Article

Eavesmining: A Critical Audit of the Amazon Echo and Alexa Conditions of Use

Stephen J. Neville

York University & Ryerson University, Canada
sjnevill@yorku.ca

Abstract

The emergence of smart speakers and voice-activated personal assistants (VAPAs) calls for updated scrutiny and theorization of auditory surveillance. This paper introduces the neologism and concept of “eavesmining” (eavesdropping + data mining) to characterize a mode of surveillance that operates on the edge of acoustic space and digital infrastructure. In contributing to a sonic epistemology of surveillance, I explain how eavesmining platforms and processes burrow the voice as a medium between sound and data and articulate the acoustic excavation of smart environments. The paper discusses eavesmining in relation to theories of dataveillance, the sensor society, and surveillance capitalism before outlining the potential contributions offered by a theoretical alignment with sound studies literature. The paper centers on an empirical case study of the Amazon Echo and Alexa conditions of use. By conducting a discourse analysis of Amazon’s End User Agreements (EUAs), I provide evidence in support of growing privacy and surveillance concerns produced by Amazon’s eavesmining platform that are obfuscated by the illegibility of the documents.

Introduction

The Amazon Echo was released in November 2014 as the first-ever smart speaker. The device, henceforth referred to as the “Echo,” advances the domestication of surveillance technologies as a new member of the Internet of Things and smart home apparatus. Yet, what is arguably novel about the device is how the Echo’s microphone and digital sensor technology alter the conditions of audibility in smart home environments. Unlike the microphones of personal computers, the Echo is designed to be always on—that is “listening” for its wake word even before circulating audio data online—and, unlike smart phones, it is non-mobile and primarily intended for home use. This development draws attention to what I call eavesmining (eavesdropping + data mining) platforms and processes, which are not ushered in by smart speaker technology but rather exemplified by it and normalized by the appeal of voice-activated personal assistants (VAPAs), such as Amazon’s Alexa. Eavesmining platforms articulate a mode of auditory surveillance that is socially divergent from issues of wiretapping, audio interception, and police informant practices because its microphone technology is non-secretive and voluntarily embraced by its users. This paper consists of a case study of Amazon’s eavesmining platform and develops a sonic epistemology of surveillance that is elucidated by the proposed neologism and concept.

Methodology: A Critical Audit of Amazon’s Conditions of Use

This study conducts a discourse analysis (Kendall and Wickham 1999) of Amazon’s EUAs to provide evidence in support of growing privacy and surveillance concerns produced by its eavesmining platform. Corporate EUAs are interpreted as a discursive formation because they exhibit a generic structure,

Neville, Stephen J. 2020. Eavesmining: A Critical Audit of the Amazon Echo and Alexa Conditions of Use. *Surveillance & Society* 18 (3): 343-356.

<https://ojs.library.queensu.ca/index.php/surveillance-and-society/index> | ISSN: 1477-7487

© The author(s), 2020 | Licensed to the Surveillance Studies Network under a [Creative Commons Attribution Non-Commercial No Derivatives license](https://creativecommons.org/licenses/by-nc-nd/4.0/)

obfuscating use of legalese, and form of hyper intertextuality. I examine the EUAs governing the use of the Echo and Alexa platform from the release of the device in November 2014 to March 2019. This maps the ongoing changes made to the “Conditions of Use,” “Amazon Privacy Notice,” “Amazon Device Terms of Use” (previously titled, “Amazon Echo Terms of Use”), and “Alexa Terms of Use.”¹ Notably, the “Conditions of Use” and “Amazon Privacy Notice” preceded the release of the Amazon Echo. I have extended my historical analysis to April 2012 to consider adjacent versions of these documents that anticipate the release of the Echo. Thus, the entire timeframe of analysis is a seven-year period from April 2012 to March 2019.

Amazon does not label EUAs with a version ID number and does not make older versions of the documents available on Amazon’s website. This makes it difficult for both consumers and researchers to access and track previous versions of the EUAs. I have utilized the Internet Archive service, the Wayback Machine (<https://archive.org/web/web.php>) to circumvent this challenge. The Wayback Machine is a non-profit research tool that downloads publicly accessible webpages by crawling the internet. There are limitations to the databank such as inconsistencies caused from partially cached websites and dead hyperlinks: the more navigation that is required to arrive at a particular webpage on a contemporary website, the less feasible it becomes to simply copy and paste its URL (Uniform Resource Locator) into the Wayback Machine archive for retrieval, especially in cases where website pathways may have been altered.

Data collection began with a visit to Amazon’s website in March 2019. I located the relevant EUAs on the live version of the website and made note of document publication dates. I then operated with the assumption that the prior version of each EUA would be locatable by accessing the webpage from at least one day prior to the current publication date using the Wayback Machine archive. I followed this logic in reverse chronological order until I had arrived at the beginning of the timeframe (April 2012). For each version of the EUAs, I downloaded the archived webpage.²

This study does not conduct a comparative analysis of the EUAs with the entirety of Amazon’s global services. Instead, I focus exclusively on EUAs from Amazon.com, which exhibit the most alarming privacy and surveillance implications due to a recent change made to the “Alexa Terms of Use” (November 27, 2018). The feature of “automatic voice recognition and voice profiles” has not yet been added to other Amazon national services. I suggest that a case study of Amazon.com can serve as a cautionary tale in a global context that is now only gradually beginning to wrestle with the privacy and surveillance implications posed by eavesmining platforms. Indeed, the rapid integration of VAPAs in household spaces makes it all the more pressing to call into question their current social trajectories (Pridmore et al. 2019: 130). It just so happens that the EUAs on Amazon.com are the most advanced along these trajectories—as reflected by Amazon’s automatic vocal biometric enrollment system—meaning that global stakeholders should pay heed to Amazon’s treatment of the American public as a trial market in the domestication of its eavesmining platform.

In total, I collected twenty-three EUAs, consisting of six versions of the “Conditions of Use,” four versions of the “Amazon Privacy Notice” as well as the “Children’s Privacy Disclosure” (August 29, 2017), seven versions of the “Amazon Device Terms of Use” (formerly titled “Amazon Echo Terms of Use”), and five

¹ Although these pages have changed over the years, the current versions can be found here: “Conditions of Use”: <https://www.amazon.com/gp/help/customer/display.html?nodeId=201909000>; “Amazon Privacy Notice”: <https://www.amazon.com/gp/help/customer/display.html?nodeId=201909010>; “Amazon Device Terms of Use”: <https://www.amazon.com/gp/help/customer/display.html?nodeId=202002080>; “Alexa Terms of Use”: <https://www.amazon.com/gp/help/customer/display.html?nodeId=201809740>.

