

Espionage and Dataveillance Technologies: Perspectives on Sound Surveillance in Surveillance Art Practices

Lorena Ferreira Alves*

CITAR - Research Center for Science and Technology of the Arts
Porto, Portugal
lfalves@ucp.pt

Abstract

This article explores the relationship between art and surveillance technologies, with a particular focus on the sonic dimension of surveillance and its intrinsic connection to espionage. Beginning with an introduction to Foucault's conception of surveillance as a mechanism of control over bodies and behaviors, the paper argues that, in contemporary society, this practice has become increasingly sophisticated through the voluntary collection of digital data and what Rouvroy and Berns term "algorithmic governmentality." The second section discusses the development of surveillance technologies and their social impacts, illustrated by examples from surveillance art, including works by Bruce Nauman, Jill Magid, and Marie Sester. The third section addresses sound surveillance as a less explored domain compared to visual surveillance, analyzing it both theoretically and through artistic practices. Here, the studies of Dimitrios Pavlounis and Audrey Amsellem are highlighted, alongside artworks situated within the concept of surveillance art, such as Roslyn Orlando's and Kyle McDonald and Brian House's artworks, which critically examine the vulnerability of sonic privacy perpetuated by major technology and communication companies. The article contends that sound surveillance remains strongly associated with espionage and illegality, in contrast to the normalization of visual surveillance propagated by CCTV systems. Finally, the paper cautions that the increasing integration of AI and automation into everyday life entails the acceptance of more invasive forms of surveillance and bodily control.

CCS Concepts

• ; • **Applied computing** → Arts and humanities; Media arts; Computer forensics; Surveillance mechanisms; Arts and humanities; Sound and music computing;

Keywords

Surveillance Art, Sound Surveillance, Artificial Intelligence, Espionage

*Integrated PhD Researcher at CITAR, working in the fields of sound art, sound surveillance, and art and surveillance. PhD in Arts from the University of Brasília and in History and Arts from the University of Granada.



This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License.

ARTECH 2025, Braga, Portugal

© 2025 Copyright held by the owner/author(s).

ACM ISBN 979-8-4007-2001-7/2025/11

<https://doi.org/10.1145/3773699.3774365>

ACM Reference Format:

Lorena Ferreira Alves. 2025. Espionage and Dataveillance Technologies: Perspectives on Sound Surveillance in Surveillance Art Practices. In *12th International Conference on Digital and Interactive Arts: Media Art Cultures, Communities & Territories (ARTECH 2025)*, November 26–28, 2025, Braga, Portugal. ACM, New York, NY, USA, 6 pages. <https://doi.org/10.1145/3773699.3774365>

1 Introduction

This article presents a study on the art and surveillance technologies, aiming to advance a perspective on the role of sound within this scope to argue that sound surveillance is intrinsically linked to the act of espionage. For this understanding, it is first essential to define the idea of surveillance before proceeding to discuss how contributions in the fields of art and surveillance address surveillance technologies, as well as their sound dimensions. The understanding of surveillance here refers to the act of obtaining information about an individual or group of individuals, whether voluntarily, coercively, or through espionage, in order to gain some form of advantage over them. This understanding of surveillance is primarily based on Foucault's *The History of Sexuality, Volume 1* [1], in which he explains how the act of confession imposed by the Christian Church since the Middle Ages functioned as a method of surveillance for the control of bodies, including the regulation of birth control. The act of confession, mandated as an obligatory practice for the Christian subject, functioned as a means of extracting intimate personal information, thereby enabling the exercise of power and control over the confessing body. It is possible to observe that this confessional methodology, once managed by the Church, has not been extinguished but rather transformed. Today, we are persuaded to voluntarily offer our personal information on websites and apps in exchange for connectivity, social interaction, or approval from others. This situates us within a technologically more sophisticated form of surveillance, as discussed in the theories of algorithmic governmentality by Antoinette Rouvroy and Thomas Berns [2]. Contemporary data surveillance via the internet is capable of knowing us to such an extent that those who control our data gain a significant advantage in influencing our behaviors and thoughts.

