21

Surveillance and Communication

Joshua Reeves

In recent years, surveillance studies and communication studies have enjoyed an increasingly cozy relationship. If we study the definition of surveillance offered by surveillance studies pioneer David Lyon, it is easy to see why this relationship has become so cozy. According to Lyon, surveillance is

> the focused, systematic, and routine attention to personal details for purposes of influence, management, protection, or direction . . . By systematic, I mean that this attention to personal details is not random, occasional, or spontaneous: it is deliberate and depends on certain protocols and techniques. Beyond this, surveillance is routine: it occurs as a "normal" part of everyday life in all societies that depend on bureaucratic administration and some kinds of information technology. (2015, p. 14)

Although surveillance scholars like Lyon have long emphasized the essential role that information and communication technologies play in surveillance, until quite recently most surveillance scholarship was carried out in departments of sociology and criminology. Yet since September 11, 2001, the political controversies surrounding surveillance have carried it into conversations across the humanities and social sciences, particularly in Communication. A number of prominent surveillance studies scholars are now housed in Communication departments, and the relationship between communication, security, and surveillance is a frequently engaged problem in the pages of Communication journals. In fact, the post-9/11 challenges of terrorism, risk, and insecurity have fueled something of a "surveillance turn" in many disciplines, with Communication counted among them (see Hall, Monahan, & Reeves, 2016).

But the relationship between surveillance and communication runs much deeper than cross-disciplinary affiliation. During the last decade, there have been at least four major ways in which scholarship in surveillance and communication have crossed paths (albeit sometimes without noticing one another). First, and most obviously, surveillance has become an attractive object of cultural and rhetorical criticism for scholars across Communication's sub-disciplines. Second, surveillance studies has always included information and communication technologies in its domain, as telephones, computers, and kindred media technologies—not to mention pencils, paper, photographs, and file cabinets—have provided the necessary technical infrastructure for mass surveillance (Mehrabov, 2015; Robertson, 2017). Third, surveillance has collided with media theory, especially as media ecology and cultural techniques research have become dominant modes of theory-building in media studies. From this perspective, media

theorists follow Friedrich Kittler (1999) and his disciples in defining media as the technological means by which data are gathered, stored, and processed. According to such a revision of media studies' agenda—a revision that focuses on how technical systems gather and produce knowledge, rather than on traditional textual analysis—there is little daylight between surveillance studies and media studies, especially regarding the question of security. And finally, fourth: surveillance and communication have been promoted as twin civic duties, especially in the context of safety and security. Through the U.S. Department of Homeland Security's "If You See Something, Say Something" program, Neighborhood Watch, and similar initiatives, citizens are trained to use surveillance and communication—that is, to "see something and say something"—in order to provide security for their communities, schools, homes, and workplaces (Reeves, 2012). Yet this trend is not limited to the United States, of course: similar programs can be seen in places like China, the U.K., and across the world.

Focusing on this surveillance turn, in general, helps clarify new cross-disciplinary possibilities for the analysis of security (in particular, the procedures, programs, and products that promote *domestic* security). Accordingly, this chapter will review these four major trends; in doing so, it will draw attention to a number of promising sites of current and future research. This chapter will begin by discussing the relationship between surveillance and domestic security in the public and private sectors, before describing the four major trends driving the convergence of communication and surveillance studies. The chapter then illustrates these four trends through an analysis of smart technology and an extended case study of Amazon's twin consumer technologies, Echo and Alexa.

SURVEILLANCE AND SECURITY

While defining the domain of surveillance is no easy task, Mark Andrejevic offers a useful gloss that emphasizes the role of power in shaping the surveillance terrain. According to Andrejevic, the object domain of surveillance tends to cover "those practices that assume the guise of scientific neutrality, bureaucratic record keeping, or the largely unexamined social imperatives of securitization, efficiency, risk management, productivity, and reproductivity" (2015, p. xii). It is difficult, therefore, to conceptually divide security from surveillance. While defining security is, like defining surveillance, no simple task, some scholars have done us a favor by delineating *security* in such a way that it forms a natural conceptual synthesis with surveillance. This is especially true of Bryan Taylor's (2017) recent discussion of media and security, which provides a number of useful insights into the relationship between these two concepts. As Taylor illustrates, the relationship between communication technology and security is, in many instances, a relationship between *surveillance* and security. That is, while Taylor reviews some of the more conventional ways in which media inform and carry out security policy (e.g., through propaganda, cultural imperialism, and the soothing flows of domestic cultural consumption; see 2017, pp. 48–49), his article's opening case studies provide a strong illustration of the inextricable relationship between surveillance and security (and, by extension, the inextricable relationship between these phenomena and communication technologies).

Taylor's argument begins with a discussion of two cases: in the first, Taylor recounts the tale of the San Bernardino terrorist attack in December 2015. What catches Taylor's attention is the central role that the assailants' iPhones played in the investigation. These phones were not primarily of interest because they were telecommunications devices; on the contrary, the FBI and allied investigative agencies most valued the phones as storehouses of information about the assailants, their networks, and their intentions. In other words, the iPhones were not valued for

their traditional telephonic functions, but for their surveillance functions—their capacities to capture and store data about users and their environments. In a related second case, Taylor describes how the forensic traces of drug kingpin El Chapo's communications—including emails, tweets, texts, and letters—allowed Mexican authorities to locate and capture the fugitive. Again, as with the case of the San Bernardino attacks, key to the relationship between media and security are media's surveillance capacities. In Taylor's words, "Data trails left by that [media] usage create highly desired evidence, enabling the state to better understand past and present events, and to intervene in the development of future events" (2017, p. 47). Therefore, while surveillance isn't the only role that media play in local, domestic, and international security production, it is one of the most prominent.