² This method proved to be successful in all cases but one: there is a missing version of the “Alexa Terms of Use” that I have deduced was published around June 2015. I was able to conclude that this amounts to an entirely negligible blind spot because, at this same time, the “Amazon Echo Terms of Use” (June 25, 2015) bifurcated to form a separate EUA, “Alexa Terms of Use.” After determining what modifications were made from the previous version of the “Amazon Echo Terms of Use” (March 18, 2015), I was able to conclude that no significant changes were made to the “Alexa Terms of Use” between June 2015 and its earliest retrievable version (February 2, 2016).

versions of the “Alexa Terms of Use.” In each case, I analyzed the initial version of the EUA and identified any significant passages. Subsequently, I collated the following version with the original and tracked any changes made to the documents, repeating this method until completing an analysis of the dataset.

I liken this study to an *audit* of Amazon’s eavesmining platform by examining its legal account of various socio-technical developments while performing a critical “hearing” or “listening” of its surveillance practices, as etymologically signified. To prepare the reader for a presentation and discussion of the research findings, I now outline the concept of eavesmining before situating a sonic epistemology in relation to surveillance studies literature.

Eavesmining

The concept of *eavesmining* characterizes a set of digital listening processes that affect acoustic space and embodied relationships with sound. This development is best understood in its relationship with the medium of the voice, which is its primary target.³ To begin, acoustic space is affected by a twofold movement: first by digitally scraping the auditory signatures of voices, words, and verbal cadences; and, second, by circulating data as analog sound within the smart home, as articulated by the voice of Alexa and other mediatized “voices” played via the Echo (e.g., music, news, podcasts, audiobooks, and radio). Thus, eavesmining affects acoustic space by listening with microphone technology to the voices of smart home inhabitants while monitoring their consumption of audible media content. Further, eavesmining alters embodied relationships with sound in a profound manner by transforming the human voice into a digital interface, or, in other terms, by transposing oral communication into a mode of technical interaction with the cloud. Resultantly, eavesmining involves more than the “semantic mode of listening” (Chion 1994).⁴ That is, due to the connectedness of the human voice with an identifiable body and its physical processes, eavesmining not only listens to linguistic flows but *overhears* one’s vocal biometrics, affect, and the daily rhythms of the body in its domestic habitat (e.g., alarms, timers, reminders, and “Alexa routines”⁵). Therefore, I assert that eavesmining serves to burrow the voice as a medium located between sound and data.

The term is a portmanteau that merges the meanings of eavesdropping and data mining. “Eave” derives from the Old English *efes*, referring to an “edge” or “border.” Historically, by standing underneath the eavesdropping—where the edge of exterior walls meets the roof of a building—unseen listeners could potentially overhear conversations occurring within interior space. In the vernacular, eavesdropping refers to any act of listening in occurring at the physical and symbolic boundaries between inside/outside, private/public, and domestic/public. Thus, the notion of eavesdropping captures the immanent tension of sound as “an entity of the edge” (Dolar 2011: 125). The concept of eavesmining expands this to characterize an act of monitoring occurring at the edges of sound/data and listening/data mining enabled through the combined use of microphones, digital sensors, signal processing algorithms, database systems, and data mining techniques.⁶ By pressing an “ear” to the metaphoric wall between acoustic space and digital infrastructure, eavesmining articulates the acoustic excavation of smart environments.

³ Eavesmining may also record and analyze ambient environments or soundscapes, non-verbal voicings (e.g., coughing, crying, breathing, and screaming), non-vocal sounds (e.g., footsteps, movements, and noisy activities), or a combination thereof, such as the sounds of violence, partying, or lovemaking.

⁴ Michel Chion (1994: 25–34) distinguishes three modes of listening: “causal listening” that listens to gather information about its source or cause; “semantic listening” that operates with reference to a code or language; and “reduced listening” that focuses on the acoustical traits of the sound itself, independent of its cause and meaning.

⁵ An “Alexa routine” is a user-programmed set of customizable actions initiated with one digitized utterance. For instance, one can program Alexa to open the blinds, play the news, wake up the kids, and start brewing a pot of coffee, all with the directive, “Alexa, good morning.”

⁶ Eavesmining should not be conflated with all forms of digital eavesdropping, some of which may utilize digital sound recording technology without the backend infrastructure of databases and data mining techniques.

Eavesmining is proposed as a label for the tangible material processes that seek to scrape and listen to the vibrational nodes of everyday life. This is epitomized by the growing ubiquity of VAPAs which effectively animate ordinary objects into quasi-conversational entities that speak, make sound, and listen. Therefore, eavesmining is not restricted to the domestic sphere but is creeping into a variety of social spaces.⁷ The proliferation of eavesmining platforms affords unprecedented corporate access to acoustic milieus which may prove to inhibit forms of agency, freedom, and subjectivity.

A deeper meaning can be attached to eavesmining that articulates a power relation from above, as with forms of panoptic, acousmatic (James 2014), and panacoustic surveillance (Szendy 2016). Earlier in its etymology, *efes* derives from the German *oben*, “above,” “up from under,” and “over.” Yet, unlike watching, listening is not as suitably exercised from physically high places (see Mann and Ferenbok 2013) but by keeping an ear to the ground. Unlike organic forms of listening, eavesmining occurs in real time with sound recording and signal processing algorithms and in the future as audio is translated into big data that is subjected to corporate data mining techniques including machine learning, collaborative filtering, and various forms of “knowledge discovery in databases” (Fayyad, Piatetsky-Shapiro, and Smyth 1996). Thus, by keeping an ear to the ground, eavesmining attends to sounds from the past, present, and future. To better understand these developments, I suggest that we, as surveillance researchers, might gain new insights by thinking critically with our ears about auditory surveillance.

Towards a Sonic Epistemology of Surveillance

This section argues for a sonic epistemology of surveillance to help analyze the media specificity and sociality of eavesmining platforms and processes. This reconceptualization of surveillance as a practice of listening in is prompted by the emergence of various eavesmining platforms and processes. This case study’s focus on the Echo and Alexa platform serves as only one example. I begin by outlining the shortcomings of Foucauldian and post-panoptic theories before introducing some potential contributions from sound studies literature to the field of surveillance studies.

The apparent ocular centrism of surveillance studies can be traced to the extensive influence of Michel Foucault on the field. Foucault has been characterized as an “exceedingly visual historian” (Rajchman 1988: 88). Commenting on the vivid images contained in *Discipline and Punish* (1977) and *The Birth of the Clinic*, John Rajchman describes them as “pictures not simply of what things looked like, but of how things were made visible, how things were ‘shown’ to knowledge or to power—two ways in which things became *seeable*. In the case of the prison, it is a question of two ways crime was made visible in the body, through ‘spectacle’ or through ‘surveillance’” (Rajchman 1988: 91; italics in the original). In either mode of visibility some things are made to be seen at the expense of others and, resultantly, contribute to the formation of a regime of truth.

