (2000) similarly observed that CCTV had little effect on violent crime but did reduce property crime such as theft or burglary

(p. 246). In these situations, security cameras do not provide safety for the whole community as they are marketed to do, but instead exacerbate class tensions by disproportionately benefitting property owners in gentrifying areas.

A noteworthy characteristic of this crime story is that evidence was produced entirely by Nest owners via Nextdoor, not law enforcement officers on patrol. Nextdoor is a Google-owned app that allows users to report crime and help each other after natural disasters (Ring, 2019a). Customer reviews also suggest that the app makes them feel safer and more connected to their neighbours. The irony is that security cameras are usually installed so that crimes can be caught *without* the need for human witnesses. Writing in the early 2000s, Benjamin Goold observed that CCTV cameras allowed police to depend less on the goodwill and cooperation of the community and more on “techno-policing” (Goold, 2004, p. 6). Techno-policing leans on surveillance devices instead of communication with witnesses, perpetrators, or victims of crime. In the case of CCTV cameras, law enforcement agencies and private companies install cameras themselves, whereas in the case of smart security cameras, citizens are encouraged to purchase, install, and maintain them alone. Regular citizens have become a more critical component of the surveillant assemblage than they were in the late 20th century because smart technology has turned them into the financiers, custodians, detectives, and subjects of the surveillance process. Once customers have laboured in these roles, their data is uploaded to Google or Amazon’s cloud servers so that private companies and law enforcement can take care of matters from there, if they so choose.

Cooperation between Ring and law enforcement agencies is evident in cities across the United States, and to a lesser extent in Canada (CBC News, 2019). As of late 2019, over 500 American police departments have partnered with Ring to improve public safety (Smiley, 2019). A representative of the Electronic Frontier Foundation points out that far from protecting the public, these products only protect affluent communities who can afford Ring devices (Smiley, 2019). Partnerships often contain quid pro quo agreements where Ring provides a discount on their products and the law enforcement agency subsidizes them. Some subsidies are drawn from taxpayer money, thus further disadvantaging everyday citizens for the benefit of wealthy homeowners (Haskins, 2019). Similarly, while Nest does not have a known partnership with law enforcement, it has provided user data in around 25 percent of subpoenas that have been submitted to them (Smiley, 2019). Large technology companies have thus joined the business of policing under the auspices of law enforcement and the public purse.

Clarity regarding the consequences of this partnership can be gained by understanding the surveillance-industrial complex. In the Routledge Handbook of Surveillance Studies, Ben Hayes (2012) writes that “the surveillance-industrial complex provides a framework for analyzing [...] the wider implications of the burgeoning relationship between the state and the surveillance industry for governance and democracy” (p. 167). Within today’s surveillant assemblage, law enforcement agencies have access to the databases of insurance companies, financial institutions, state departments, telecommunications companies, marketing firms, public schools, and now smart security camera companies (Haggerty & Ericson, 2000, p. 617).

Should these databases become fully interoperable, one could attain “full spectrum dominance” over all aspects of an individual’s life (Hayes, 2012, p. 170). Within the surveillance-industrial complex, it is private actors who profit most from their relationship with state actors (Hayes, 2012, p. 167). This can be seen in the case of Ring, where subsidies from police departments led to high sales for Amazon (Haskins, 2019). This is also evident when government agencies contract private companies to develop security technology, but then still have to purchase the technology once it is developed (Hayes, 2012, p. 170).

Shaping Consumption

Not only do technology companies profit from the sale of their products, but they can use the data captured *by* said products to sell *more* products and services. Herein lies two important distinctions between CCTV and smart cameras. Unlike CCTV distributors, smart camera companies sell other smart products as well. This means they are motivated to collect information about customers in order to continue profiting off them after the sale of the initial item. Additionally, they often control multiple levels within their supply chain. For instance, Amazon owns the product (Ring Doorbell), the accompanying app (Neighbors), the facial recognition software (Rekognition), and the online retailer (Amazon.com). This provides them with *carte blanche* to sell products as they wish, instead of cooperating with competitors with diverse values and considerations.

