Sonic Privacy

Jasmine E. McNealy[†]

Introduction

We make noise.

That is, we make sounds, both intentional and unintentional, organic, and unwanted, with our bodies: our voices and heartbeats, or rhythms inaudible to the naked ear. These sounds we make are ripe for use for law enforcement investigations,[1] human resources

[†] Associate Professor in the University of Florida College of Journalism and Communications; Associate Director of the Marion B. Brechner First Amendment Project. I am grateful to the Yale Information Society Project and Michigan State University's Quello Center for helpful discussions related to the ideas in this Article.

[1] Alexandra S. Gecas, Note, *Gunfire Game Changer or Big Brother's Hidden Ears: Fourth Amendment and Admissibility Quandaries Relating to Shotspotter Technology*, 2016 U. ILL. L. REV. 1073; Christopher Benjamin, *Shot Spotter and FaceIt: The Tools of Mass Monitoring*, 6 UCLA J.L. & TECH. 1 (2002).

decisions,[2] and to attempt identifications.[3] Sounds are "sonic data," which I define as those *representations or observations* that define the characteristics of sound and its cognitive and emotive forces.[4] "Sonic" is traditionally used in reference to sounds that can be heard by the human ear, a range of around 20 Hz to 20 KHz.[5] Sounds outside of this range are infrasonic (below traditional hearing range) or ultrasonic (above traditional hearing range). Organizations collect data in all these ranges. Advertisers, for example, can use ultrasonic beacons to track users on their mobile devices through the microphone and ultrasound-enabled apps.[6] I include all three ranges in my definition of sonic data, as advances in data collection and processing have facilitated ultra- and infra-sonic machine-listening and learning. Advertisers, of course, use ultrasonic data to send personalized advertisements;[7] at the same time, civil society organizations collect and process voice data to identify refugees.[8]

---

[2] *See* Winifred R. Poster, *Sound Bites, Sentiments, and Accents: Digitizing Communicative Labor in the Era of Global Outsourcing*, *in* DIGITALSTS 240-262 (Janet Vertesi & David Ribes eds., 2019) (describing how AI is used to evaluate call center workers); Josh Dzieza, *How Hard Will the Robots Make Us Work?*, THE VERGE (Feb. 27, 2020), https://www.theverge.com/2020/2/27/21155254/automation-robots-unemployment-jobs-vs-human-google-amazon (same).

[3] *See* Michelle Hampson, *The Bioacoustic Signatures of Our Bodies Can Reveal Our Identities*, IEEE SPECTRUM (Nov. 4, 2019), https://spectrum.ieee.org/the-bioacoustic-signatures-of-our-bodies-can-reveal-our-identities.

[4] *Accord* Cohen v. California, 403 U.S. 15, 26 (1971) (opining that linguisitic expressions serve not only to convey ideas, but also to express emotions).

[5] Liwei Song & Prateek Mittal, *POSTER: Inaudible Voice Commands*, *in* PROCEEDINGS OF THE 2017 ACM SIGSAC CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY 2583, 2583 (2017); Francisco Gonçalves, Vítor Carvalho & José Machado, *Tool Development for Human Audible Spectrum Compensation*, 2 RECENT INNOV. MECHATRON. 6, 8 (2015).

[6] *See, e.g.*, Daniel Arp et al., *Privacy Threats through Ultrasonic Side Channels on Mobile Devices*, 2017 IEEE EUR. SYMP. ON SEC. & PRIV. 35, 35; Vasilios Mavroudis et al., *On the Privacy and Security of the Ultrasound Ecosystem*, 2 PROC. ON PRIV. ENHANCING TECH. 95, 95-96 (2017).

[7] *Supra* note 6.

[8] *E.g.*, Kerrie Holloway et al., Digital Identity, Biometrics and Inclusion in Humanitarian Responses to Refugee Crises 14-20 (unpublished Humanitarian Pol'y Grp. working paper), at https://cdn.odi.org/media/documents/Digital_IP_Biometrics_case_study_web.pdf.

These examples illustrate new frontiers in sound collection and processing for various purposes.

A growing area of scholarly research uses sound to identify persons or groups. Although the study of animal bioacoustics has existed for centuries,[9] the use of human body sounds for biometric purposes is a relatively new and growing scientific field. Recent studies indicate a concerning turn for this kind of data. For example, one study announced in May 2021 that human body vibrations could be used as personal identification.[10] The researchers developed a tool that, when applied to a participant's fingers, could collect microvibrations and information about the participant's anatomy, biomechanics, and tissues, allowing the capture of a unique bioacoustic signature. They were able to identify subjects with a 97.16% accuracy rate.[11] Of course, this study was not the first scientific foray into the use of bioacoustics for identification; scientists have also examined the use of heart sounds for personal identification.[12] During the continued COVID-19 pandemic, technology developers and scientists have worked to use the sounds of coughs to make diagnoses.[13] Beyond research, voice and voice data also continue to be used to identify and presumptively assess or predict emotion in marketing and other settings.[14]

Voice, probably the most recognizable kind of sonic data, has the potential to be both publicly accessible and audible to the natural ear.[15] Joseph Turow, for example, investigated the use of voice by

---

[9] *See, e.g.*, Robert Dooling & Micheal L. Dent, *A Brief History of Avian Bioacoustics*, 143 J. ACOUSTICAL SOC'Y AM. 1766 (2018).

[10] *See* Joo Yong Sim et al., *Identity Recognition Based on Bioacoustics of Human Body*, 51 IEEE TRANSACTIONS ON CYBERNETICS 2761 (2021).

[11] *Id.* at 2762.

[12] *E.g.*, Tao Ye-wei et al., *A Biometric Identification System Based on Heart Sound Signal*, 3 CONF. ON HUM. SYS. INTERACTION 67, 67 (2010).

[13] Betsy McKay, *Coughs Say a Lot About Your Health, if Your Smartphone Is Listening*, WALL ST. J. (Sept. 8, 2021), https://www.wsj.com/articles/diagnose-respiratory-illness-smartphone-11631041761; Harry Coppock et al., Comment, *COVID-19 Detection from Audio: Seven Grains of Salt*, 3 LANCET DIGITAL HEALTH e537, e538 (2021).

[14] *See generally* Joseph Turow, THE VOICE CATCHERS: HOW MARKETERS LISTEN IN TO EXPLOIT YOUR FEELINGS, YOUR PRIVACY, AND YOUR WALLET (2021).