Surveillance's chief role in state and corporate security has been acknowledged, of course, by many scholars working in surveillance. The relationship between surveillance and security is a perennial problem in surveillance studies—and this is true not only for analyses of government-sponsored security programs and procedures, but also for those developed, adopted, and promoted in the private sector. When spearheaded by government agencies and major militaries, security production is characterized by threat assessment, risk analysis, and appropriate tactical operations. Following 9/11 these procedures have been globalized as GPS, satellites, international communications networks, and drone aircraft have fueled the desire for maximum security that only "total informational awareness" (Gates, 2011, pp. 97–98) can supposedly offer. As Edward Snowden's 2013 leaks disclosed, the U.S.'s National Security Agency (NSA) exploited the United States' global communications dominance to spy on activists, world leaders, and anyone else unfortunate enough to find themselves the tangential targets of a seemingly limitless NSA information collection (Murakami Wood & Wright, 2015). In the private sector, alternately, the relationship between surveillance and security typically appears in forms quite distinct from traditional policing, including purchase security, identity verification for credit purposes, and financial market regulations (see, e.g., Lauer, 2017; Williams, 2015).

The knowledge required to establish security in the public or private domains is theoretically boundless and thus instigates the continuous development of means for gathering and analyzing data (often on the order of "big data"). In a remark about policing that could apply just as well to the private sector, Didier Bigo observes:

> the state's duty to protect implies that it must act efficiently, not only to detect those responsible after an act of violence, but also to respond at the time, and more importantly, beforehand, so that violence may be prevented. In order to act in this way, the state and its agencies need to gather, store, analyze and apply as much information as possible. This dominant narrative assumes also that the more information is gathered by the state, and in a timely way, the greater the level of security is offered to it and its citizens. (2015, p. 277)

The irony of this desire for total information/total security, of course, is that these actions often have the effect of simply bringing into view new insecurities and risks—not to mention, of course, its tendency to actually produce conditions that incite future security threats. As Taylor et al. point out (2017), it is no surprise that debates about U.S. domestic security have only gathered steam during "the protracted conduct of U.S.-led military campaigns in Iraq and Afghanistan, the evolution of terrorist organizations, civil wars, and insurgencies, the expansion of state covert operations such as drone-conducted assassination, and a humanitarian crisis arising from international refugee flows" (Taylor et al., 2017, p. 113).

The technologies of the U.S.'s multi-decade, global War on Terror—including the surveillance technologies like drones that provide its technical conditions of possibility—have helped introduce new insecurities into its homeland (in the form of terrorist "blowback" and its domestic

management, for example). By the same token, the drive to make financial data more transferable and secure by linking them to cloud databases has also given rise to new methods of hacking, fraud, and identity theft. In both the private and the public sectors (to the extent that we should separate these), media innovation ensures that insecurity will always be chasing security. Adopting a malleable definition of security that encompasses the actions of individuals, local communities, and nation states, Bryan Taylor and Hamilton Bean argue that "institutions are inevitably concerned with 'security' as they enforce both custom and law to preserve order and public safety . . . and exchange needed commodities such as food and energy" (2017, p. 312). While this is (as the authors acknowledge) hardly an exhaustive definition of security, it does focus on several characteristics that are central to the domestic security/surveillance relationship. Law enforcement, for example, has long been on the cutting edge of surveillance procedures, as population analysis has always lain at the center of the political economy of policing (see Reeves & Packer, 2013). Along the same lines, disease prevention, food provisions, and the circulation of goods have demanded a wide array of surveillance techniques such as record keeping, census collection, food inspection, medical screenings, and land surveys (see Foucault, 1977; Scott, 1998). The close relationship between these surveillance procedures and domestic security management also points to a crucial missing factor in this equation: communication.

SURVEILLANCE AND COMMUNICATION: INTERSECTIONS AND NEW PATHS

There are at least four major ways in which problems in surveillance and security merge with common problems addressed in Communication. First, surveillance and security have become popular objects of cultural criticism for scholars concerned with topics like counterterrorism, risk management, and war. Second, scholars across disciplines have focused considerable attention on the fact that media technologies are inextricably tied to the work of surveillance. Third, we have witnessed something of an ongoing "surveillance turn" in media scholarship, as many media scholars have turned their attention to technologies' surveillance capacities rather than their representational functions. And fourth, scholars have begun to recognize that citizens' capacities for surveillance and communication (for "seeing something and saying something") are co-constitutive phenomena in the domestic production of security and insecurity.