Amazon has always understood that consumer data will allow them to predict and influence long-term consumption. When the company was founded in 1994, its explicit mission was to sell cheap books to gather data on affluent, educated shoppers (Packer, 2014). Unable to compete with Amazon’s low prices, smaller bookstores closed all around the world. Since 1994, the company has continued the practice of predatory pricing, meaning “selling goods below cost to drive out competition,” to dominate the book, toy, and electronics industries (Mitchell, 2018). They have also become a leading provider of cloud computing services, with Amazon Web Services hosting data for Netflix, Nordstrom, and the CIA among others (Mitchell, 2018). An article in *The Nation* titled “Amazon doesn’t just want to dominate the market - it wants to become the market” argues that multinational technology companies are “moving away from a democratic political economy, in which commerce takes place in open markets governed by public rules” (Mitchell, 2018). Amazon’s growing vertical control of markets and its capacity to collect vast amounts of data allows it to shape economic behaviour in favour of their goods and services. A monopolization of the security economy would thus lead to a corrosion of our democratic freedom of choice.

In addition, tools for economic surveillance and data extraction are often used without explicit consent. Julie Cohen (2016) argues that “within the political economy of informational capitalism, commercial surveillance practices are tools for resource extraction” (p. 213).

Surveillance companies see the public domain as a resource to be extracted for profit, rendering public spaces a “construct through which political-economic power is exercised” (Cohen, 2016, p. 215). While smart camera owners willingly purchase their devices, there is no consent mechanism for pedestrians who walk by the cameras. Those who look into a Ring Doorbell are often unaware that their image may be shared with various entities within the surveillance-industrial network. Cohen observes that consent is “redefined as a status that attaches at the moment of marketplace entry,” meaning pedestrians hand over their likeness the moment they walk through a surveilled neighbourhood (p. 220). While many smart security cameras have two-way communication capabilities that allow visitors to communicate with owners, the former cannot communicate with the entity that holds their personal information (i.e. Google, Amazon). Therefore, smart security cameras can be considered a sign that the rhizomatic leveling of hierarchy theory is outdated; we are returning to a hierarchical model of surveillance with corporations at the top and average citizens at the bottom. Within this model, stylish security cameras are the messengers that capture and feed our data up to the top.

Camera Footage Analysis

Finally, we will briefly address the analysis of security camera footage to further illustrate how citizens produce the labour required for private companies to police them and influence their consumption. One way in which security camera footage is analyzed is through crowdsourcing, which refers to a process where non-professionals engage in a collaborative project for little to no financial compensation (Trottier, 2014, p. 611). Daniel Trottier (2014) observed that in the mid-2000s, private companies began crowdsourcing their CCTV recordings to achieve greater surveillance of social life at a minimal cost. He noted that crowdsourced surveillance paradoxically “represents distribution and diffusion of control, yet it is also a greater concentration of surveillance-based control” (Trottier, 2014, p. 610). In the case of Ring and Nest, Amazon and Google have distributed their devices across households and crowdsourced their customers to analyze their data through sleek neighbourhood watch apps. However, these companies remain in control of the information, as it is hosted on their cloud services. Since app users lack professional training, their “analysis” can exacerbate discriminatory practices that have already been identified with professional security camera operators (Trottier, 2014, p. 613).

Discrimination is an ongoing question in the field of machine learning, a popular method of sorting through extensive video footage using algorithms, which are more efficient than human workers and not bound by labour laws. Whereas panoptic surveillance depended on a human watchman, today we rely on machines such as smart security cameras to make sense and react to subjects’ behaviour (Haggerty & Ericson, 2000, p. 610). While the internal designs of Ring and Nest are not publicly available, they may function similarly to other security camera companies that use machine learning methods. Since 2006, the company IC Realtime has used natural language processing to provide security cameras with effective search functionality,