[15] See Elizabeth Stokoe, *Public Intimacy in Neighbour Relationships and Complaints*, 11 SOC. RES. ONLINE 1 (2006), available at:

marketers looking to use voice data to predict an individual's potential purchases. This *voice intelligence industry*—"an emerging sector of society that involves smart speakers, car information systems, customer service calls to contact centers, and 'connected-home' devices such as thermostats, home-security alarms and other tools"—now makes inferences about an individual's personality and emotional state through the collection of voice data with the goal of using this data to create personalized persuasion tactics.[16] Use of voice data collected in private, semi-private, and public settings to predict consumption decisions creates more than simply the possibility of profit for marketers. It also impacts privacy expectations and our willingness to participate in the public sphere—the spaces of deliberation, self-governance, and interaction—because of the growing recognition that even the once-innocuous noises we made in public can now be used to make inferences and predictions about us.[17]

This essay argues for the recognition of sonic privacy to protect (non)participation in the public sphere through a framework for the creation of policy that restrains machine interactions with sonic data. Sounds, sonic data, are environmental; they inhabit the surroundings, although they are products of an individual's network: their bodies, connected devices, and other sounds networked to their identities. In this respect, sound is ecological—it is part of the system that provides details about an individual and their "social context, both formal and informal."[18] The collection and use of sound, like that of all kinds of human-related data, allows for the creation of inferences and predictions about individuals and can modify individual behavior because of constant surveillance.[19] Scholars across disciplines have discussed how the perception of

---

https://www.socresonline.org.uk/11/3/stokoe.html; Elizabeth Stokoe & Alexa Hepburn, *'You can hear a lot through the walls': Noise formulations in neighbour complaints*, 16 DISCOURSE & SOC'Y 647 (2005).

[16] Joseph Turow, *Journalism and the Voice Intelligence Industry*, 9 DIGITAL JOURNALISM 1000, 1001 (2021). For a fuller inquiry into how marketers use voice, see TUROW, *supra* note 14.

[17] *See* TUROW, *supra* note 14, at 77-81.

[18] Urie Bronfenbrenner, *Toward an Experimental Ecology of Human Development*, 32 AM. PSYCH. 513, 514 (1977).

[19] *See generally* Yong Jin Park, *Structural Logic of AI Surveillance and Its Normalisation in the Public Sphere*, 28 JAVNOST: PUB. 341 (2021); MICHEL FOUCAULT, DISCIPLINE AND PUNISH: THE BIRTH OF THE PRISON (1975).

being watched changes how people act, identifying these changes as various kinds of observer effects.[20] The power of constant surveillance to influence human behavior, coupled with people's fear of possible punishment or the negative outcomes of information collection and use, requires sophisticated law and policy-making to protect public and private life from machine processing. Therefore, in creating a framework for sonic privacy, I use an ecological approach, looking to the "relationships/connections that can and/or should influence governance choices, the institutions and societal structures that impact governance and who will be tasked with enforcement and implementation."[21] This approach also addresses the environment in which sound is created and used by considering how individuals, organizations, and environments interact to shape sonic privacy rights. At its foundation, this framework for sonic privacy examines individuals' rights in their sonic emissions. It furthermore distinguishes between sounds passively heard by other individuals and sounds actively collected through technological machinations.

I. Lessons from Sound Law

Sound-related privacy has traditionally been discussed in studies of construction or architectural design. These studies consider the opposition between unmediated access to sound and an individual's right (and opportunity) to refrain from encountering sound. They also consider organizational attempts at masking sound in employment and living contexts. The research examines, for

---

[20] *See* Shoshana Zuboff, *Big Other: Surveillance Capitalism and the Prospects of an Information Civilization*, 30 J. INFO. TECH. 75, 82 (2015) ("In this world of no escape, the chilling effects of anticipatory conformity give way as the mental agency and self-possession of anticipation is gradually submerged into a new kind of automaticity."); Luke F. Chen et al., *The Hawthorne Effect in Infection Prevention and Epidemiology*, 36 INFECTIOUS CONTROL & HOSP. EPIDEMIOLOGY 1444, 1445-46 (2015) (explaining that participants of medical studies may alter their behavior partly because they are aware that they are under observation); Oscar H. Gandy, Jr., *The Surveillance Society: Information Technology and Bureaucratic Social Control*, 39 J. COMMC'N. 61, 71 (1989) (discussing studies suggesting that people value privacy more when they believe they have less control over their personal information).

[21] Jasmine E. McNealy, *An Ecological Approach to Data Governance*, 37 NOTRE DAME J.L. ETHICS & PUB. POL. (forthcoming 2022) (manuscript at 16).

example, the design of workplaces,[22] and has helped develop rating systems for speech privacy, or privacy influenced by how voices travel in modern buildings. It shows that perceived speech privacy in buildings is more related to the intelligibility of overheard noise than it is to volume.[23]

Sound-related privacy studies have also considered the affirmative creation of a zone or space of privacy.[24] For example, drivers play music partly to ensure privacy in their cars.[25] Other studies explored how the ability to hear coital sounds of another couple, though accidental, changed the intimacy of other couples.[26] Coital sound privacy studies differ from other prior literature focused on the individuals receiving sound, instead exploring the implications on individuals who may, at some point, be sound creators. They focus on the expectations of individuals as sound producers. More importantly, in these studies, coital sound is framed as "sound pollution," from which no zone of privacy could be created to protect others from overhearing. Because this kind of sound impacts the individuals in the surrounding environment despite attempts at creating a space for privacy, it transgresses the public/private boundary.[27]

---

[22] *See generally* Nomana Anjum et al., *Privacy in the Workplace Design*, 7 DESIGN J. 27 (2004); A. C. C. Warnock, *Acoustical Privacy in the Landscaped Office*, 53 J. ACOUSTICAL SOC'Y AM. 1535 (1973).

[23] W. J. Cavanaugh et al., *Speech Privacy in Buildings*, 34 J. ACOUSTICAL SOC'Y AM. 475, 476 (1962). "Noise" has long been defined as unwanted or undesired sound, although this definition may be obsolete. *See* Daniel Fink, *A New Definition of Noise: Noise is Unwanted and/or Harmful Sound. Noise is the New 'Secondhand Smoke,'* 39 PROC. MEETINGS ON ACOUSTICS 1, 2 (2019) (recounting the history of the definition but arguing its obsolescence).

[24] *See, e.g.*, Nigel Helyer, *The Sonic Commons: An Embrace or Retreat?*, 14 INT'L SYMP. ELEC. ART 217 (2008); Nicola Dibben & Victoria J. Williamson, *An Exploratory Survey of In-Vehicle Music Listening*, 35 PSYCH. MUSIC 571 (2007).