Deleuze was, of course, keenly aware of Foucault’s “art of seeing” as both a historian and philosopher (Rajchman 1988: 115). Perhaps with this in mind, Deleuze (1992) sought to extend Foucault’s analyses of power by writing on the transition from disciplinary society and panopticism to societies of control. In order to expand on the limited writings of Deleuze and Guattari on the topic of surveillance, Haggerty and Ericson (2000) propose the surveillant assemblage as a post-panoptic model. This is offered as a corrective to surveillance studies literature that, they argue, can overtly bend and distort the concepts put forth by Foucault and in George Orwell’s 1949 novel *1984* by attempting to adapt their ideas to contemporary developments, as others have similarly argued (see Albrechtslund 2008). To this end, the surveillant assemblage is certainly a valuable analytical tool, yet Haggerty and Ericson’s (2000) emphasis on visualization effectively advocates for a non-Foucauldian, ocular-centric approach to surveillance studies. To illustrate, their notion of the surveillant assemblage is characterized as “a *visualizing* device that brings

⁷ For example, Walmart recently patented an audio surveillance tool that uses aural performance metrics to calculate the productivity of employees and customer satisfaction levels at checkout counters (Weiner 2018). This reflects the combination of eavesdropping and data mining characteristic of eavesmining processes.

into the *visual register* a host of heretofore opaque flows of auditory, scent, chemical, visual, ultraviolet and informational stimuli. Much of the *visualization* pertains to the human body, and exists beyond our normal range of perception” (Haggerty and Ericson 2000: 611; emphasis added). Evidently, the surveillant assemblage remains committed to visual metaphors in its theoretical treatment of surveillance, unlike the sonic epistemologies developed in sound studies literature (Goodman 2010; Miyazaki 2013, 2016; James 2014, 2019; Labelle 2018).

Foucault’s (1977) writing on Jeremy Bentham’s diagram of the panopticon has been revisited and reformulated to suit various forms and modes of surveillance (Poster 1990; Gandy 1993; Mathiesen 1997; Bigo 2006). In Greg Elmer’s (2004) reading of David Michael Levin (1997), Elmer clarifies that Foucault’s interpretation of the panopticon is not only premised on the hegemony of light, vision, and the gaze being exercised on carceral bodies but is also only productive when it is coordinated with a general system of “continuous registration, perpetual assessment and classification” (Foucault 1977: 220). Thus, the panopticon is a system of both light and language (Elmer 2004: 33) whereby the effects of power can be read both through the self-discipline of carceral bodies and the set of discursive statements made about those bodies. If Foucault’s reading of the architecture of the panopticon explicates the “general deployment of a system of power” (Elmer 2004: 34) then how do eavesmining platforms articulate a different set of force relations through the hegemony of sound, audition, and the ear?

Bracketing this question, other scholars have argued that ideas of looking, hearing, and other modes of organic sensing can obfuscate the technical operations of surveillance mechanisms, which, indeed, do not analogously reproduce human modes of sensing. The sensor society thesis is offered as an account for the emerging sensing environment whereby the interactive devices and applications that permeate everyday life come to double as sensors that “do not watch and listen so much as they detect and record” (Andrejevic and Burdon 2015: 25). The sensor society thesis is similar to Roger Clarke’s (1988) influential notion of dataveillance but with a crucial difference in its operational logic. To be precise, dataveillance is useful in explaining the discriminatory effects of panopticism in relation to debates about personal privacy, as outlined by Elmer (2003) and expanded by some of the figureheads in surveillance research (Gandy 1993; Lyon 2001). Yet, whereas dataveillance focuses on pre-identified or identifiable persons, this is not entirely true of sensor-based monitoring: in the sensor society, discrete targets may emerge from a network of monitored behaviours, but, unlike dataveillance, this can be untargeted, non-systematic, and opportunistic (Andrejevic and Burdon 2015: 23). For instance, a subpoena was issued to Amazon in 2017 demanding information collected from a first-degree murder suspect’s Echo device in the United States (McLaughlin 2017), reflecting a non-systematic and opportunistic form of intervention.

Eavesmining shares aspects of dataveillance and sensing-based monitoring: first, like dataveillance, it focuses on identifiable persons because its primary target, the voice, embodies a personally identifying biometric trait; second, eavesmining platforms exhibit a general mode of acoustic excavation that indiscriminately treats all sounds as data—the new oil that awaits capitalist extraction and accumulation. This resonates with the goal of sensing-based monitoring to “capture a specific dimension of activity or behavior across the interactive, monitored space—to open up new data-collection frontiers” (Andrejevic and Burdon 2015: 24). Thus, as eavesmining targets identifiable voices and opens an acoustic frontier of data collection, it indicates a vibrational oscillation between modes of dataveillance and sensing-based monitoring.

Before briefly turning to sound studies literature, one final connection with surveillance studies literature must be established. Due to its futurity and structuration by market logics, eavesmining contributes to Zuboff’s (2015, 2019) conception of surveillance capitalism, a political economic regime centered around the accumulation of big data for the marketized production of behavioral predication and modification schemes. I wish to conceptualize eavesmining in relation to surveillance capitalism’s mechanisms of extraction and control with one stipulation for its theoretical alignment: despite the richness of Zuboff’s (2019: 255–269) discussion of “digital assistants,” she does not differentiate between the motivations and dataveillance affordances of the variety of eavesmining platforms (see Pridmore et al. 2019). Amazon is

clearly focused in its efforts to increase personalized sales on its shopping platform through Alexa, whereas Google, in contrast, primarily seeks to build its targeted advertising platform through its VAPA (Pridmore et al. 2019: 126). For Zuboff (2019: 377), the apparatus of surveillance capitalism, called “Big Other,” can be heard “through the tireless devotion of the One Voice—Amazon-Alexa’s chirpy service, [and] Google Assistant’s reminders and endless information.” Rather, just as we must speak of political economies and not “a” political economy of surveillance (Pridmore 2013), I suggest that Big Other can be heard through a multiplicity of voices that correspond to a growing diversity of eavesmining platforms that exhibit varied design motivations and surveillance affordances.

Sounding Out Potential Contributions to the Field

Here, I momentarily lean on sound studies literature to illustrate why the auditory spectrum is significant to surveillance studies and how future research on eavesmining platforms and processes may reveal new problems of “social sorting” (Lyon 2003) and discrimination. For instance, issues of intersectionality come into new focus with consideration of Jennifer Stoever-Ackerman’s (2010) notion of the “sonic colour-line,” which, under “the shadow of vision’s cultural dominance[,] describes how race is mediated through aural signifiers as well as visual ones” (Stoever-Ackerman 2011: 21). Historically, the sonic colour-line sought to separate “blackness” and “femaleness” from the human through a set of white listening practices that rendered non-verbal sounds as unintelligible and meaningless. Stoever-Ackerman’s (2010: 62) work posits listening as an “interpretive site where racial difference is coded, produced, and policed.” The sonic colour-line complements Simone Browne’s (2015: 97–102) discussion of Frantz Fanon’s (1982) “epidermalization” by considering how race is both visually and aurally imposed on the body. A sonic epistemology of surveillance might explore how the construction of a digital sonic colour-line is articulated by emergent biometric technologies such as eavesmining platforms. Thus, a sonic epistemology of surveillance might contribute to a critical biometric consciousness (Browne 2015: 116) that confronts the auralization of racial difference.