meaning that users can query “man with red hat” to recall clips of any man in a red hat who has passed by. IC Realtime even hopes to develop technology that can predict fights, and aims to support video technology globally (IC Realtime, 2019). Similarly, Boulder AI sells DNNCam to government organizations and aims to implement “automated observation without barriers to implementation” (Boulder AI, n.d.). This begs the question of whether a democratic process should be considered for determining whether the spread of these cameras in public space is desirable. The Chinese government has been widely accused of human rights abuses due to their use of machine learning-powered cameras to monitor Uighurs in Xinjiang province (Vincent, 2018). Similarly, the Russian government has implemented a system of cameras that covers 90 percent of Moscow’s apartment entrances (Vincent, 2018). In North America, Nest and Ring are beginning to cover as much ground as these repressive governments, although in a manner that is supposedly consensual because consumers are the ones installing them. As computer vision and gait recognition technology improves, Amazon and Google will be able to identify even the most privacy conscious individuals and target them accordingly.

The California State Legislature recently passed a bill to ban the use of facial recognition technology (FRT) on police-worn body cameras on the basis that “requiring every person to show a personal photo identification card at all times is in violation of recognized constitutional rights” (California State Legislature, 2019, sec. 1C). In particular, the bill states that FRT disproportionately impacts the civil rights and liberties of people in highly policed communities and discourages those with unpaid fines from seeking police assistance or assisting police (sec. 1F). While this bill focuses on police-worn body cameras, it raises the question of whether similar laws should be considered regarding smart security cameras.

Conclusion

California’s recent anti-FRT bill is evidence that government bodies are considering the negative social impacts of new surveillance technologies. This will be increasingly important as smart security cameras spread across neighbourhoods and Amazon develops more partnerships with law enforcement agencies. As we wait for government bodies to reconsider their private partnerships and draft protective regulations, privacy conscious citizens have developed alternative means of staying secure. For instance, a recent article called “How to Give Ring and Nest the Boot and Set up Your Own Home Security Camera” provides tips on where to source hardware and set up a closed security network (Nield, 2019). Without 24/7 customer service, setting up a homemade network is time consuming; however, it is customizable and gives owners sole access to the information captured.

While smart security cameras are marketed as a means of empowering communities, they have in fact siphoned power away to select multinational technology companies. Those of us who support them, whether by purchasing cameras or subscribing to their other services, must be aware of our role as both the financiers and subjects of an increasingly corporate surveillant

assemblage that does not improve safety for all. Furthermore, should these companies overtake the security camera market, existing security infrastructures will be displaced and law enforcement agencies will have no choice but to partner with the likes of Amazon and Google on their conditions. We must reflect on who should manage our safety: law enforcement agencies, multinational technology companies, a combination of both, or an alternative option? While law enforcement agencies are far from perfect, they are at least mandated to protect us and are beholden to citizens through legislation. In contrast, Google and Amazon are for-profit companies who can hide their practices as trade secrets, all the while monitoring our most private spaces.

Works Cited

- Ball, K. (2002). The Labours of Surveillance. *Surveillance & Society*, 1 (2), 125-137. Retrieved from <https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/3349>
- Boulder AI. (n.d.) Solutions. *Boulder AI*. Retrieved from <https://www.boulderai.com/solutions/>
- California State Legislature. A.B. No. 1215. (2019). Retrieved from https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB1215
- Caught on Camera. (2019). What are the different types of CCTV camera? *Caught on Camera*. Retrieved from <https://www.caughtoncamera.net/news/different-types-of-cctv/>
- CBC News. (2019, December 11). RCMP reveal they've been working with Amazon to catch thieves with bait packages. *CBC*. Retrieved from <https://www.cbc.ca/news/canada/british-columbia/prince-george-rcmp-amazon-catch-thieves-bait-packages-1.5393279>
- Cohen, J. (2016). The biopolitical public domain: the legal construction of the surveillance economy. *Philosophy and Technology*. 31 (2), 213–233. Retrieved from <https://search-proquest-com.myaccess.library.utoronto.ca/docview/2087965791?accountid=14771>
- Collins. (2019). Surveillance. *Collins Dictionary*. Retrieved from <https://www.collinsdictionary.com/dictionary/english/surveillance>