[25] Michael Bull, *Soundscapes of the Car: A Critical Study of Automobile Habitation*, *in* CAR CULTURES 185, 192-93 (Daniel Miller ed., 2001). Music "exorciz[es] . . . the random sounds of the environment by the mediated sounds of the cassette or radio." *Id.* at 187.

[26] *E.g.*, Craig M. Gurney, *Transgressing Private-Public Boundaries in the Home: A Sociological Analysis of the Coital Noise Taboo*, 13 VENEREOLOGY 39, 39 (2000).

[27] *See id.* at 40 ("[C]oital noise . . . respects none of the boundaries with which intimate and private spaces are usually encircled.").

II. The Public versus Private Problem

The public versus private dichotomy is one of the hallmarks of the privacy debate in the United States, which seeks to define whether an individual has a reasonable expectation of privacy based on the "location" of the activity, behavior, or data at issue. This dichotomy also considers whether the individual maintains "control" over information disclosed. A usual refrain is that a person has the highest expectation of privacy in their own home. In *Dietemann v. Time, Inc.*,[28] for example, a man sued *Time* magazine after it published a story painting him as a quack doctor using quotes and photos gathered from a hidden camera and microphone that the magazine's reporters surreptitiously brought into his home. The reporters were invited into the man's home after posing as patients seeking his medical help.[29] The Court ruled that when Dietemann invited the reporters into his private home, where he had the greatest expectation of privacy, he did not assume the risk that his actions or conversation would be photographed or recorded.[30] Further, the court declined to recognize the hidden camera and recording device as "indispensable tools of investigative reporting."[31]

In contrast, individuals are said to have the lowest expectation of privacy in public, and generally courts have found no invasion of privacy when individuals have engaged in activities in a public setting. In *Wilkins v NBC, Inc*.,[32] for example, a California appellate court ruled that two businessmen had no expectation of privacy in a conversation that took place during a lunch meeting held on the outdoor patio of a restaurant.[33] Two producers for NBC contacted SimTel, a pay-per-call company, in response to a national advertisement, arranged a lunch meeting with company representatives, and surreptitiously recorded the SimTel representatives, later broadcasting excerpts from the recording.[34] The California appellate court found no invasion of privacy because

---

[28] 449 F.2d 245 (9th Cir. 1971).

[29] *Id.* at 246. The reporters initiated the investigation in conjunction with the District Attorney's Office of Los Angeles County. *Id.*

[30] *Id.* at 249.

[31] *Id.*

[32] 84 Cal. Rptr. 2d 329 (1999).

[33] *Id.* at 336.

[34] *Id.*

no reasonable expectation of privacy existed in either the location nor the subject matter of the conversation; the men had freely spoken about their business in a public place.[35] The journalists had not intruded into the men's private lives or homes; "NBC photographed the two men in a public place and taped their conversations which were about business, not personal matters. There was no intrusion into a private place, conversation or matter."[36] The men had no reasonable expectation of privacy in their lunch discussion.

But cases like *Dietemann* and *Wilkins* provide little in the way of answering how our expectations should reflect the fact that many of the ways we engage with the world have both public and private components. Although a person might, for example, take a call on their mobile phone out in public, they would probably not expect someone to follow them to listen. Helen Nissenbaum dismisses the public/private dichotomy outright and advocates for a view of privacy as "contextual integrity," which focuses on adequate information flows rather than artificially distinguishing between private and public information.[37] This approach rejects theories of privacy that place a premium on control and access or which draw strict boundaries around "zones of privacy," and instead focuses on the flows of personal information and the norms that are appropriate to governing these flows in context.

Nonetheless, the public versus private dichotomy persists in American law and shapes the reasonable expectations of personal privacy, which are supposed to reflect objective societal expectations and to avoid the subjective judgments, or "idiosyncratic individual preferences."[38] But the cases briefly presented above are hardly dispositive of a settled judicial interpretation of the expectation of privacy based on whether an individual is deemed to have been in public or private. It is the cases in which the designation of public versus private is more complex that offer suggestions for better understanding privacy, particularly

---

[35] *Id.*

[36] *Id.*

[37] HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE 116-19, 129-37 (2009).

[38] DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 71 (2009) After all, "[s]ome individuals may have an unusually strong desire for privacy and may make impossible demands for privacy." *Id.*

in relation to sound. The courts do not necessarily decide these cases based on whether another person could hear the sounds, but on whether the individual making the sound could expect that the person who might overhear would not use that information in ways beyond the context of the setting.

Consider, for example, *Sanders v. ABC, Inc.*, in which a reporter secretly recorded the conversations of her co-workers while working as a telephone psychic.[39] The *Sanders* court noted that although California law required the plaintiff to prove that they had a reasonable expectation of privacy, this did not mean that the privacy had to be "*absolute* or *complete*."[40] The use of technology to collect and record information "may constitute an intrusion [on privacy] even when the events and communications recorded were visible and audible to some limited set of observers at the time they occurred."[41] In other words, seclusion is relative; even though an individual did not have an expectation of confidentiality in a conversation in the sense that it would not be overheard, they might have a reasonable expectation of privacy that the conversation would not be recorded.[42] "There are degrees and nuances to societal recognition of our expectations of privacy; the fact that the privacy one expects in a given setting is not complete or absolute does not render the expectation unreasonable as a matter of law."[43]

The events leading to *Sanders* occurred in a call center, a place often holding many employees in an open space with workstations. Yet the court was unpersuaded that the employees were without an expectation that their conversations would not be recorded and then published widely. This expectation was reasonable despite the employees not being in complete control of the information once it was disclosed, or the space in which it was disclosed. In other words, the opinion ignored the strict traditional approach. Instead, it looked

[39] 978 P.2d 67 (Cal. 1999).

[40] *Id.* at 71.

[41] *Id.* at 72.