As to the first point: Since the September 11 attacks a steadily increasing number of Communication scholars have turned their attention to historical and contemporary security policies, texts, and programs, particularly those involving surveillance (Taylor et al., 2017). Rachel Hall (2015), for example, has analyzed the airport as an exemplary site where the convergence of security and surveillance is on especially bright display. For Hall, the current state of this relationship can be best seen in the airport's transformation of travelers into "transparent" bearers of security data. As passengers rush through today's highly securitized airports, numerous identification procedures and surveillance protocols force travelers to pass through constant rituals of "compulsory transparency" (2015, p. 7). These rituals, which function by producing "docile and compliant subjects" (2015, p. 9), play an important role in training citizens how to live, work, and obey in the post-9/11 security regime.

Yet as we all know, these security rituals, procedures, and technologies extend far beyond the walls of the airport. Schools, for example, continue to provide an important immersive environment of surveillance and discipline (see Foucault, 1977). As Lizbet Simmons has pointed out, schools are an exemplary site because they, like prisons and other immersive institutions, "enable the constant visibility of the subject" (2010, p. 56). While under the direct supervision of teachers, peers, and administrators, students also face countless accountability procedures (such

as standardized testing and attendance monitoring). This is not even to mention the increasingly ubiquitous video monitoring devices, metal detectors, and motion sensors with which so many of today's schools are outfitted (and which form a key topic in public debates about school shootings). This environment, like the airport, organizes power in such a way that students' conduct is constantly modulated: students learn how to behave according to the surveillance/power relationships in which they are embedded at any given moment. Accordingly, students learn to navigate the "maximum security school" (Monahan & Torres, 2010, p. 10) by internalizing a diverse array of behavioral protocols that satisfy the demands of a given surveillance relationship (e.g., teacher to student, administrator to student, student to fellow student, bully to student, and so forth).

In one of the more interesting takes on the relationship between security, surveillance, and communication, scholars have analyzed how discourses of insecurity have allowed surveillance consumerism to sweep the marketplace. As we see the rise of the "insecurity subject" that is assailed on all sides by cultural anxieties about terrorism, risk, danger, and preparedness, a familiar solution emerges: *consumptive* solutions to insecurity management. In the words of Torin Monahan, while insecurity is constructed, it also "constructs us." "[D]iscourses of insecurity posit a certain type of ideal citizen who can flexibly respond and adapt to the vicissitudes and uncertainties of modern life without relying on the state. This *insecurity subject* anticipates risks and minimizes them through consumption" (2010, p. 2).

What we should keep in mind, therefore, is that the circular logic of insecurity production often creates its own conditions of resolution: the consumption of technology-based security commodities. Whether this comes in the guise of home alarms, "prepper" goods, gates and fences, or—perhaps most importantly—surveillance systems and apps that allow for the monitoring of one's household, one's loved ones, or even one's own biological health and wellness (Hasinoff, 2016), this entrepreneurial spirit places the responsibility for security onto each individual citizen. This insecurity subject then displays its mastery of the security marketplace by surrounding itself with consumer products that allow it to be responsive and self-sufficient in the face of scarcity, crime, terrorism, poor health, and other potential threats (see Levina, 2016).

Second: while surveillance has provided the focal point for many other forms of cultural criticism—e.g., reality television (Andrejevic, 2003), music videos (Dubrofsky, 2016), and film (Wise, 2017)—scholars have also generated provocative thinking about the key role that media technologies play in surveillance. In a recent overview of the surveillance landscape, veteran sociologist and surveillance scholar Gary T. Marx emphasizes the primary role of media technologies:

> the new surveillance . . . may be defined as *scrutiny of individuals, groups and contexts through the use of technical means to extract or create information*. In this definition the use of "technical means" to extract and create the information implies the ability to go beyond what is naturally offered to the senses and minds unsupported by technology. (2016, p. 20)

As Marx points out, the kind of digital surveillance we see today is in many ways a unique phenomenon that disrupts the continuity of surveillance history. Because of the emergence of digital media—and mobile communication technologies, in particular—surveillance has extended its reach into the very center of culture, labor, and leisure. New surveillance-based technologies and related digital phenomena—such as smartphones, GPS, drones, tracking software, smart devices, and fitness monitoring devices—have deeply changed our culture and our economy while enthroning a new class of surveillance entrepreneurs (not the least of which are executives at surveillance corporations like Google and Facebook).

Along the same lines, media technologies have played the predominant technical role in identity verification. For Craig Robertson (2009), a hallmark of the modern nation state is its

establishment of "archival" identities. This is, of course, a completely media-dependent process: from the index card and the file cabinet to the camera, phonograph, driver's license, the birth certificate, and the passport, modern regimes of citizenship rely on the archival documentation of identity (also see Lauer, 2011). As Robertson points out, this establishment of archival identity gave rise to a radical change in governance:

> This rethinking of identity as the collection, classification, and circulation of information made practicable not only the passport, but also the documentation of individual identity. This was achieved as personal identity and legal identity were collapsed into a new identity that provided a stable and reliable object for governing. (2009, p. 330)

The establishment of a uniform, "official identity"—an identity which could be copied, stored in file cabinets and databases, and circulated throughout numerous public and private domains of scrutiny and verification—called for the emergence of new forms of surveillance and new forms of government. This stable subject—with its "official identity"—could be studied, compared, and classified as an object of social scientific reflection. Hence, this stable subject and its aggregated abstractions becomes the object of countless security practices, including disease prevention drives, health and wellness programs, and identification procedures designed to determine risk, pinpoint potential threats, and delineate the boundaries of civic belonging (see Browne, 2015).