In another vein, a sonic epistemology of surveillance should take seriously how historical listening practices and techniques are recuperated by eavesmining platforms. This offers a return to Foucault, who discussed how the voice was treated first as a window of the soul and later—under the aegis of the psy-disciplines—of the mind (see Brinkmann 2005). Writing on the ritual of confession, Foucault (1978) provides an account of power that is systematized in the dialogic relations between confessor and priest. He explains: “By virtue of the power structure immanent in it, the confessional discourse cannot come from above...but rather from below, as an obligatory act of speech...[whereby] the agency of domination does not reside in the one who speaks (for it is he who is constrained), but in the one who listens and says nothing” (Foucault 1978: 62). Similarly, for the user of Amazon’s eavesmining platform, interaction is marked by an obligatory act of speech, an “incitement to discourse” (Foucault 1978: 17), directed to the Echo and Alexa and overheard by Amazon, which listens in from a position of silence but never speechlessness. Much like confessional discourse, I suggest that discourse enclosed by eavesmining processes exerts force on the user and surrenders the agency of domination to Amazon and third parties, a suggestion that is supported by my critical audit of EUAs.

The recuperation of historical listening practices and techniques by eavesmining platforms expands discussion of auditory surveillance beyond issues of semantic listening. Specifically, the voice represents a biometric trait and can potentially be interpreted for behavioural, affective, and psychological variables. In a recent interview, Amazon’s VP of Alexa AI Prem Nataraja states that, in the future, he would like Alexa to respond to “mood, sentiment, feeling as expressed in your speech” (Nataraja 2018). This reality may lie just beyond the horizon since computational analysis of vocal expression has already been applied in non-commercial areas for the detection of affect and psychological conditions (González, Carter, and Blanes 2007; Mitra et al. 2015; Scherer et al. 2016). A sonic epistemology of surveillance supports the assertion that “computational politics are as much about psychology as about computing” (Stark 2018: 220). Indeed, eavesmining affordances appear to recuperate psychoanalytic listening practices (Reik 1958; Lagaay 2008). As Sigmund Freud’s pupil, Theodor Reik (1949: 136) writes: “It is not the words spoken by the voice that

are of importance, but what it tells us of the speaker. Its tone comes to be more important than what it says, ‘Speak, in order that I may see you,’ said Socrates.” Thus, in the psy-disciplines, the voice is interpreted as deeply indicative of who we are. Similarly, eavesmining platforms can be attuned to what is non-consciously communicated by the voice. A sound studies approach to surveillance would help examine the interesting histories of listening practices, techniques, and technologies (see Sterne 2003) to better inform understandings about the power/knowledge yielded by eavesmining platforms.

Having situated a sonic epistemology in relation to surveillance studies literature and argued for the potential contributions of this approach to the field, I have raised a series of privacy and surveillance concerns around eavesmining platforms and processes. The empirical study that follows specifically addresses the relationship of Amazon’s eavesmining platform with a surveillance capitalist regime. Although the Echo and Alexa are voluntarily embraced by Amazon customers, they articulate “unexpected and illegible mechanisms of extraction and control” (Zuboff 2015: 85). In the case of Amazon’s conditions of use, a critical audit reveals that endemic privacy concerns are obfuscated around the implementation and management of eavesmining platforms and processes in home environments. Using a method of discourse analysis, this study asks: What conditions of use are imposed by Amazon’s EUAs and how are these changing over time to affect individuals and households of users? To what extent do these changes articulate intensifying privacy and surveillance concerns within the domestic sphere? And, lastly, how is the domestication of Amazon’s eavesmining platform reproducing and modulating power relations in home environments?

EUAs Research Findings

My research findings are segmented according to three historical timeframes: (1) The *pre-Alexa timeframe* from April 6, 2012 to November 5, 2014. In this period, I summarize the pre-existing corporate legal framework of Amazon’s web services. (2) The *nascent timeframe* from November 6, 2014 to August 28, 2017. During this period the EUAs are highly unstable documents, meaning that the terminology and definitions are being continually updated. (3) The *contemporary timeframe* from August 29, 2017 to November 27, 2018.⁸ At this point, all current interactive features of the device have been integrated into the EUAs and each document has been expanded in detail.

Pre-Alexa Timeframe: April 6, 2012 to November 5, 2014

Amazon collects a variety of consumer information through its use of online shopping services, as detailed in the “Amazon Privacy Notice.” During the pre-Alexa timeframe, the EUAs reproduce generic language featured in conditions of use for consumer platforms. Table 1 contains the mechanisms, information types, and privacy control options of Amazon’s data collection practices as of April 6, 2012, as outlined in the “Amazon Privacy Notice.”

Data Collection Mechanism	Types of Information Collected	Privacy Control Options
1. Information provided by the user	Account and user profile information (e.g., name, address, email, and phone number); credit card information; people to whom purchases have been shipped, including their addresses and phone numbers	Information can be withheld at the expense of certain services
2. Automatic information (collected from cookies and other software tools such as JavaScript)	Internet protocol (IP) address; login and password; computer and connection information (e.g., browser type, time zone setting, browser plug-ins, operating system); search and purchase history, including full Uniform Resource Locator (URL) clickstream; session information (e.g., page interaction	Cookie settings can be adjusted in web browser settings at the expense of certain services

⁸ I conducted this research in March 2019; Amazon has not updated the EUAs since November 27, 2018.

	information such as scrolling, clicks, and mouse-overs)	
3. Mobile information (collected from Amazon applications downloaded on a mobile device)	Location information; mobile device information, including a unique identifier of the device	Location services can be disabled in mobile device settings
4. Email communications	Activity information if an email from Amazon has been opened by the customer	User can opt out of emails from Amazon
5. Information collected from other sources	Updated delivery and address information from Amazon's carriers or other third parties, search results, and links (including paid listings and sponsored links); and credit history information from credit bureaus	None

Table 1: Privacy control options during the pre-Alexa timeframe

Using a combination of three mechanisms (numbers one, three, and five from Table 1), Amazon can potentially infer where a user lives and at what times they are at home. A shipping address is not a determinant of one's home address, yet Amazon can easily cross-reference this with the billing address associated with one's credit card and credit history. In cases where a shipping address and billing address correspond, this correspondence may still not be a determinant of one's home address. If a user has not opted-out of the mobile device location settings, the company can cross-reference one's GPS (Global Positioning System) history with the shipping and billing address to deduce which of these corresponds with a user's home address. Following this logic, Amazon can roughly determine when a user is at home and when they are away to help optimize its carrier delivery schedules or productize this information using collaborative filtering (see Brandt 2011). For instance, users who remain at home between working hours may be unemployed, stay-at-home parents, or home business entrepreneurs, insights that could be valuably added to one's consumer's profile for marketing and advertising purposes.