[42] *Id.*

[43] *Id.*

to the degree of control an individual reasonably expected to exercise over the information giving rise to a privacy lawsuit.[44]

The court had reached a similar conclusion in the earlier case of *Shulman v. Group W. Productions, Inc*,[45] which arose when a film crew rode along with a medical helicopter team to a car accident. A camera crew filmed both the rescue and the medical care at the scene and within the helicopter; the flight nurse wore a microphone that recorded conversations with the patient.[46] The footage and sound were later broadcast as part of a documentary.[47] The court found that the patient was entitled to privacy in her conversations with the flight nurse at the scene, and in the information being relayed about her.[48] The circumstances, including the setting, the degree of intrusion, and the motives for the recordings, were determinative for this ruling.[49] According to the court, a reasonable jury could find that the recording and the filming inside the helicopter were "[i]nformation collecting techniques that may be highly offensive when done for socially unprotected reasons," which might include continuous surveillance.[50]

Sanders and *Shulman* are but two of many instances in which the traditional understanding of the public/private dichotomy did not withstand scrutiny when applied in context, as Nissenbaum discusses in her approach. Lior Strahilevitz, too, has discussed the need to move away from the hard-and-fast public/private dichotomy, which he called "abstract, circular, and highly indeterminate," toward thinking more about how information moves

---

[44] Contrast *Sanders*, with, for example, *U.S. Dep't of Just. v. Reps. Comm. for Freedom of Press*, 489 U.S. 749, 770 (1989) (holding that individuals do not lose their privacy interests simply by participating in an event that is not wholly private).

[45] 955 P.2d 469 (Cal. 1998).

[46] *Id.* at 474-475.

[47] *Id.* at 475.

[48] *Id.* at 491.

[49] *Id.* at 493.

[50] *Id.* The court's definition of "socially unprotected reasons" included, but was not limited to, "harassment, blackmail or prurient curiosity." *Id.* In other words, the court differentiated the acceptableness of constant surveillance based on the party involved in the watching.

through networks and what that means for privacy.[51] He argues for a social science-based understanding of the "extent of dissemination the plaintiff should have expected to follow his disclosure of that information to others."[52] According to Strahilevitz, this expectation is not subjective and can be shaped by structural and cultural factors that influence when and whether information is shared. For example, the culture of Alcoholics Anonymous, illness support groups, and other community groupings on sensitive issues is one of non-disclosure, in which those attending or encountering the information understand that information is not to be shared with outsiders.[53]

In sum, just because information is shared or communicated in the presence of others and, therefore, the sharer can no longer fully control that information, does not mean that the information does not carry a reasonable expectation of privacy or non-disclosure. The above-mentioned cases indicate that sound can be personal information to which individuals might attach a reasonable expectation of privacy. That is, sounds made by or pertaining to humans can be used to identify and make inferences about that person, as well as those to whom the individual is networked in some way; such uses might cause shame, humiliation, and discrimination. In the next section, I demonstrate how court opinions in wiretapping and eavesdropping cases show that the law can be responsive to such deleterious effects.

III. Active versus Passive

Title III of the Omnibus Crime Control and Safe Streets Act of 1968, as amended by the Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510-2520 (Title III) prohibits the intentional interception and/or disclosure of any "wire, oral or electronic communication,"[54] and many states have similar laws prohibiting the interception and disclosure of private communications. Cases

---

[51] Lior Strahilevitz, *A Social Networks Theory of Privacy*, 72 U. CHI. L. REV. 919, 921 (2005); *see also* Jasmine E. McNealy, *The Privacy Implications of Digital Preservation: Social Media Archives and the Social Networks Theory of Privacy*, 3 ELON L. REV. 133, 151 (2012).

[52] Strahilevitz, *supra* note 51, at 921.

[53] *Id*. at 959-962.

[54] *See* 18 U.S.C. §§ 2510-2520.

that fall under these laws often involve hidden cameras or microphones. Many of the rulings in these cases turn on whether there was active or passive involvement in the recording or data collection.

The Supreme Court's foray into differentiating between active and passive data collection was *Bartnicki v. Vopper*,[55] a case involving the interception and then radio broadcast of a cellphone conversation. Usually thought of as a First Amendment case, *Bartnicki* also involved privacy rights. The case arose when an unknown party intercepted and recorded a conversation between a teachers union negotiator and the president of the union, then delivered the recording to the head of the local taxpayers' organization, who sent the tape to media outlets including a local radio journalist who played it on his talk show.[56] Both the union president and chief negotiator sued the radio journalist for violating both federal and Pennsylvania state wiretap statutes.[57] The Court recognized that the radio journalist played no role in intercepting and recording the union members' conversation; punishing him would not deter third parties from intercepting and recording conversations.[58] The radio journalist did not actively intercept the phone conversation or make recordings; he had only been provided access. More importantly, the *Bartnicki* opinion provides further critical considerations for sound law: *how* sound is obtained can determine liability.

A second important consideration is the "public interest" in the contents of the recordings. The Court ruled in *Bartnicki* that in context—a very public and acrimonious negotiation between the public teacher's union and the school board—the content of the recording was of public importance. This meant that the use of the information contained in the recording served a purpose that appeared to outweigh the privacy interests of those who were recorded. Although under normal circumstances, the speakers'

---

[55] 532 U.S. 514 (2001).

[56] *Id.* at 519.

[57] *Id.* at 520.

[58] *Id.* at 530. The Court also rejected the idea that the unlawful conduct of a third-party should be grounds to prohibit publication by the press, finding "no empirical evidence to support the assumption that the prohibition against disclosures reduces the number of illegal interceptions." *Id.* at 531.

privacy interest in not having their private conversation broadcast would be of paramount importance, it was dispositive that this conversation contained information potentially useful to the public in making governance decisions.[59]

Although the Court in *Barnicki* did not find that the journalist had actively participated in the information collection, a wealth of lower federal court cases exists in which the courts have ruled that active participation in surreptitious recording creates liability under § 2511(2)(d) of Title III, which allows someone who is involved in a conversation to record without the knowledge or consent of the other parties. This is called "one-party" consent because, presumably, the party recording is the only party consenting.[60] One-party consent does not apply, however, if the recording is made to commit a crime or to injure another party, or if the recorder was not an actual participant in the conversation. Therefore, plaintiffs in Title III civil actions often argue that the interceptor/recorder was not a party to the communication, or that the recording was made with the intent to commit an injury. For the most part, the courts have ruled in favor of the party that recorded, broadly defining the parties to a communication and almost never finding an intent to break the law or cause harm by recording.[61]

But these rulings contradict what participants in a conversation might reasonably expect, particularly when compared to the *Sanders*/*Shulman* cases, which dealt with the complexity of communication and expectations between parties. It is one thing to

---

[59] *See id.* at 534 (asserting that privacy concerns give way when balanced against the interest in publishing matters of public importance).

[60] 18 U.S.C. § 2511(2)(d). The statute states:

> It shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire, oral, or electronic communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State.

Id.