Of course, in the twenty-first century technologies of identification have come to play an even more important role in security procedures. As analog archives have come to be seen as inefficient, insecure, and imprecise, identity verification has been grafted onto the digitized body. Biometrics, in particular, has emerged as a popular method of identification for corporations, police agencies, and militaries around the globe. With their roots in analog databases that housed thousands of photographs and accompanying "anthropometric" measurements used for criminal identification (Reeves & Packer, 2013; Tagg, 1988), in recent years biometric technologies have emerged as the gold standard for identity verification. Digital fingerprint technologies and iris scanners, in particular, are praised for displacing the inefficiency of the analog identity archive. While these epistemologies of biometric data are notoriously biased and otherwise suspect (see Magnet, 2012), security agencies and corporations succeed in promoting their further adoption by stoking a sense of security "technostalgia"—that is, by arguing that if only we had possessed the right technologies and had the right security procedures in place, we could have stopped 9/11 and other terrorist attacks (see Gates, 2011, p. 2; Gill, 1997). This rationalizes the further development and adoption of more intensive security methods, all the while escalating deeper into the supposedly pure epistemology of the biometric (see Horn, 2003).

This brings us to our third theme, that of an emerging "surveillance turn" in media studies. While each of these other themes in surveillance, communication, and security suggests the increasing popularity of surveillance among communication scholars, the "surveillance turn" is a more general conceptual development that can be seen primarily in media theorists working from the German tradition of cultural techniques research (see Winthrop-Young, 2013). While these theorists might not focus on surveillance and security per se, their approach to media jibes in interesting ways with the traditional technological objects of surveillance studies. To explain: Friedrich Kittler's approach to media (1999; see Winthrop-Young, 2011), which emphasizes those technologies which manipulate the time/space axis by offering different means of capturing, storing, and processing data, reorients media studies' object domain by privileging media's surveillance functions over their representational functions.

With the changing landscape of everyday media usage, and especially with the rise of mobile media technologies, we have witnessed a remarkable shift in media's primary function. Now that the sensing function of technical devices like smartphones outweighs their traditional

communicative functions—that is, now that the majority of the data generated by smartphones is related to the passive surveillance of users' activities rather than to active user functions like talking, emailing, and texting (Andrejevic & Burdon, 2015)—the "surveillance turn" in media studies has been all but inevitable. This has led Communication scholars like Jeremy Packer to emphasize the "epistemological" power of media over their "ideological" power. Pivoting from the work of Kittler and his followers, Packer argues:

> Understanding media not merely as transmitters—the old "mass media" function—but rather as data collectors, storage houses, and processing centers, reorients critical attention toward the epistemological power of media . . . The breakthrough of digital media, as Kittler rightly pointed out, is that all media—all of reality—is not translatable. The world is being turned into digital data and thus transformable via digital manipulation. This is the realm of media's greatest power. (2013, p. 297)

For Packer, the traditional approaches to media criticism—e.g., ideology critique and textual analysis—still have considerable value. And to be sure, many media scholars today continue to produce innovative analyses of media texts that reveal the "ideological" power wielded through legacy media and new digital technologies. Yet the signature function of today's predominant media platforms are not their representational capacities, but rather their ability to capture data about their users and their surroundings. According to Packer, this epistemological function has eclipsed the traditional ideological power of media to broadcast and transmit reality. The increasing commercial centrality of big data, smart technologies, GPS, and mobile media provides legitimacy to Packer's call for an epistemological turn—that is, a *surveillance* turn—in media studies. Likewise, as it has become clear that U.S. security agencies collaborate with tech giants like Google and Yahoo (Lyon, 2015), approaching media through this surveillance lens considerably broadens the potential for analyzing the relationship between communication and state security programs. One of the most striking examples of this corporate/police collaboration can be seen in China, where facial recognition technologies and related biometric sensors are being integrated into citizens' everyday activities of work, leisure, and consumption. The Sharp Eyes program, active in locales throughout China, aims to consolidate the data gleaned from government-run security cameras—for example, those found in transportation centers and shopping malls—with the data gathered from the private security cameras that citizens use to protect their businesses and homes (Denyer, 2018). This integrated database would provide a wealth of information for government agencies and security professionals, especially as it would aid in the construction of facial recognition databases that could potentially allow for the real-time tracking of Chinese citizens as they shuffle between fluid domains of private, corporate, and police surveillance.

Finally, the relationship between communication and surveillance has been explored according to their parallel utility in the governance of risk and insecurity. As Marnie Ritchie (2015) points out, citizens have been recruited to "feel for the state"—that is, to be affectively attuned to certain bodies and behaviors that are potentially threatening. In Ritchie's words, citizens on the frontline not only feel for the nation, they must also "organize their senses for the state, or toward ends that benefit national security . . . [This] works through the production of affect, or the capacity to act and be acted upon, a potentiality that can be rhetorically channeled" (2015, p. 180).