Nascent Timeframe: November 6, 2014 to August 28, 2017

Following the release of the Echo, the EUAs become highly changeable. Although many of the alterations and revisions are relatively insignificant, their cumulative effect makes it increasingly challenging to track changes from one version to the next. The first version of the "Amazon Echo Terms of Use" (November 6, 2014) includes a clause titled "Changes to Services; Amendments" that carries through all subsequent versions: this stipulates that any of the Alexa Services and Amazon EUAs can be altered at any time without notice to the consumer. Amazon will post the revised terms and conditions on Amazon.com and they will immediately come into effect. Most significantly: "Your continued use of the Amazon Echo after the effective date of the revised Agreement constitutes your acceptance of the terms."

Initially, the "Amazon Echo Terms of Use" (November 6, 2014) was the sole document added to Amazon's corporate privacy framework. These terms were updated five times during the nascent timeframe, despite eventually being renamed as "Amazon Device Terms of Use" (March 3, 2016). Further, some of the terminology and definitions contained in the "Amazon Echo Terms of Use" are eventually molded into the "Alexa Terms of Use" (February 2, 2016). Table 2 outlines the changing terminology corresponding to the key definitions contained in these two EUAs during the nascent timeframe. Although this table does not capture the changing definitions associated with their terms, it demonstrates that the mutability and intertextuality of these documents makes it difficult to track any changes.

EUA	EUA Version	General Terminology in EUAs							
Amazon Echo Terms of Use (ToU)	Nov. 6, 2014	Digital Content	Amazon Echo	Amazon Echo App	Voice Services	Services	Software	Third Party Service	
Amazon Echo ToU	Jun. 25, 2015	(moved to Alexa ToU)		(moved to Alexa ToU)		(combined with Voice Services)	Echo Software	(moved to Alexa ToU)	Alexa
Alexa ToU	Feb. 2, 2016	Digital Content	Alexa Enabled Product	Amazon Alexa App	Voice Services		Software	Third Party Service	Alexa (moved from Amazon Echo ToU)
Amazon Device ToU	Mar. 3, 2016	(moved back from Alexa ToU)	Amazon Device	(moved to Alexa ToU)		Services (separated again from Voice Services)		Third Party Content	Alexa (moved to Alexa ToU)

Table 2: Outline of changing terminology in EUAs during nascent timeframe

The first version of the “Amazon Echo Terms of Use” (November 6, 2014) outlines Voice Services, referring to voice-based interaction with Alexa and entailing the transmission of audio to Amazon’s servers (i.e., the cloud). Amazon processes and retains voice-input data as well as other types of information such as music playlists, to-do lists, and shopping lists. The more significant privacy and surveillance concerns relate to voice-input data. Amazon has anticipated consumer concerns by providing some privacy control options that “may degrade your experience using Amazon Echo”: Users can review their voice-input data, delete specific audio recordings, or delete them en masse. Users can also manage how their voice-input data are used by Amazon when developing new features and improving services. First, from the Alexa app, users can opt out of having their data used to help develop new features. This comes at the expense of said new features potentially not functioning properly for them. Second, users can opt out of having their audio data used to help test and improve Alexa’s transcription accuracy, although this privacy control option is not foregrounded clearly within the Alexa app (Settings > Alexa Account > Alexa Privacy > Manage How Your Data Improves Alexa).

Contemporary Timeframe: August 29, 2017 to November 27, 2018

From August 29, 2017 until November 27, 2018, the EUAs become more stable with fewer definitions and terminologies being added, modified, or relocated to other documents. At this stage, however, the more significant developments in privacy and surveillance concerns begin to emerge: these developments are featured specifically within the “Amazon Privacy Notice” and “Alexa Terms of Use.”

On August 29, 2017, Amazon added a “Children’s Privacy Disclosure” addendum. The company defines anyone under the age of thirteen as a child, while the “Privacy Notice” states that Amazon does not knowingly collect information from anyone under the age of eighteen without the consent of a parent or guardian. In accordance with the Children’s Online Privacy Protection Act of 1998, Amazon can collect personal information from children only after receiving verifiable parental consent. To reflect its use of Alexa and the Echo platform, this includes the collection of voice data from child users. As with adult users, the personal information of children is used by Amazon to improve its products and services and provide personalized recommendations for children. If a parent chooses to rescind the permission provided on behalf of a child or requests deletion of their child’s personal information, various services and features become

unavailable: for instance, the collection and processing of voice data are integral to the basic operation of Alexa and the Echo platform. Notably, any third-party services accessed through the Echo, such as Alexa Skills, are not covered by Amazon's EUAs.

The "Children's Privacy Disclosure" articulates a potential form of custodial surveillance, outlining the various parental controls available in monitoring a child's use of Amazon's services. In this addendum, Amazon gives parents "visibility into how their children use our products and services." Using the Amazon Parent Dashboard, a parent or guardian can actively and passively control their child's consumption of media and interaction with Alexa, such as filtering explicit songs from music streaming services, restricting voice shopping, setting daily time limits, reviewing activity, and pausing Alexa on their child's device. The Parent Dashboard provides a summary of the content that kids have accessed during "FreeTime," an optional monthly subscription providing access to abundant content suitable for children under the age of thirteen. The Parent Dashboard also provides "conversational points" based on the content that children have accessed, encouraging parents to speak to their kids about their media consumption and interaction with Alexa (Amazon n.d.b). Despite Amazon's emphasis on parental controls as a form of "visibility," the conversational points resonate with Foucault's notion of the "incitement to discourse" (Foucault 1978: 17). As with confessional discourse, the Parent Dashboard helps localize power in the act of listening by prompting children to openly discuss with their parents or guardians what they have consumed and learned through Amazon's services.

During the contemporary timeframe, Amazon added a section called the "Alexa Calling and Messaging Schedule" to the "Alexa Terms of Use" (October 24, 2017). Users can opt in to the "Alexa Calling and Messaging Schedule," which gives the Echo access to one's phone number, phone contacts, message history, and call record metadata. This is a significant development that allows Amazon to identify and monitor social connectivity with relatives, friends, and other contacts. Within this section, Amazon added a further optional feature called "Drop In." Drop In allows the user to remotely activate the audio signal (and video signal for compatible devices) of an external device for instant communication with any permissioned Echo user from one's contact list, acting as an intercom between Echo devices on a local network or between households via the internet. Arguably the most substantial privacy concern here is that, after exchanging Drop In permission with a contact, everyone in the user's household and that contact's household also grants and receives Drop In permission. This raises issues of power dynamics in households and families because one user is able to extend Drop In permission to a contact on behalf of the entire household or family.