[61] *See, e.g.*, Smith v. Cincinnati Post & Times-Star, 475 F.2d 740, 741 (6th Cir. 1973) (finding that it was not unlawful for a party to a communication to later publish the contents of that communication).

overhear a conversation; we regularly overhear the sounds made by others. Technology, however, allows listeners to hear more than they could with the natural ear. Likewise, reasons may exist to record a conversation for personal use. Those reasons for recording that conversation begin to lose their legitimacy when the recording is widely distributed and then used for purposes beyond the speaker's imagination. The use of technology in these cases amplifies the harm. Hidden recorders make it so that it is no longer merely a conversation that was overheard, but a conversation that was memorialized and made available for use and distribution to others with absolutely no connection to the original speakers. Rulings like these ignore the structural and cultural factors, as Strahilevitz identifies them, in the creation of norms about information disclosure in particular communities. A definition of privacy with its focus on whether the speaker is always in control of information is archaic and is out of touch with the way people behave. Therefore, while prior sound law cases offer some direction for considering what needs to be done so that law and policy are adequately able to deal with the further advances in sonic data collection and analysis, their normative shortcomings demonstrate the need for critical considerations of human sociality and the realities of everyday life, especially human participation in the public sphere.

IV. Sound and the Public Sphere

A traditional description of the public sphere is that it is a space for deliberation.[62] Under the Habermasian tradition, mass media, along with places like pubs, coffee houses, and civic organizations, represent spaces for deliberative communication, and lead to discussions of public affairs. These discussions offer the opportunity for civic participation and are connected to the idea of healthy self-governance.[63] The *choice* to participate in a shared or deliberative system, as opposed to a private world, is a hallmark of the Habermasian idea of the public sphere. Important for the idea of

---

[62] JURGEN HABERMAS, THE STRUCTURAL TRANSFORMATION OF THE PUBLIC SPHERE: AN INQUIRY INTO A CATEGORY OF BOURGEOIS SOCIETY 27 (Thomas Burger trans., MIT Press 1991).

[63] Zizi Papacharissi, *The Virtual Sphere: The Internet as a Public Sphere*, 4 NEW MEDIA & SOC'Y 9, 15, 17 (2002); Lincoln Dahlberg, *Visibility and the Public Sphere: A Normative Conceptualisation*, 25 JAVNOST: PUB. 35, 35 (2018).

participation is the concept of visibility, which is key to understanding the *publicness* of the public sphere.[64] According to Lincoln Dahlberg, visibility can be defined as "disclosure or opening of norms and political power to scrutiny by all affected persons, persons granted the freedom to form and make visible (as in express and publish) their opinions through participation in rational public debate."[65] For digital technology, visibility is the ability to be noticed or heard, "in the sense of being respected or recognized."[66] But visibility is more than being noticed or unnoticed. It is also centered on the control of whether information is made available, whether that information is permitted to be shared, and whether third parties may access it.[67]

Dahlberg identifies six normative visibility conditions necessary for the formation of a public sphere: the visibility of dissensus, the visibility of reasoned argumentation about conflicts, participatory equality, exposure to the processes of powerful actors, autonomy from coercion from external forces, and a recognition of the impossibility of normative conditions and, therefore, the need for the existence of counter-publics.[68] As this essay focuses on sonic privacy, it is concerned with how the collection and use of sonic data can impact how we might participate in the public sphere. This focus demands an investigation of the implications of the conflict between sound creators (us) and the organizations capturing sonic data. Three of Dahlberg's factors are especially relevant to this inquiry: 1) the impact of sound data collecting systems on participatory equality, 2) exposure to the processes of powerful actors, and 3) autonomy from coercion from external forces.

Although Dahlberg calls these normative conditions of visibility, with sonic data, I reframe them as conditions of *audibility*. Audibility includes the choice of whether to be heard, and the choice of the kinds of sonic products we place in the public sphere. Each of

---

[64] Dahlberg, *supra* note 63, at 38; ANDREA MUBI BRIGHENTI, VISIBILITY IN SOCIAL THEORY AND SOCIAL RESEARCH 109 (2010).

[65] Dahlberg, *supra* note 63, at 35-36.

[66] Cornelia Brantner & Helena Stehle, *Visibility in the digital age: Introduction*, 21 STUD. COMMUN. SCI. 93, 93 (2021).

[67] *See generally* Mikkel Flyverbom et al., *The Management of Visibilities in the Digital Age*, 10 INT'L J. COMMC'N 98 (2016).

[68] Dahlberg, *supra* note 63, at 37-39.

the three normative conditions influences sonic participation. First, participatory equality is defined as the ability of all parties in a deliberation to be seen or heard, as well as their ability to set limitations on being seen or heard.[69] The problem of participatory equality in the conditions of audibility is that, often, sonic products are collected without regard for whether an individual wants to be heard, or any consideration of how they might allow these products to be used. Undergirding these concerns is datafication or the transformation of interactions into "quantified format[s] so that [they] can be tabulated and analyzed."[70] While some scholars have championed the potential of datafication and fields like data science that uses these datafied products, other scholars have suggested caution with *dataism*—the "widespread *belief* in the objective quantification and potential tracking of all kinds of human behavior and sociality through online media technologies."[71] A primary source of concern is that dataism requires trust in powerful corporate, civil society, and government organizations—the entities responsible for large-scale collection of data. Yet, automated datafication ignores the will of the individual and/or may go far beyond the bounds of their affirmative choices. Datafication is surveillance.[72]

The conditions of audibility, then, would consider whether individual and community choice about participation is being respected. Participatory equality, within this framing, requires that the humanity of the individual be recognized, which can empower the individual to make personal choices.[73] Without this condition of audibility, individuals' sonic information may be left to the whims and interests of powerful corporate, civil society, and governmental

---

[69] *Id.* at 38.

[70] VIKTOR MAYER-SCHÖNBERGER & KENNETH CUKIER, BIG DATA: A REVOLUTION THAT WILL TRANSFORM HOW WE LIVE, WORK, AND THINK 78 (2013).

[71] Jose van Dijck, *Datafication, Dataism and Dataveillance: Big Data Between Scientific Paradigm and Ideology*, 12 SURVEILLANCE & SOC'Y 197, 198 (2014).

[72] *See, e.g.*, Ulises A. Mejias & Nick Couldry, *Datafication*, 8 INTERNET POL'Y REV. 1, 6-7 (2019); *see also* Julie E. Cohen, *What Privacy is For*, 126 HARV. L. REV. 1904, 1915 (2013) ("Networked information technologies enable surveillant attention to become continuous, pervasively distributed, and persistent.").