For Ritchie, citizens form a reserve of potential affect that can be activated to respond to the world in certain ways. Yet this civic labor does not end there: These citizens are expected to act on these intuitions, feelings, and observations by notifying the authorities. This dual movement of sensing and alerting—of seeing and saying, of surveillance and communication—arises in

many of our society's most important forms of security management. Perhaps the most explicit form of this development is the "If You See Something, Say Something" program introduced by the U.S. Department of Homeland Security in 2010, but it takes diverse forms: for example, in Neighborhood Watch, cultural programming like *America's Most Wanted* and *Unsolved Mysteries*, and youth outreach initiatives such as Dare America. As Ott, Bean, and Marin (2016) demonstrate, cultural/educational institutions like Denver, Colorado's CELL "Counterterrorism Education Learning Lab" also illustrate how the affect/surveillance relationship can be managed in order to recruit citizens into homeland security initiatives. These programs work on citizens insofar as they are creatures that can see and say—that is, insofar as they can see something and say something. In the name of security, citizens are trained to be on the lookout for potential crime and terrorism—yet again, they must complement this surveillant labor with appropriate forms of communicative action: reporting crimes, calling the cops, tattling on their classmates, and so forth (see Reeves, 2017). This training of citizens to see and say in the service of security provides one of the classic political articulations of communication and surveillance.

SMART SURVEILLANCE, SMART SECURITY

One consumer product, in particular, helps clarify the connections between these research trends. At the same time, this product—Amazon's Echo—illustrates the danger that corporate intrusion poses to consumer security. As this case shows, the private/public partnerships between digital media corporations and local, state, and national policing authorities threaten citizens' security from corporate and state intrusion. In an odd yet all too predictable twist, they achieve this—at least in good measure—through appeals to safety, convenience, and security.

In 2015 Amazon launched Echo, a "smart" speaker that constantly records audiovisual information and is outfitted with a virtual assistant named Alexa. Designed to catapult smart technology into consumers' domestic lives, Echo allows users to give commands to Alexa, which uses the Bluetooth open standard to wirelessly connect to devices around the home. Originally touted as a novel way for families to use voice commands to control their music, set timers, control thermostats, check the weather, or create shopping lists, Echo helped make the "Internet of Things" (IoT) a consumer reality. As of late 2017, more than twenty million Echo devices had been sold. Like other IoT command centers, Echo can only operate by always being "on"—that is, by always listening to its surroundings to determine whether it is being sent commands. To turn off its audio surveillance features one would have to turn off the entire product, immediately terminating its use as a smart technology center that functions via verbal control.

Like similar innovations in consumer artificial intelligence and smart technology, Echo thus provides a glimpse into what Jonathan Cinnamon (2017) and Shoshana Zuboff (2019) call "surveillance capitalism"—the ongoing and pervasive economic shift that has prompted an explosive rise in surveillance entrepreneurism. Many of the world's most successful corporations, such as Amazon, Google, Yahoo, and Facebook, specialize in this surveillance capitalism and continue to pioneer new methods for gathering, storing, and analyzing data from as many points as possible. While the surveillance of stationary Internet users' browsing habits allowed for certain kinds of data to be gathered, the surveillance of the mobile subject (especially through the smartphone) exploded the potential for corporations to monitor and decode these subjects' behavior in the outside world. Needless to say, while Echo and similar devices recenter that surveillance on the home front, they open the door for new forms of data mining and behavioral decoding—not to mention offering new opportunities for the management and production of insecurity.

While this sociotechnical juncture provides many new possibilities for cultural criticism and theory-building, it also illustrates how shifts in communication and information technology constantly remake the surveillance landscape. This is necessary, of course, because nearly all corporate and state surveillance is conducted with and/or on media technologies, especially cell phones and personal computers. The drive to make new appliances, cars, thermostats, entertainment systems, and security alarms "smart" is, in essence, the drive to make all of these things *media* in the traditional sense. Indeed, the very key to their "smart-ness" is their distinctly media-logical capacities—through their integration with motion sensors, microphones, cameras, GPS, and related technologies they have each become instruments for the collection, storage, and processing of data. This integrated ubiquity, which allows for the coordination of many surveillance devices through a centralized command hub like Echo, contributes to a shift in the realm of the secure. With such a comprehensive spread of sensors, "total information awareness" ceases to be a shadowy government program and is instead given life in our broader cultural imagination: when everything can become media, total-security-through-total-knowledge becomes an apparently realizable telos for technical innovations and security initiatives (see Marx, 2016).

While smart technology in general lends itself to these concerns, one Echo feature has generated widespread concerns about surveillance in the home. Launched in summer 2017, the Echo Show functions like a video-based intercom device. Enabled by a network of Echo video sensors spread throughout a given house, Echo Show allows users to view what is happening in another room. While in its early years Echo was primarily touted as an audio technology, the Echo sensors on certain 2017 and later models are equipped with the capacity to capture video, as well. Hence with a simple verbal command, Echo Show users can see live footage of what is happening in a different room: when a user activates Show and requests to video conference with another room, the video camera in the chosen room activates and then, after an audio notification and a ten-second waiting period, begins transmitting video footage to the requesting device. Privacy advocates are quick to point out the myriad privacy implications of Show—as one tech journalist puts it, "It isn't just creepy. It's asking for trouble" (Matyszczyk, 2017). Consider, for instance, the possibility that someone originates a video request while the other person is out of the room. Then the audio warning sounds, the ten-second waiting period expires, the video feed begins, and several minutes later the targeted person walks into that room unaware that s/he is being watched (see Jackson & Orebaugh, 2018).