The final feature that I would like to address, called "Voice Profiles," was added to the "Alexa Terms of Use" (October 24, 2017), and it allows users to create and upload an "acoustic model" of their voice to Amazon's servers. This was initially released as an opt-in feature that required users to manually upload samples of their recorded speech. Amazon states that it will automatically delete these biometric profiles if a user stops using Alexa and their voice has not been recognized for three years (Amazon n.d.a). This feature was subsequently updated in the "Alexa Terms of Use" (November 27, 2018) as "Automatic Voice Recognition & Voice Profiles," allowing Alexa to "automatically recognize the voices of users in your household over time." This automatic process of biometric enrollment now requires a user to opt out on behalf of the entire household. Additionally, as per the "Changes to Services; Amendments" from the "Amazon Echo Terms of Use," Amazon was not required to notify users about this change. The technology now operates by passively learning the voice profiles of everyone in the household even if only one user has explicitly provided their consent to the EUAs. Further, frequent visitors in one's household who come into contact with Alexa may also be targeted for their voice profiles. Amazon continues to delete these biometric profiles after three years of inactivity, although there is no certainty that all traces of one's data have been permanently deleted from Amazon's servers.

Discussion

The language, length, radical mutability, and intertextuality of the EUAs makes it challenging to read and comprehend their content and to trace their ongoing evolution. Empirical findings (Obar and Oeldorf-Hirsch

2018) reveal that this discursive genre contributes to a common social practice of consumers skipping over EUAs without having read them or having understood the underlying information privacy framework. The discursive formation of Amazon's EUAs articulates two social agendas. First, these documents are made to protect corporate interests by shirking liability and proactively managing the platform's conditions of use. And, second, the EUAs appear designed to purposefully discourage users from reading and making the effort to fully understand their surveillance implications. This powerful combination allows Amazon to stealthily introduce new features and services to its eavesmining platform without raising any immediate alarms about intensifying privacy and surveillance concerns. Users are unreasonably expected to keep themselves informed of any changes to the EUAs—which grow considerably in length over time—without receiving consistent notification from Amazon that would include a comprehensive and readable summary of the changes.

Customer data have always been essential to Amazon's operations, yet, increasingly, it is not only collecting data generated through its web services but is also actively designing new services and products whose main purpose is to collect more data about consumers (West 2019: 28): the release of Amazon's eavesmining platform in November 2014 exemplifies this latest approach. Moreover, Richard Brandt (2011) and Emily West (2019) outline Amazon's deployment of collaborative filtering algorithms that compare consumer purchases, searches, and other datasets with those collected from other consumers with similar preferences, behaviours, and personal identifiers. Eavesmining platforms provide new affordances in delivering personal recommendations, personalization of services, and interest-based advertising.

Beginning in the nascent timeframe, users are required to opt out of having their voice-input data used by Amazon to develop new features and improve Alexa's transcription accuracy and services. A recent privacy scandal surrounding the Echo (Valinsky 2019) arose after Amazon admitted that employees manually listen to voice-input data from customers for transcription analysis. This practice is vaguely reflected in an update to the "Amazon Echo Terms of Use" (March 18, 2015), which mentions the types of data that "may be processed in the cloud to improve your experience and our services." The scandal indicates that consumers were unaware of certain privacy control options and failed to notice the subtle alteration in the EUAs or understand the implications of their ambiguous language. This points to the social problem of introducing opt-out privacy control options in the context of an ever-updating platform and conditions of use. Further, the section on "Information" in the "Amazon Echo Terms of Use" stipulates that any customer information may be stored on servers outside the country in which you live. Indeed, the recent privacy scandal involved full-time employees and contract workers in the United States, Costa Rica, and Romania auditing voice-input data (Valinsky 2019). Thus, change to EUAs articulate intensifying privacy and surveillance concerns within the domestic sphere by amplifying corporate eavesmining processes with a global human auditory and machine learning taskforce.

Amazon requires parental or guardian consent whenever a child is declared as the user of any Amazon service. Beginning in the contemporary timeframe, new monitoring tools are offered to parents or guardians that articulate a form of custodial surveillance. Without being indicated in the EUAs, it is left open as to whether Amazon analyzes interaction data with the Parent Dashboard to refine customer profiles based on parenting styles and relations of trust in families: for instance, based on one's interaction with the Parent Dashboard, Amazon might determine if a user is laissez-faire and trusting or anxious and highly protective in their parenting approach. In providing a form of control to parents and guardians over children's activities, this development in the conditions of use articulates intensifying concerns of corporate surveillance, as user data yielded about households and family relations may be productized through collaborative filtering.

The Voice Profile feature was initially introduced as an opt-in, manual biometric enrollment practice. This was subsequently updated as an automatic data collection practice, requiring the user to opt out on behalf of the entire household. Despite the social significance of this development, Amazon did not update consumers about this change, as per the EUAs. A recent class-action lawsuit has been filed in the United States over this issue, alleging that Amazon lacks parental consent in capturing the "voiceprints" of children (Kelion 2019). Further, the conditions of use potentially affect household guests who interact with the Echo,

having their personal data collected without any awareness of the biometric system or providing personal consent to the EUAs. This development articulates intensifying privacy and surveillance concerns within the domestic sphere, allowing Amazon to passively collect biometric information and automatically recognize the voices of dwellers and visitors within home environments.

Amazon is now capable of monitoring the social connectivity of households with relatives, friends, and other interpersonal contacts after the primary user has opted in to the “Alexa Calling and Messaging Schedule.” With this development, Amazon can determine particularly intimate relations within one’s social network based on two or more users exchanging Drop In privileges between their separate households. The metadata of Drop In interactions indicate the frequency and duration of inter-household communications, although there is no indication in the EUAs as to whether Amazon is also collecting ideational content of Drop In dialogue.⁹ This development in the EUAs prompts intensifying privacy concerns by enabling corporate surveillance of intimate relations and communications.

This discussion of the corporate privacy framework has determined what conditions of use Amazon’s EUAs impose, how these are changing over time to affect individuals and households of users, and how these developments articulate intensifying privacy and surveillance concerns within the domestic sphere. This prompts a final question: how is the domestication of Amazon’s eavesmining platform reproducing and modulating power relations in home environments?