[73] *Cf.* Andrea Brighenti, *Visibility: A Category for the Social Sciences*, 55 CURRENT SOCIO. 323, (2007) (arguing that social *visibility* can be empowering); Brantner & Stehle, *supra* note 66, at 94 (same).

organizations. But recognition of humanity, and ultimately individual autonomy, does not mean continued reliance on current consent and notice-and-choice frameworks. These frameworks have proven unsuccessful at protecting rights and informing users about the collection, use, and sharing of data.[74] A recognition of humanity would mean the acknowledgement data is networked—the data collected implicates not one individual but many.[75] The networked nature of data requires, then, the reconceptualization of consent mechanisms to recognize that focus on individual consent is insufficient for protecting autonomy.

A concern for protecting autonomy also demonstrates the need for transparency regarding the processes of powerful actors. This second condition focuses on the ability to critically assess the data collection and use practices of governments, civil society organizations, and corporations. Transparency and its fraternal twin explainability are popular requirements for policies targeting AI and machine learning systems. Some critics argue that although transparency-increasing regulations have an admirable goal, they are a poor fit for complex algorithmic processes.[76] This means that even if information about these processes is made available, the average person may not be able to understand their meaning or functions. Instead, commenters have called for making the usual black box algorithmic and artificial intelligence information available to oversight organizations including advocacy organizations, universities, and government agencies.[77]

---

[74] *See, e.g.*, Neil Richards & Woodrow Hartzog, *The Pathologies of Digital Consent*, 96 WASH. U. L. REV. 1461, 1478-91 (2019) (discussing the various defects of consent models); John A Rothchild, *Against Notice and Choice: The Manifest Failure of the Proceduralist Paradigm to Protect Privacy Online (or Anywhere Else)*, 66 CLEV. ST. L. REV. 559, 559, 608-35 (2018) (arguing that the notice-and-choice model is "fundamentally flawed"); Robert H. Sloan & Richard Warner, *Beyond Notice and Choice: Privacy, Norms, and Consent*, 14 J. HIGH TECH. L. 370, 390-407 (2014) (criticizing the notice-and-choice model as insufficiently informative and only capable of producing "passive acquiescence").

[75] Data & Society Research Institute, *Databite No. 127: Jasmine McNealy*, YOUTUBE (Jan. 8, 2020), https://youtu.be/jB5_NrdWH7k.

[76] Yavar Bathaee, *The Artificial Intelligence Black Box and the Failure of Intent and Causation*, 31 HARV. J.L. & TECH. 889, 928-31 (2018).

[77] *See, e.g.*, FRANK PASQUALE, THE BLACK BOX SOCIETY 57-58, 147, 157 (2015).

Even with the understanding of data collection and use that could be provided through transparency and explainability, sound creators—people—still need to have autonomy to prevent surveillance and control by external powers. Autonomy is the "chance to experiment with new behaviors without fear of social consequences."[78] In other words, autonomy involves control and can be conceptualized as the individual being able to decide the kinds of behaviors in which they are willing to engage. Autonomy from coercion from external powers would mean freedom from nudges from targeted advertisement based on predictions about your purchasing behavior made from, for example, analysis of your voice data. Voice and other sound data make up part of what Park calls the "public spheres of ubiquitous surveillance."[79] In these surveillance spheres, algorithmic systems "gobble[] up personal data and surveille[] us 'automatically,'"[80] creating a process called *normalization* in which artificial intelligence-based systems, in connection with social institutions, become structures of governance over individuals, changing how they behave and interact with their environments.[81] As noted above, human behavior changes when we perceive that we are being watched whether by corporate, government, or social actors.[82] A similar process has been called *mutual domestication*, as users of AI technology incorporate algorithmic guidance into their daily lives and are, in turn, "colonize[d] . . . into ideal consumers . . . ."[83] This normalization or domestication affects how and whether we behave in certain ways, in particular locations, to avoid specific real or potential consequences. This institutional data collection and analysis thereby chips away at our individual ability to be free from unwanted external influences.

---

[78] Kimberly M. Christopherson, *The Positive and Negative Implications of Anonymity in Internet Social Interactions: "On the Internet, Nobody Knows You're a Dog"*, 23 COMPUT. HUM. BEHAV. 3038, 3041 (2007).

[79] *See* Park, *supra* note 19, at 341.

[80] *Id.* at 342.

[81] *Id.*

[82] *See supra* note 20 and accompanying text.

[83] Ignacio Siles et al., *The Mutual Domestication of Users and Algorithmic Recommendations on Netflix*, 12 COMMC'N CULTURE & CRITIQUE 499, 500, 516 (2019).

In prior research, I identify these surveillance institutions and their logics related to personal data collection and use as comprising an exo-system in the ecology of data governance.[84] This exo-system of data governance includes both formal and informal structures of policy enforcement and creates the environments that shape how we, as data subjects, interact with the technologies deployed in those environments.[85] The data hoarded by these organizations and then used to train algorithmic systems provide the power to shape lives and institutions, removing the ability of individuals, in the case of sonic data, to be free from constant listening.[86] Algorithms and associated surveillance technology are part of technological assemblages[87] that construct power through data collection, modeling, and usages.[88]

V. A Framework for Sonic Privacy

Sound law and the critical factors of public sphere audibility provide lessons for reshaping the power dynamics impacting sonic privacy. These can be summarized as follows:

There is a clear distinction between active information collection and passive encounters.

---

[84] *See* McNealy, *supra* note 21; *see also* McNealy, *supra* note 75.

[85] *See* McNealy, *supra* note 21.

[86] *See* Meredith Whittaker, *The Steep Cost of Capture*, ACM INTERACTIONS, Nov.-Dec. 2021, at 51, 53-54 (discussing the perils implications of surveillance for academic freedom and knowledge production).

[87] Siles et al., *supra* note 83, at 500; Ignacio Siles et al., *Folk Theories of Algorithmic Recommendations on Spotify: Enacting Data Assemblages in the Global South*, BIG DATA & SOC'Y, Jan.-June 2020, at 1, 2-3; Nick Seaver, *Algorithms as Culture: Some Tactics for the Ethnography of Algorithmic Systems*, BIG DATA & SOC'Y, July-Dec. 2017, at 1, 4-5 (describing algorithms as "broad patterns of meaning and practice that can be engaged with empirically").