While this relatively mundane example illustrates the privacy dangers inherent in intra-home snooping—not to mention, of course, the potential for hackers to tap into that video data—even more interesting is the corporate research potential of all that video data. While Amazon, Google, Facebook, and the other kings of surveillance capitalism have become very successful in tracing users' communications, sleeping habits, movements, purchases, and other daily routines, these advances are based primarily on the capture of "metadata"—that is, the GPS-determined location of the user, the subject lines of emails, time-stamps of when consumers activate certain applications and turn on their phones, and related data not typically related to the main "content" of interactions (Landau, 2013). However, Echo's audio and video capacities have opened up new possibilities for capturing, storing, and analyzing the very "content" of our daily habits. These video and audio data generate an immense wealth of resources for Amazon, who stores all Echo-recorded data in its cloud and uses it for research purposes. Users of Echo, therefore, find themselves the objects of facial recognition research, as Amazon engineers search for new ways to analyze—and eventually, manipulate—how people react to various stimuli. By adding at such a large scale audiovisual "content" to the purview of surveillance capitalism, Echo and related devices have turned a new page in the surveillance and security conversation. While we have all grown accustomed to providing free labor for the corporations that use our data to create wealth

and experiment with our behavior, these corporations are enclosing more and more of our lives in surveillance, analysis, and experimentation (Andrejevic, 2007). By capturing the content of our domestic conversations and actions, the realm of this enclosure is expanding in remarkable ways.

Of course, expanding this enclosure into the home generates a number of ethical and political quandaries, especially regarding the relationship between surveillance, privacy, and security. While it is certainly reasonable to be concerned about corporate snooping, family snooping, government snooping, and related issues, the libertarian privacy paradigm cannot really address the fact that within the current system our data actually *are* private. We are not the ones who own "our" data. All the data captured by Echo's cameras and microphones belong to Amazon: all the conversations it captures; all the changes in pitch and tone; one's hesitations, one's anger, one's triggers, one's joys, one's vulnerabilities—i.e., all those things that are displayed in everyday interactions can be captured by microphones and cameras and decoded by extensive technical analysis. Particularly when compared to the behaviors of millions of other users, these data allow consumers to be analyzed, categorized, and targeted according to their perceived preferences and vulnerabilities. While consumers do not own this invaluable data trove, those data nonetheless remain private—they are owned by Amazon and are completely unavailable to the person who believes it is his or her right to access and control (Andrejevic, 2011). The perhaps laudable goal of more personal privacy, therefore, is wholly incapable of protecting citizens against the encroachments of corporations who are constantly converting data about our lives into privately held resources.

This data insecurity is perhaps best exemplified by one of Echo's more controversial capacities—its integration with police departments. There is, for example, a mysterious policing case that occurred in Albuquerque, New Mexico on July 2, 2017. That night a violent confrontation broke out between a local couple, Milana Honorio and Eduardo Barros. Honorio and Barros were housesitting the home of Honorio's parents, where an Echo device had been installed. When Honorio received a text message, Barros accused her of infidelity and suddenly became violent. Throwing her on the floor and beating her in the face and stomach, Barros pulled out a gun and threatened that he was "going to kill her if she called the cops" (Mele, 2017). He then demanded to know, "Did you call the sheriff?" A few minutes later, cops arrived at the house and, after a six-hour standoff, charged Barros with aggravated battery with a deadly weapon and other felonies (Mele, 2017).

While Amazon insists that Echo/Alexa does not make outgoing calls to phones that are not also hooked up to Echo/Alexa, the sheriff's office in Bernalillo County New Mexico has presented evidence that suggests otherwise. According to the sheriff's department, Honorio's Alexa called the police station when Honorio desperately yelled "Alexa, call 911" as she was being attacked. Bernalillo County Sheriff's Deputy Felicia Romero claims there can be little doubt that Honorio activated her Alexa device when she made that verbal command. In the days following the incident, Deputy Romero refused to back down from her claim: "The 911 recording is consistent with her statements, as she can be heard screaming in the background, 'Alexa call 911' . . . All we know is Alexa saved a life" (Mele, 2017). Because Echo/Alexa can be integrated with a user's phone, users can give Alexa a command—e.g., "call 911"—and if a contact named "911" is programmed into the user's phone, then that phone will call the invoked contact. Despite Amazon's denials, Romero maintains that Alexa autonomously accessed Honorio's contacts and called 911—and that that action saved Honorio's life.

While this new feature has the ability to save lives and provide for consumer security against violence, it can also have negative unforeseen consequences. On the one hand, increasing the ease with which citizens can report the perceived misdeeds of their neighbors, family members, fellow students, and coworkers can have troubling political and social effects.