- Dwoskin, E. (2018, May 22). Amazon is selling facial recognition to law enforcement - for a fistful of dollars. *The Washington Post*. Retrieved from <https://www.washingtonpost.com/news/the-switch/wp/2018/05/22/amazon-is-selling-facial-recognition-to-law-enforcement-for-a-fistful-of-dollars/>
- Fuchs, C. (2010, October 1). How Can Surveillance Be Defined? Remarks on the Theoretical Foundations of Surveillance Studies. *The Institute for a Global Sustainable Information Society*. 1-22. Retrieved from <http://www.sns3.uti.at/wp-content/uploads/2010/10/The-Internet-Surveillance-Research-Paper-Series-1-Christian-Fuchs-How-Surveillance-Can-Be-Defined.pdf>
- Goold, B. (2004). *CCTV and Policing: Public Area Surveillance and Police Practices in Britain*. Oxford: Oxford University Press.
- Haggerty, K. & Ericson, R. (2000). The Surveillant Assemblage. *British Journal of Sociology*. 51 (4), 605-622.
- Haskins, C. (2019, August 2). US cities are helping people buy Amazon surveillance cameras using taxpayer money. *VICE Motherboard*. Retrieved from https://www.vice.com/en_us/article/d3ag37/us-cities-are-helping-people-buy-amazon-surveillance-cameras-using-taxpayer-money?xyz
- Hayes, B. (2012). The surveillance-industrial complex. In K. Ball, K. Haggerty, D. Lyon (Eds.), *Routledge Handbook of Surveillance Studies* (pp. 167-175).
- IC Realtime. (2019). Product Catalog. *IC Realtime*. Retrieved from <https://www.icrealtime.com/docs/IC-Realtime-Catalog.pdf>
- Koskela, H. (2000). 'The gaze without eyes': video-surveillance and the changing nature of urban space. *Progress in Human Geography*, 24(2), 243-265.
- Lyon, D. (2018). *The culture of surveillance: watching as a way of life*. Cambridge, UK: Polity Press.
- McMullan, T. (2015, July 23). What does the panopticon mean in the age of digital surveillance? *The Guardian*. Retrieved from <https://www.theguardian.com/technology/2015/jul/23/panopticon-digital-surveillance-jeremy-bentham>

- Mitchell, S. (2018, February 15). Amazon doesn't just want to dominate the market - it wants to become the market. *The Nation*. Retrieved from <https://www.thenation.com/article/amazon-doesnt-just-want-to-dominate-the-market-it-wants-to-become-the-market/>
- Packer, G. (2014, February 9). Cheap Words. *The New Yorker*. Retrieved from <https://www.newyorker.com/magazine/2014/02/17/cheap-words>
- Paul, K. (2019, August 30). Amazon's doorbell camera Ring is working with police - and controlling what they say. *The Guardian*. Retrieved from <https://www.theguardian.com/technology/2019/aug/29/ring-amazon-police-partnership-social-media-neighbor>
- Ring Inc. (2019a). Neighbors. *Ring*. Retrieved from <https://shop.ring.com/pages/neighbors>
- Ring Inc. (2019b). Security Cameras. *Ring*. Retrieved from <https://shop.ring.com/pages/security-cameras>
- Smiley, L. (2019, November 1). The porch pirate of Potrero Hill can't believe it came to this. *The Atlantic*. Retrieved from <https://www.theatlantic.com/technology/archive/2019/11/stealing-amazon-packages-age-nextdoor/598156/>
- Trottier, D. (2014). Crowdsourcing CCTV surveillance on the Internet. *Internet, Communication & Society*, 17 (5), 609-626. Retrieved from <https://www.tandfonline.com/doi/full/10.1080/1369118X.2013.808359>
- Vincent, J. (2018, January 23). Artificial intelligence is going to supercharge surveillance. *The Verge*. Retrieved from <https://www.theverge.com/2018/1/23/16907238/artificial-intelligence-surveillance-cameras-security>