The approach used to argue that sound surveillance inherently embraces qualities related to espionage will be developed through bibliographic examples that discuss the contexts in which sonic surveillance technologies have been applied, drawing on the surveys by Steve Wright [3] and Audrey Amsellem [4]. Additionally, the dissemination of the collective imaginary about sound surveillance technologies through media will be examined based on the studies of Dimitrios Pavlounis [5]. Finally, artistic examples addressing sound within the realms of surveillance art will be analyzed

through the works of Roslyn Orlando and Kyle McDonald and Brian House.

These sources were selected for being consistent studies that specifically address sound surveillance within the humanities, a topic that remains less explored compared to surveillance studies focusing on the visual field, a premise that will be further discussed throughout this article. The same applies to artworks that engage with sound in the context of surveillance art, where only a limited number of examples currently exist. Both the bibliographic and artistic references on sound surveillance complement each other, allowing for a discussion of sound surveillance aspects related to espionage practices involving both institutional and technocorporate power.

2 Surveillance Art as Technological

When positioned within the field of surveillance studies, artistic practice is, or may come to be, classified under terms such as art and surveillance, artveillance, or surveillance art. These designations all refer to the same phenomenon: artistic practices that critically engage with the subject of surveillance. The investigation into the relationship between contemporary surveillance art has been approached from the perspectives of visual arts, performance, new media, photography, cinema, surveillance aesthetics, and art activism. These approaches are reflected in key references such as the exhibition catalogue CTRL [SPACE]: Rhetorics of Surveillance from Bentham to Big Brother published in 2002, as well as in the ongoing discussions and contributions published in the journal *Surveillance & Society*.

As Andrea Brighenti [6] has stated, surveillance not only generates substantial social control or social triage, but also produces a collective imaginary of what constitutes security, insecurity, and control, as well as the landscape of moods and affects expressed by a surveillance society. According to Brighenti, surveillance art is a domain that considers art as technological, that is, it is always connected to a technology of production as well as a technology of mediation and remediation. This reflection can be followed through the extensive Michel Foucault's study *Discipline and Punish* [7], which analyzes the apparatus of surveillance, an activity comprising methods, procedures, and techniques carried out by humans supported by a panoptic architecture. Foucault offers a profound perspective on how surveillance can be understood as a strategy to maintain control over bodies, rendering them docile and disciplined. While Foucault did not explicitly address surveillance technologies such as cameras or electronic devices equipped with wiring and electronic components, the theoretical framework he developed around the panopticon has been widely applied in contemporary analyses of electronic surveillance. For example, Zygmunt Bauman's [8], concept of post-panoptic surveillance, characterized by invisible data monitoring in the context of the Internet era, demonstrates the continued efficacy of surveillance mechanisms in exercising control over bodies.

From the development of surveillance technologies, we can observe Brighenti's [6] assertion that surveillance art engages in discussions about how surveillance expresses a surveillance society according to its temporal and technological context. The term

“surveillance society,” coined by Gary T. Marx [9] in the 1980s, visualizes the full behavioral control of citizens through computer-based surveillance technologies employed by the state, raising critical concerns about the misapplication and abuse of power. It is important to highlight that, at the time Marx developed this concept, CCTV (closed-circuit television) surveillance technologies were becoming increasingly popular in both public and private spaces. This device subsequently became a technological symbol of surveillance within the field of art and surveillance.

The following section presents key examples of surveillance artworks exhibited in internationally recognized galleries. As Brighenti suggests, art and surveillance practices reflect the conditions of the surveillance society and the technological developments of a specific time and place. Since the 1970s, cameras have been integral to the field of surveillance art. In subsequent decades, artistic practices have progressively incorporated emerging surveillance technologies, demonstrating an evolution from optical observation toward more complex forms of data-driven monitoring that encompass Big Data analytics, algorithmic computation, and artificial intelligence.