This is particularly true when this capacity is integrated with crime crowdsourcing apps launched by police departments. In 2018 in Lancashire, England, a county with more than 1.5 million residents, local police departments launched an official collaboration with Amazon. Touted as a way for citizens to learn about crimes, fugitives, and missing persons, the app allows the police to broadcast this information to Alexa/Echo users. Recruiting citizens into policing efforts, however, is not the only goal of Lancashire's Amazon experiment. According to Ava Kofman of *The Intercept*, in the very near future Amazon is expected to officially launch a "Call 9-1-1" function on its Echo devices (Kofman, 2017). Accordingly, these rituals of seeing (surveillance) and saying (communication) for the state play an essential role in contemporary security campaigns; they also tend to increase suspicion among neighbors, exacerbate the marginalization of certain groups, and turn us against one another in exchange for civic gratification (Reeves, 2017). While these social and political trends are hardly unique to the digital era, AI has increased the number and reach of outlets that empower citizens to see something and say something for the sake of safety and security.

CONCLUSION

While smart technologies are not the only contemporary cultural phenomena that are fueling an ongoing "surveillance turn" in Communication research, they are certainly among the most important. Moreover, they present a cutting-edge example of how new communication technologies are having a serious impact on how we live, work, and play, and hence on how we approach our world and ourselves. Modern technological ideals of efficiency, accountability, and certainty have only been exacerbated by a diverse assortment of products. Wearable smart tech like the Fitbit, for example, turns biological activities once obscured by skin and bone into objects of scrutiny and reflection. Sleep-cycle alarm clocks pry into our brainwaves to ensure that we are efficient and precise even in our sleep. ("Never oversleep again!", urges an advertisement for the popular Sleep As Android app.) Just as some argue that our society can never have too much security, it can also be argued that it can never have too much surveillance. And in a familiar trend that follows this logic of escalation, the more surveillance our experts conduct, the more insecure they ensure us we are. In the end: just as insecurity chases security, the sensor wants to sense everything.

Using Amazon Echo/Alexa for illustration's sake, this chapter has described four main ways in which surveillance and security have impacted the practice and analysis of communication. First, surveillance and security have become popular objects of criticism for scholars in a number of fields, especially Communication. Second, the role of communication technologies in surveillance is increasingly acknowledged as a central, not a secondary, concern for surveillance scholars. Third, exciting new strands of media theory have shifted media scholars' attention toward the data-gathering functions of media technologies, rather than their symbol-generating functions. And fourth, surveillance and communication have become two commonly invoked civic duties, as citizens are increasingly called on to "see something and say something" in order to ensure their communities' security. Amazon's Echo and Alexa not only illustrate these cultural and political trends, they also present new opportunities for theory-building in communication and security. Smart technologies, more generally, pose an interesting challenge to those interested in the communication/security relationship, as they foreground the fact that our everyday technical companions—especially our communication technologies—have been transformed into surveillance devices. The character and effects of this transformation deserve extended critical attention from scholars, especially as "surveillance capitalist" corporations and police agencies merge their resources in order to chase the dragon of greater security.

REFERENCES

Andrejevic, M. (2003). *Reality TV: The work of being watched*. New York: Routledge.

Andrejevic, M. (2007). Surveillance in the digital enclosure. *The Communication Review*, *10*(4), 295–317.

Andrejevic, M. (2011). Surveillance and alienation in the online economy. *Surveillance and Society*, *8*(3), 278–287.

Andrejevic, M. (2015). Foreword. In R. Dubrofsky & S. A. Magnet (Eds.), *Feminist surveillance studies*. Durham, NC: Duke University Press.

Andrejevic, M., & Burdon, M. (2015). Defining the sensor society. *Television and New Media*, *16*(1), 19–36.

Bigo, D. (2015). Security, surveillance, and democracy. In K. Ball, K. Haggerty, & D. Lyon (Eds.), *Routledge handbook of surveillance studies*. New York: Routledge.

Browne, S. (2015). *Dark matters: On the surveillance of blackness*. Durham, NC: Duke University Press.

Cinnamon, J. (2017). Social injustice in surveillance capitalism. *Surveillance and Society*, *15*(5), 609–625.

Denyer, S. (2018). Beijing bets on facial recognition in a big drive for total surveillance. *Washington Post*, www.washingtonpost.com/news/world/wp/2018/01/07/feature/in-china-facial-recognition-is-sharp-end-of-a-drive-for-total-surveillance/?noredirect=on&utm_term=.a96a91cd7069.

Dubrofsky, R. (2016). A vernacular of surveillance: Taylor Swift and Miley Cyrus perform white authenticity. *Surveillance and Society*, *14*(2), 184–196.

Foucault, M. (1977). *Discipline and punish: The birth of the prison*, trans. Alan Sheridan. New York: Random House.

Gates, K. (2011). *Our biometric future: Facial recognition technology and the culture of surveillance*. New York: New York University Press.

Gill, P. (1997). Technostalgia: Making the future past perfect. *Camera Obscura*, *14*(1–2), 161–179.

Hall, R. (2015). *The transparent traveler: The performance and culture of airport security*. Durham, NC: Duke University Press.

Hall, R., Monahan, T., & Reeves, J. (2016). Editorial: Surveillance and performance. *Surveillance and Society*, *14*(2), 153–167.

Hasinoff, A. A. (2016). Where are you?: Location tracking and the promise of childhood safety. *Television and New Media*, *18*(6), 496–512.

Horn, E. (2003). Knowing the enemy: The epistemology of secret intelligence. *Grey Room*, *11*(1), 58–85.

Jackson, C., & Orebaugh, A. (2018). A study of security and privacy issues associated with the Amazon Echo. *International Journal of the Internet of Things and Cyber Assurance*, *1*(1), 91–100.