[88] *See generally* SAFIYA UMOJA NOBLE, ALGORITHMS OF OPPRESSION: HOW SEARCH ENGINES REINFORCE RACISM (2018); CATHY O'NEIL, WEAPONS OF MATH DESTRUCTION: HOW BIG DATA INCREASES INEQUALITY AND THREATENS DEMOCRACY (2016); VIRGINIA EUBANKS, AUTOMATING INEQUALITY: HOW HIGH-TECH TOOLS PROFILE, POLICE, AND PUNISH THE POOR (2018).

The publicness of information—including the public interest and impact—influences whether data will be considered protected by judicial recognition of a reasonable expectation of privacy.

Advances in technology heighten the implications of data collection and shift the balance away from allowing unfettered collection of data, especially that which is available from public sources, and toward protecting data and the data subject.

Both the kinds of technology and how data was used in the representative sound law cases are distinguishable from current data collection systems and uses in terms of volume and the impacts of the inferences that can be made. The purposes for which data are collected are different, the impacts significant.

A. Hearing versus Listening: A Return to Audibility

I propose a framework for understanding data collection harms in a dichotomy I call *hearing versus listening*. Though often used interchangeably, a clear difference exists between hearing and listening. Hearing is the recognition of sound, involving an input of sound from a source, and an understanding of it. Listening, in contrast, is more than simple recognition of sound. Instead, it is the intensive processing of sound. Where hearing is passive, listening is an active process. Hearing, then, can be analogized to passively encountering data. In contrast, listening is the active collection and processing of data for a purpose, like in cases of surreptitious recording.

This framework incorporates four important factors:

First, *organizations are engaging in active sonic data collection*; passivity is not a norm under the current regime of surveillance and data capitalism.[89] Organizations do not passively encounter data; instead they deploy machine tools into the environment looking for ways to collect and use data even if they have no logic for how that data will be used. After all, data is valuable and can be accumulated simply for future use. Failing that,

[89] Sarah Myers West, *Data Capitalism: Redefining the Logics of Surveillance and Privacy*, 58 BUS. & SOC'Y 20, 21 (2019) (defining data capitalism as the system that adheres value to personal data, for use by those who have the power to access and interpret the information).

access can be sold to third parties. Because data is valuable, it is profitable to store data to sell access to third-party users—organizations that may lack the technological capability to collect the vast amounts of data, but are willing to pay for access to what I have called data hoarders.[90]

Second, *the focus on "publicness" of sonic data is inconsistent with protecting data subjects and harm prevention*. From the sound law cases, *publicness*, in both the consideration of the locale (public versus private) and interest or value of the data, was a factor that limited liability or provided a privilege against the prohibition on collecting and using the data. A continuing focus on the public versus private dichotomy ignores the many ways in which data can be used and the inferences that might be made from these uses. Just because data is available in the public does not mean that an individual loses any expectation over how or whether it will be collected and used. Furthermore, data can be used in ways that have long-term negative impacts on individuals and communities. Zip code data, for example, has been used to predict an individual's potential to pay back a loan, often to the detriment of those in lower income areas.[91] The focus on the public interest or value of data, too, must be reassessed to allow for the public to use parts of data for evidence-based governance and research, while protecting individuals and communities from the harms associated with data use. This should involve consultation with those communities that would be the most impacted by data collection and use.

Third, *the technologies used to collect sonic data endow sound and other data encounters with permanence.* Unlike hearing with the human ear, the use of technology, including algorithmic and machine learning systems, allows easy storage of and access to voluminous amounts of data. This active, in-depth processing by organizations changes the nature of sonic data from ephemeral—a brief encounter with sound—to a perpetual part of a dataset available for multiple uses.

Fourth, *these encounters also reflect organizational logics of profit-making and efficiency that often conflict with individual and*

---

[90] Jasmine E. McNealy, *Hoarder, Handler, Bricoleur, Spy: An Explication of Information Distribution Organisations*, 8 J. INT'L. COMPAR. L. 385, 396-98 (2021).

[91] O'NEIL, *supra* note 88, at 200.

community desires for obscurity and autonomy. Organizations—corporate, governmental, and civil society—are listeners, looking to process and store data for specific organizational purposes. Listening, then, reflects active engagement, seeking, and processing of information. In contrast, most individuals and communities would rather remain practically obscure[92] and not be implicated within the schemes for value—monetary or otherwise—defined by outsider organizations.

B. Audibility and Policy

The four frame factors demonstrate the need for governance and policy that reflect the heightened harms that might result from the continued collection and use of sound and other data. Audibility, the choice of whether to be heard, and disposition of the kinds of sonic products placed in the public sphere, requires protection from traditional conceptions of what is public versus private. Technological innovations have lowered the threshold for access to data that would at one time have been considered private, even in public spaces. The ability to listen, beyond the scope of the natural ear, and then to process and store data require a change in the definition of a reasonable expectation of privacy. A different approach would "would leave [us] at the mercy of advancing technology"[93] able to listen, store, and use our sound data.

To ensure that these critical factors properly inform governance, policy created using this framework must consider audibility from both individual and community perspectives. Any policy created must consider the question not only of whether a person has chosen to be recorded—to have their sonic data captured—but also whether the network of people implicated in the data are, too, able to assert their autonomy. The policy would need to critically assess and expose organizational data practices. Ideally, these would be evaluated by some authority with input from community or advocacy organizations. Finally, we must be free to be able to expect a life where data collection—surveillance—is

---

[92] *See generally* Woodrow Hartzog & Frederic Stutzman, *The Case for Online Obscurity*, 101 CALIF. L. REV. 1 (2013) (discussing practical obscurity in a technological context).

[93] Kyllo v. United States, 533 U.S. 27, 35 (2001) (ruling that the use by police of a then-novel thermal imager constituted a search under the 4th Amendment).

minimal. Is this utopian? Probably. But normalization of surveillance chills participation. Audibility, in contrast, requires that an individual be allowed autonomy over the decision to (not) participate.

I am not, however, advocating for an individual choice model in the form of a consent waiver or opt-out provisions. Other scholars have already discussed the failures of the current notice-and-choice or consent designs including the control offered to users being illusory, and that consent can be coerced.[94] Instead, lawmakers should focus on specifying permissible kinds of data-collection practices, and clarifying that collection for some purposes does not license collection for other purposes. An example of this kind of policy was proposed by U.S. Senator Sherrod Brown in the Data Accountability and Transparency Act of 2020.[95] The draft bill sharply departed from other attempts at a federal privacy law in that it outright rejected notice and choice, making no mention of opt-out or opt-in to predetermined terms and conditions.[96] Instead, the draft would have banned the collection of personal data unless allowed by law, prohibited retention of personal data for any time longer than is strictly necessary to carry out a permissible purpose, prohibited the use of personal data for discrimination, and required that organizations deploying algorithms audit these systems and provide accountability reports. It also would have created a new federal agency with rulemaking and enforcement authority. Of course, the

---

[94] *See, e.g.*, Richards and Hartzog, *supra* note 74, at 1486-90 (discussing coerced consent in the online privacy regulation space); Woodrow Hartzog, *Website Design as Contract*, 60 AM. UNIV. L. REV. 1635, 1664-68 (2011) (discussing website design choices that coercively violate user privacy); Woodrow Hartzog, *The Case Against Idealising Control*, 4 EUR. DATA PROT. L. REV. 423, 426-27 (2018) (discussing the illusion of online control).