In the field of surveillance art, numerous artworks employ surveillance cameras, such as the seminal piece in surveillance art *Live- Taped Video Corridor* (1969–70) by Bruce Nauman. According to Dörte Zbikowski [10], Nauman was one of the first artists to explore the use of surveillance cameras. This installation explores the technical potential of the surveillance camera through a spatial, emotional, and interactive setup, creating a tension between physical presence and real space, and the image of the real space surveilled and manipulated by the camera. Other examples of artworks that engage with surveillance through the scope of CCTV include works by the artist Jill Magid, such as *System Azure Security Ornamentation* (2002) [11], in which the artist subverts the security function typically attributed to the surveillance camera by assigning to this device a personal, intimate, and comic perspective, where the ornamentation of CCTV serves as a means to foster a connection between the surveilled person and the device that watches them. Perhaps one of the most renowned and recent examples incorporating CCTV within the field of art are the works of Banksy (Figures 1 and 2). In these pieces, Banksy employs cameras installed on walls to disrupt the banal perception of this device within the urban landscape, transforming it into a critical focal point that both recalls and reconfigures its presence and function as a mechanism for surveilling public spaces.

Beyond surveillance cameras, we find examples of surveillance art that relate to technologies that are more intrusive, such as genetic surveillance, as critically addressed by Heather Dewey-Hagborg in her work *Stranger Visions* (2013) [12]. The piece draws attention to the extent to which DNA samples can be used to infer a person's appearance, while also warning of the potential errors involved in treating such data as a reliable basis for developing facial prediction technologies in forensic research, where stereotypical projections could lead to forms of genetic determinism. The issue of stereotypical predictions generated by algorithms based on datasets captured through surveillance technologies (dataveillance on the Internet) is also explored by Trevor Paglen and Kate Crawford in their exhibition *Training Humans* (2019) [13]. In this exhibition, they reflect on and raise critical concerns about how AI and machine



Figure 1: Banksy, untitled. <https://www.banksy.co.uk/>

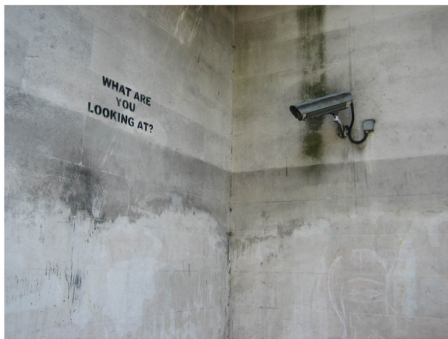


Figure 2: Banksy, untitled. <https://www.banksy.co.uk/>

learning technologies are trained to read the world, producing problematic interpretations and classifications of human beings. The artistic installation reveals how a massive quantity of images (datasets), collected from online sources, including social media platforms, serves as the basis for generating patterns of meaning, leading not only to misclassification but also to distorted forms of judgment, such as racism, misogyny, ableism, and sexism. It opens up a critical discussion about how such technologies can impact our daily lives.

The technologies of surveillance or *tracking technologies* as described by Levin, Frohne, Weibel [14], have transitioned from a military context to the domestic sphere. Foucault's panoptic surveillance paradigm has evolved into what Paula Sibilia [15] terms data-surveillance, a form of digital monitoring characterized by the invisible surveillance of data circulating through the global internet network. Today the enhancement of AI technologies for automation and profitability, or simply convenience, speed, and efficiency, the use of tools and services that rely on data surveillance has become indispensable. Such reliance is now a prerequisite for performing everyday tasks and communicating at a pace dictated by the compulsive scale of contemporary production and consumption. Within a contemporary discussion on how surveillance is intricately tied to the current capitalist mode of life, Shoshana Zuboff [16] reflects that user behavioral data from internet navigation has become an indispensable resource for companies to generate profit. She coined the term surveillance capitalism to assert that, through the constant monitoring of browsing data by companies managing

websites, applications, and online services, this big data possesses immeasurable value, which, through algorithmic interpretation, enables the achievement of diverse financial objectives.