Kittler, F. A. (1999). *Gramophone, film, typewriter*, trans. Geoffrey Winthrop-Young and Michael Wutz. Palo Alto, CA: Stanford University Press.

Kofman, A. (2017). Amazon partnership with British police alarms privacy advocates. *The Intercept*, March 9, 2017, https://theintercept.com/2018/03/09/amazon-echo-alexa-uk-police.

Landau, S. (2013). Making sense from Snowden: What's significant in the NSA surveillance revelations. *IEEE Security Privacy*, *11*(4), 54–63.

Lauer, J. (2017). *Creditworthy: A history of consumer surveillance and financial identity in America*. New York: Columbia University Press.

Lauer, J. (2011). Surveillance history and the history of new media: An evidential paradigm. *New Media and Society*, *14*(4), 566–582.

Levina, M. (2016). Disrupt or die: Mobile health and disruptive innovation as body politics. *Television and New Media*, *18*(6), 548–564.

Lyon, D. (2015). The Snowden stakes: Challenges for understanding surveillance today. *Surveillance and Society*, *13*(2), 139–152.

Magnet, S. (2012). *When biometrics fail: Gender, race, and the technology of identity*. Durham, NC: Duke University Press.

Marx, G. T. (2016). *Windows into the soul: Surveillance and society in an age of high technology*. Chicago, IL: University of Chicago Press.

Matyszczyk, C. (2017). Amazon's Echo Show strips you of your last shred of privacy. *CNET.com*, www.cnet.com/news/the-amazon-echo-oh-no.

Mehrabov, I. (2015). Exploring terra incognita: Mapping surveillances studies from the perspective of media and communication research. *Surveillance and Society*, *13*(1), 117–126.
Mele, C. (2017). Did an Echo call 911 during a domestic assault? Amazon says no. *New York Times*, July 11, 2017, www.nytimes.com/2017/07/11/business/amazon-echo-911-emergency.html.
Monahan, T. (2010). *Surveillance in the time of insecurity*. New Brunswick, NJ: Rutgers University Press.
Monahan, T., & Torres, R. D. (2010). Introduction. In T. Monahan & R. D. Torres (Eds.), *Schools under surveillance: Cultures of control in public education*. New Brunswick, NJ: Rutgers University Press.
Murakami Wood, D., & S. Wright. (2015). Editorial: Before and after Snowden. *Surveillance and Society*, *13*(2), 132–138.
Ott, B. L., Bean, H., & Marin, K. (2016). On the aesthetic production of atmospheres: The rhetorical workings of biopower at The CELL. *Communication and Critical Cultural Studies*, *13*(4), 346–362.
Packer, J. (2013). Epistemology not ideology OR why we need new Germans. *Communication and Critical/Cultural Studies*, *10*(2–3), 295–300.
Reeves, J. (2012). If you see something, say something: Lateral surveillance and the uses of responsibility. *Surveillance and Society*, *10*(3–4), 235–248.
Reeves, J. (2017). *Citizen spies: The long rise of America's surveillance society*. New York: New York University Press.
Reeves, J., & Packer, J. (2013). Police media: The governance of territory, speed, and communication. *Communication and Critical/Cultural Studies*, *10*(4), 309–331.
Ritchie, M. (2015). Feeling for the state: Affective labor and anti-terrorism training in U.S. hotels. *Communication and Critical/Cultural Studies*, *12*(2), 179–197.
Robertson, C. (2009). A documentary regime of verification: The emergence of the US passport and the archival problematization of identity. *Cultural Studies*, *23*(3), 329–354.
Robertson, C. (2017). Learning to file: Reconfiguring information and information work in the early twentieth century. *Technology and Culture*, *58*(4), 955–981.
Scott, J. C. (1998). *Seeing like a state: How certain schemes to improve the human condition have failed*. New Haven, CT: Yale University Press.
Simmons, L. (2010). The docile body in school space. In T. Monahan & R. D. Torres (Eds.), *Schools under surveillance: Cultures of control in public education*. New Brunswick, NJ: Rutgers University Press.
Tagg, J. (1988). *The burden of representation: Essays on photographies and histories*. Minneapolis, MN: University of Minnesota Press.
Taylor, B. C. (2017). 'The movie has to go forward': Surveying the media-security relationship. *Annals of the International Communication Association*, *41*(1), 46–69.
Taylor, B. C., & Bean, H. (2017). Conceptualizing multicultural discourses of security: Introduction to the special issue. *Journal of Multicultural Discourses*, *12*(4), 213–331.
Taylor, B. C., Bean, H., O'Gorman, N., & Rice, R. (2017). A fearful engine of power: Conceptualizing the communication-security relationship. *Annals of the International Communication Association*, *41*(2), 111–135.
Williams, J. W. (2015). Law, surveillance, and financial markets. *Surveillance and Society*, *12*(2), 306–309.
Winthrop-Young, G. (2011). *Kittler and the media*. Malden, MA, Polity Press.
Winthrop-Young, G. (2013). Cultural techniques: Preliminary remarks. *Theory, Culture, and Society*, *30*(6), 3–19.
Wise, J. M. (2017). *Surveillance and film*. New York: Bloomsbury.
Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. New York: PublicAffairs.