The domestication of the technology localizes power around the Amazon account holder, since it is this person who is charged with the authority of consenting to the EUAs on behalf of others. Significantly, this person is not necessarily the primary user of the device since they may be charged with responsibility for a child, adolescent, or a non-savvy user such as an elderly relative. The Amazon account holder is responsible for managing the privacy control options for the entire household. As a result, negotiation of privacy relations is not evenly distributed amongst all members of a family or household (Pridmore et al. 2019: 130). Features such as Drop In and the Parent Dashboard help reproduce power relations in the domestic sphere by granting the Amazon account holder authority over others, especially non-adult users or visitors in one’s home. Meanwhile, eavesmining processes modulate power relations in home environments by allowing Amazon to monitor one’s use of such features and productize this information by means of collaborative filtering. By charging the Amazon account holder with authority over others, power relations are further modulated because this user is responsible for the platform’s privacy control options, which constantly evolve and are obfuscated in the EUAs. Thus, the domestication of Amazon’s eavesmining platform reproduces power relations by constructing the account holder as an authority figure and modulates relations of mastery in the domestic sphere by granting corporate monitoring privileges within individuated home environments.

In conclusion, this study of Amazon’s conditions of use for its eavesmining platform explicates a mode of consumer monitoring that operates on the edge of sound and data. The documents reveal a combination of dataveillance, sensing-based monitoring, and auditory surveillance practices. I have proposed a sonic epistemology of surveillance that conceptualizes eavesmining dynamics as a vibrational oscillation between modes of dataveillance and sensing-based monitoring, an oscillation that occurs at the edge of acoustic space and digital infrastructure. Findings indicate that user “consent” to Amazon’s eavesmining platform subjects individuals, entire households, and their visitors to the acoustic excavation of smart environments whereby sounds of the past, present, and future may be stored, circulated, and analyzed by data mining techniques that rapidly evolve in scope, variety, and intensity.

Further, the study helps in understanding how the voice—as the primary target of eavesmining processes—is not a neutral carrier of meaning but rather a personally identifying biometric medium that opens a new frontier of auditory surveillance. Based on patents and statements from a corporate executive, Amazon is

⁹ An Amazon patent for a “voice sniffer” algorithm indicates that interpersonal communication over the device may potentially be monitored for keywords and semantic sentiment (Maheshwari 2018).

poised to apply new features and services that would probe voices for non-ideational signifiers, such as semantic sentiment, vocal affect, psychological variables, and, presumably, other vocal qualities such as age, accent, and gender. Although the findings do not provide evidence of ambient auditory surveillance practices by Amazon's eavesmining platform, this remains a significant possibility due to the affordances of the technology. Future research in this area might consider how eavesmining platforms target soundscapes and the unspoken yet audible rhythms of everyday life.

Endemic privacy concerns related to Amazon's eavesmining platform are discursively obfuscated by the illegibility of EUAs. Even with a careful reading and analysis of these documents, a great deal of uncertainty remains about the platform's black boxed technical design and Amazon's application of data mining techniques. To confront this shortcoming, a degree of aural speculation is demanded at this stage to conceptualize the nascent mode of surveillance represented by eavesmining platforms and processes. Put simply, to challenge these developments one must think critically and sonically about surveillance. My critical audit and interpretation of research findings has attempted to do just this by sounding out the social issues of Amazon's eavesmining platform. Future research should approach eavesmining platforms with a critical biometric consciousness (Browne 2015) and an understanding of how the recuperation of historical listening practices and techniques, such as those featured in the psy-disciplines, pose emergent issues of social sorting and discrimination.

References

- Albrechtslund, Anders. 2008. Online Social Networking as Participatory Surveillance. *First Monday* 13 (3).
- Amazon. N.d.a. Alexa and Alexa Device FAQs. <https://www.amazon.com/gp/help/customer/display.html?nodeId=201602230> [accessed April 29, 2019].
- . N.d.b. Parent Dashboard. <https://www.amazon.com/b?node=17395968011> [accessed April 29, 2019].
- Andrejevic, Mark, and Mark Burdon. 2015. Defining the Sensor Society. *Television & New Media* 16 (1): 19–36.
- Bigo, Didier. 2006. Security, Exception, Ban and Surveillance. In *Theorizing Surveillance: The Panopticon and Beyond*, edited by David Lyon, 46–68. Cullompton, UK: Willan Publishing.
- Brandt, Richard L. 2011. *One Click: Jeff Bezos and the Rise of Amazon.Com*. New York: Portfolio Penguin.
- Brinkmann, Svend. 2005. Human Kinds and Looping Effects in Psychology: Foucauldian and Hermeneutic Perspectives. *Theory & Psychology* 15 (6): 769–91.
- Browne, Simone. 2015. *Dark Matters: On the Surveillance of Blackness*. Durham, NC: Duke University Press.
- Chion, Michel. 1994. *Audio-Vision: Sound on Screen*. Translated by Claudia Gorbman. New York: Columbia University Press.
- Clarke, Roger. 1988. Information Technology and Dataveillance. *Communications of the ACM* 31 (5): 498–512.
- Deleuze, Gilles. 1992. Postscript on the Societies of Control. *October* 59: 3–7.
- Dolar, Mladen. 2011. The Burrow of Sound. *Differences* 22 (2–3): 112–39.
- Elmer, Greg. 2003. A Diagram of Panoptic Surveillance. *New Media & Society* 5 (2): 231–47.
- . Greg. 2004. *Profiling Machines: Mapping the Personal Information Economy*. Cambridge, MA: MIT Press.
- Fanon, Frantz. 1982. *Black Skin, White Masks*. Translated by Charles Lam Markmann. New York: Grove Press.
- Fayyad, Usama, Gregory Piatetsky-Shapiro, and Padhraic Smyth. 1996. From Data Mining to Knowledge Discovery in Databases. *AI Magazine* 17 (3): 37–37.
- Children's Online Privacy Protection Act of 1998. 15 U.S.C. §§ 6501–6505. <http://uscode.house.gov/view.xhtml?req=granuleid%3AUSC-prelim-title15-section6501&edition=prelim> [accessed July 9, 2019].
- Foucault, Michel. 1977. *Discipline and Punish: The Birth of the Prison*. Translated by Alan Sheridan. New York: Vintage Books.
- . 1978. *The History of Sexuality*. Translated by Robert Hurley. New York: Vintage Books.
- Gandy, Oscar H. 1993. *The Panoptic Sort: A Political Economy of Personal Information*. Critical Studies in Communication and in the Cultural Industries. Boulder, CO: Westview.
- González, Gerardo M., Colby Carter, and Erika Blanes. 2007. Bilingual Computerized Speech Recognition Screening for Depression Symptoms: Comparing Aural and Visual Methods. *Hispanic Journal of Behavioral Sciences* 29 (2): 156–80.
- Goodman, Steve. 2010. *Sonic Warfare: Sound, Affect, and the Ecology of Fear*. Cambridge, MA: MIT Press.
- Haggerty, Kevin D., and Richard V. Ericson. 2000. The Surveillant Assemblage. *British Journal of Sociology* 51 (4): 605–22.
- James, Robin. 2014. Acousmatic Surveillance and Big Data. *Sounding Out!* (blog), October 20. <https://soundstudiesblog.com/2014/10/20/the-acousmatic-era-of-surveillance/> [accessed April 29, 2019].
- . 2019. *The Sonic Episteme: Acoustic Resonance, Neoliberalism, and Biopolitics*. Durham, NC: Duke University Press Books.
- Kelion, Leo. 2019. Amazon Sued over Alexa Child Recordings. *BBC*, June 13. <https://www.bbc.com/news/technology-48623914> [accessed July 9, 2019].
- Kendall, Gavin, and Gary Wickham. 1999. *Using Foucault's Methods*. London: Sage Publications.
- LaBelle, Brandon. 2018. *Sonic Agency: Sound and Emergent Forms of Resistance*. Cambridge, MA: Goldsmiths Press.