[95] SHERROD BROWN, 116TH CONG. DISCUSSION DRAFT OF DATA ACCOUNTABILITY AND TRANSPARENCY ACT (2020) https://www.banking.senate.gov/imo/media/doc/Brown%20-%20DATA%202020%20Discussion%20Draft.pdf.

[96] *Senator Brown Unveils Data Accountability and Transparency Act*, EPIC.ORG (June 18, 2020), https://epic.org/senator-brown-unveils-data-accountability-and-transparency-act/; Geoffrey Fowler, *Nobody reads privacy policies. This senator wants lawmakers to stop pretending we do.*, WASH. POST (June 18, 2020), https://www.washingtonpost.com/technology/2020/06/18/data-privacy-law-sherrod-brown/.

draft was not limited to sonic data. But it did embody the necessary factors for ensuring audibility in the public sphere.

Conclusion: The Future of Sonic Data

A repeated worry of users of both hardware and software focuses on whether technology is "listening to them."[97] Anecdotes about users speaking with a friend about something, then logging into a site or beginning to use their devices, only to find advertisements for that thing, have peppered news networks. And while many scholars and journalists have denied that apps and (some) devices are constantly listening, the uneasiness remains, and stories persist.[98] At the heart of these worries is legitimate concern about constant surveillance and surreptitious data collection.[99]

Some might argue that by having devices like voice assistants in the home, an individual assumes the risk of data collection, especially when that data collection is detailed in a privacy policy. Further, voice assistant technology has been touted as expanding accessibility and convenience to individuals with certain disabilities.[100] But devices have been found to be listening beyond

---

[97] Bree Fowler, *Is Your Smartphone Secretly Listening to You?*, CONSUMER REPS. (July 10, 2019), https://www.consumerreports.org/smartphones/is-your-smartphone-secretly-listening-to-you; Rani Molla, *Your smart devices are listening to you, explained*, VOX (Sept. 20, 2019), https://www.vox.com/recode/2019/9/20/20875755/smart-devices-listening-human-reviewers-portal-alexa-siri-assistant.

[98] *E.g.*, Joe Tidy, *Why phones that secretly listen to us are a myth*, BBC NEWS (Sept. 5, 2019), https://www.bbc.com/news/technology-49585682; Molla, *supra* note 97.

[99] *See, e.g.*, Alex Hern, *Apple contractors "regularly hear confidential details" on Siri recordings*, THE GUARDIAN (July 26, 2019), http://www.theguardian.com/technology/2019/jul/26/apple-contractors-regularly-hear-confidential-details-on-siri-recordings; Sarah E. Needleman & Parmy Olson, *Google Contractors Listen to Recordings of People Using Virtual Assistant*, WALL ST. J. (July 11, 2019), https://www.wsj.com/articles/google-contractors-listen-to-recordings-of-consumers-addressing-virtual-assistant-11562865883.

[100] *See, e.g.*, Saminda Sundeepa Balasuriya, *Use of Voice Activated Interfaces by People with Intellectual Disability*, 30 PROC. AUSTRALIAN CONF. ON COMPUT.-HUM. INTERACTION 102, 103-04 (2018); Alessandro Vieira et al., The Impact of Voice Assistant Home Devices on People with Disabilities: A Longitudinal Study 4 (Dec. 21, 2021) (unpublished manuscript) (https://papers.ssrn.com/abstract=3993227).

the scope to which individuals have consented. This thinking falls back, again, on the idea of control as the foundation for privacy, in conflict with how people live and the privacy expectations they form in specific contexts. Of course, the problems with sonic privacy are not limited to devices recognizably collecting data within the home or on personal devices. In 2022, researchers reported that sonic data might be recovered from "lightweight reflective objects" that are common to the home workspaces many have occupied since the COVID-19 pandemic began in 2020.[101] Unfortunately, current understandings of privacy may mean that we, as sound creators, have little recourse when organizations use technological advances to collect and interpret sound data.

In his 1993 doctoral dissertation, the late Michael Hawley asserted that computers had "no sense of sound."[102] At that time, according to Hawley, computers were woefully behind the natural world, which used sound as the predominant mode of communication. Computer-made sounds were limited to "blips and beeps," unable to mimic the "evanescen[ce]" of "real world acoustics" and developers had focused instead on spreadsheets, pictures, and text. Computers, also, had no way of dealing with the complexity of sound, according to Hawley, while at the same time needing to be able to understand sound and to "operate all along the continuum between a sound wave and representations of its content."[103] In the early 1990s, however, although sound and human hearing capabilities were the subject of much research, "little of that knowledge ha[d] found its way into day-to-day [computing] systems."[104]

Fast-forward nearly 30 years and computers have developed from machines unable to hear, to sound processing and creation devices. Computers and other machine systems can "deal with" sound very well. What must happen, then, to ensure our privacy and

---

[101] Ben Nassi et al., The Little Seal Bug: Optical Sound Recovery from Lightweight Reflective Objects 2 (Feb. 25, 2022) (unpublished manuscript) (https://eprint.iacr.org/2022/227.pdf).

[102] Michael J. Hawley, Structure out of Sound 15 (Aug. 6, 1993) (Ph.D. dissertation, Massachusetts Institute of Technology) (https://dspace.mit.edu/bitstream/handle/1721.1/29068/29881814-MIT.pdf).

[103] *Id.* at 16.

[104] *Id.* at 17.

autonomy over the decision on whether to participate? Care must be taken to ensure the creation of policy that adequately protects our ability to live as intentional and unintentional sound creators. Such a policy must embody an understanding of how we might, and might not, want the sounds we produce to be used. This requires a recognition, like in *Sanders* and *Shulman*, that even if a sound can be heard, there remains an expectation that there will be no (machine) listening.[105]

[105] *Supra* notes 39-50 and accompanying text.