Profit generation is no longer the sole function of big data utilization by companies today. Alarmingly, with ongoing armed conflicts and the persistent advance of neocolonialism, we are witnessing a pronounced resurgence of the military context in the development of contemporary and sophisticated surveillance technologies, increasingly shaped by artificial intelligence. As Krzysztof Sliwinski explains.

“AI is heavily used in systems that integrate target and object recognition and geospatial intelligence. Analysis of satellite images, geolocating and analysing open-source data such as social media photos in geopolitically sensitive locations. On top of that neural networks are used, for example, to combine ground-level photos drone video footage and satellite imagery.” [17]

We are currently witnessing the use of warfare technologies developed with the assistance of AI, such as Lavender and The Gospel, employed by Israel to generate potential targets on an unprecedented scale. This raises a series of moral and legal concerns regarding the deployment of such technology in alignment with military operations. At the time of writing this article, no scientific bibliographic sources analyzing or specifically addressing the technologies The Gospel and Lavender have been identified. However, journalistic reports provide research into how these surveillance technologies operate and are being deployed. The report produced by Al Jazeera Media Network (2023) [18] describes that The Gospel identifies targets through multiple operational layers, which are briefly outlined as follows: The Alchemist, which collects information from a database of surveillance devices in both physical and digital spaces; Fire Factory, which analyzes the collected data; and The Gospel itself, which generates potential targets perceived as threats to the State of Israel. According to the same report, the targets generated by the AI are subsequently reviewed by human operators, who decide whether to authorize airstrikes on locations that include not only military infrastructure but also civilian buildings and public service facilities such as schools and hospitals. This process results in a high scale of collateral damage of the deaths of civilians.

The interactive installation Threatbox.us (2005–2007) [19] by Marie Sester is a notable reference in the area of surveillance art, addressing surveillance technologies that are present in both contexts of warfare and mass entertainment. The installation consists of a web-based surveillance interface, in which a robotic video projector and a computer vision tracking system identify a target and 'attack' it using a spotlight and a loud, startling noise. The spotlight follows the target if it attempts to escape. A montage of violent film excerpts, individuals using social media, and computer games unfolds in fluid patterns across the walls, ceiling, and floor, accompanied by immersive and aggressive audio. After a few seconds, the projector returns to the wall, resumes playing the videos, and becomes ready to detect the next person. Surveillance cameras

embedded in the installation stream the scene live to the web, displaying the space, its audience, and the attacks. Online users act as voyeurs, with no possibility of interaction or intervention.

Marie Sester's artwork raises important questions about the current facets of surveillance technologies, where the same medium, the web, serves simultaneously as a space for content creation, mediation, and surveillance. It also offers a critique of how social media exposes and disseminates information. As online users, or voyeurs, watch scenes that are both tragic and entertaining, the stark contrast between these types of content, rapidly scrolling through news feeds, causes emotions such as sadness, anger, joy, or amusement to become diluted in the short span of time during which content is consumed.

Beyond the visual-centric perspective of surveillance art, where image capture, reproduction, creation, and analysis are foregrounded, it is also possible to identify artistic practices that engage with surveillance technologies through sound. The following subchapter presents an overview of how sound surveillance technologies are currently being employed, as well as a discussion on how sound is explored by artists and artworks that critically address issues related to surveillance technologies.

3 Sound Surveillance and espionage

In the study of surveillance art, it becomes evident that closed-circuit television (CCTV) cameras have been extensively explored as a device for representing and critically examining the implications of surveillance technologies on human behavior and ways of living. Much of this is due to the increased use of surveillance cameras in urban contexts. As Julie K. Petersen [20] notes, since the 1980s, the growing presence of CCTV devices has spread across public spaces such as squares, subway stations, and parking lots, as well as private spaces including banks, commercial establishments, buildings, and residential complexes. This device became an element that integrated and still integrates the urban landscape today.