- Lagaay, Alice. 2008. Between Sound and Silence: Voice in the History of Psychoanalysis. *E-Pisteme* 1 (1): 53–62.
- Levin, David Michael. 1997. *Sites of Vision: The Discursive Construction of Sight in the History of Philosophy*. Cambridge, MA: MIT Press.
- Lyon, David. 2001. *Surveillance Society: Monitoring Everyday Life*. Issues in Society. Buckingham, UK: Open University.
- . 2003. *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination*. London: Routledge.
- Maheshwari, Sapna. 2018. Hey, Alexa, What Can You Hear? And What Will You Do With It? *The New York Times*, March 31, 2018. <https://www.nytimes.com/2018/03/31/business/media/amazon-google-privacy-digital-assistants.html> [accessed April 15, 2019].
- Mann, Steve, and Joseph Ferenbok. 2013. New Media and the Power Politics of Sousveillance in a Surveillance-Dominated World. *Surveillance & Society* 11 (1/2): 18–34.
- Mathiesen, Thomas. 1997. The Viewer Society. *Theoretical Criminology* 1 (2): 215–34.
- McLaughlin, Elliott C. 2017. Suspect OKs Amazon to Hand over Echo Recordings in Murder Case. *CNN*, April 26. <https://www.cnn.com/2017/03/07/tech/amazon-echo-alexa-bentonville-arkansas-murder-case/index.html> [accessed April 29, 2019].
- Mitra, Vikramjit, Elizabeth Shriberg, Dimitra Vergyri, Bruce Knoth, and Ronald M. Salomon. 2015. Cross-Corpus Depression Prediction from Speech. In *2015 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, Brisbane, QLD, April 19–24, 4769–73.
- Miyazaki, Shintaro. 2013. AlgoRhythmic Sorting. *Adafruit Industries - Makers, Hackers, Artists, Designers and Engineers!* (blog), September 10. <https://blog.adafruit.com/2013/09/10/algorithmic-sorting-by-shintaro-miyazaki/> [accessed June 9, 2019].
- . 2016. Algorithmics, Media Archaeology and Beyond. *Medium*, March 30. <https://medium.com/@algorithmics/algorithmics-archaeology-and-beyond-2eff6595e6ab> [accessed June 9, 2019].
- Nataraja, Prem, interview by Rachel Crane. 2018. Amazon is Using AI in Almost Everything it Does. *CNN*, video, October, 3. <https://www.cnn.com/videos/business/2018/10/03/amazon-ai-behind-the-scenes-orig-mss.cnn-business> [accessed April 14, 2019].
- Obar, Jonathan A., and Anne Oeldorf-Hirsch. 2018. The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services. *Information, Communication & Society* 23 (1): 128–147.
- Poster, Mark. 1990. *The Mode of Information: Poststructuralism and Social Context*. Cambridge, UK: Polity Press.
- Pridmore, Jason. 2013. Collaborative Surveillance: Configuring Contemporary Marketing Practice. In *The Surveillance-Industrial Complex: A Political Economy of Surveillance*, edited by Kirstie Ball and Lauren Snider, 107–21. London: Routledge.
- Pridmore, Jason, Michael Zimmer, Jessica Vitak, Anouk Mols, Daniel Trottier, Priya C. Kumar, and Yuting Liao. 2019. Intelligent Personal Assistants and the Intercultural Negotiations of Dataveillance in Platformed Households. *Surveillance & Society* 17 (1/2): 125–31.
- Rajchman, John. 1988. Foucault's Art of Seeing. *October* 44: 89–117.
- Reik, Theodor. 1949. *Listening with the Third Ear: The Inner Experience of a Psychoanalyst*. New York: Farrar, Straus, and Giroux.
- . 1958. *Ritual: Psycho-Analytic Studies*. New York: International Universities Press.
- Scherer, Stefan, Gale M. Lucas, Jonathan Gratch, Albert Skip Rizzo, and Louis-Philippe Morency. 2016. Self-Reported Symptoms of Depression and PTSD Are Associated with Reduced Vowel Space in Screening Interviews. *IEEE Transactions on Affective Computing* 7 (1): 59–73.
- Stark, Luke. 2018. Algorithmic Psychometrics and the Scalable Subject. *Social Studies of Science* 48 (2): 204–31.
- Sterne, Jonathan. 2003. *The Audible Past: Cultural Origins of Sound Reproduction*. Durham, NC: Duke University Press.
- Stoever-Ackerman, Jennifer. 2010. Splicing the Sonic Color-Line Tony Schwartz Remixes Postwar Nueva York. *Social Text* 28 (102): 59–85.
- . 2011. The Word and the Sound: The Sonic Color-Line in Frederick Douglass's 1845 Narrative. *SoundEffects - An Interdisciplinary Journal of Sound and Sound Experience* 1 (1): 19–36.
- Szendy, Peter. 2016. *All Ears: The Aesthetics of Espionage*. Translated by Roland Végső. New York: Fordham University Press.
- Valinsky, Jordan. 2019. Amazon Reportedly Employs Thousands of People to Listen to Your Alexa Conversations. *CNN*, April 11. <https://www.cnn.com/2019/04/11/tech/amazon-alexa-listening/index.html> [accessed April 29, 2019].
- Weiner, Sophie. 2018. Walmart Patents Audio Surveillance Tool to Monitor Employee Conversations. *Splinter*, July 11. <https://splinternews.com/walmart-patents-audio-surveillance-tool-to-monitor-empl-1827529033> [accessed April 15, 2019].
- West, Emily. 2019. Amazon: Surveillance as a Service. *Surveillance & Society* 17 (1/2): 27–33.
- Zuboff, Shoshana. 2015. Big Other: Surveillance Capitalism and the Prospects of an Information Civilization. *Journal of Information Technology* 30 (1): 75–89.
- . 2019. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: Public Affairs.