In contrast, sound surveillance technologies, also referred to as audio surveillance or sonic surveillance, have followed a different trajectory. According to Dimitrios Pavlounis [21], such technologies have existed since the 1910s, beginning with recording systems that employed dictaphones and magnetic tapes. The use of wiretapping technologies or microphones installed in private and public spaces has traditionally been associated with espionage, particularly by professionals such as detectives and security authorities who possess the technical expertise to operate such devices. These individuals are also trained to manipulate recorded audio by removing noise in order to better isolate and interpret the sounds of the surveilled subject. As a result, unlike video surveillance cameras, sound surveillance devices have not been widely popularized, since their use has remained largely confined to covert operations and cases of espionage carried out by specialized individuals or groups.

From this perspective, Petersen [20] explains that the technique known as "listening" is primarily associated with sound surveillance of the human voice. It involves covert, clandestine, and investigative access to conversations that may be intercepted through physical lines, such as telephone wiretaps, or wireless networks, including radio frequencies or microphones placed in specific environments.

As Petersen [20] states, a listening device is any device designed to channel, focus, or amplify sounds to help the listener better recognize the characteristics or content of the sounds.

An example of the high level of sound surveillance capabilities can be observed in the existence of the international espionage network known as ECHELON, which has been employed by government intelligence agencies since the 1940s. Duncan Campbell [22], investigative journalist, made the existence of the ECHELON surveillance network public in 1988. As reported by Campbell, ECHELON was:

"Originally established the vast international global eavesdropping network has existed since shortly after the second world war, when the US, Britain, Canada, Australia and New Zealand signed a secret agreement on signals intelligence, or "sigint". It was anticipated, correctly, that electronic monitoring of communications signals would continue." [22]

According to Steve Wright [23], ECHELON operates through a global infrastructure of facilities, including stations recognizable by their huge antennas. These are used by the U.S. National Security Agency (NSA) for the mass surveillance of electronic telecommunications, including telephone, fax, and email, through keyword and contextual filtering. By diverting messages transmitted via satellite, microwave relay links, or fiber-optic cables, this surveillance system is capable of operating at a prodigious rate, processing more than two million intercepts per hour.

The context of espionage and forensic activity related to sound surveillance is examined by Pavlounis [21] through the lens of popular imaginaries shaped by cinema. Films such as *The Conversation* (1974), directed by Francis Ford Coppola, and *The House on 92nd Street* (1945), directed by Henry Hathaway, portray scenarios in which sound surveillance is employed by professional detectives, law enforcement officers, and intelligence agents in cases involving murder investigations and espionage operations. These cinematic narratives often reflect real-world historical events, such as the Watergate scandal of the 1970s, which involved wiretapping under the administration of former U.S. President Richard Nixon. This scandal was dramatized in Alan J. Pakula's *All the President's Men* (1976), highlighting the characteristics contained in the popular imagination about espionage involving police investigation and scandals involving public persons through sound surveillance.

The espionage character of sound surveillance predates even electronic and digital technologies. As introduced by Dörte Zbikowski [24], the act of covertly listening, of lying in wait to hear secret sounds, has long relied on simple tools such as horns, seashells, or even hands cupped behind the ears to enhance auditory perception. This practice eventually evolved with the use of microphones, or what Zbikowski refers to as "bugs," a term that emerged in the 19th century to describe devices used for eavesdropping and information transmission. In this context, the term "bug" metaphorically conveys the invasive, unwelcome presence of an insect or fly that feeds off its host, being these bugs, sound surveillance technologies, increasingly smaller and portable. Borrowing from Zbikowski's interpretation, we may argue that today's 'bugs' are our smartphones: portable surveillance technologies whose presence is no longer unexpected. Instead, the rhythm of contemporary life embeds these

devices into our daily existence, making constant surveillance a normalized and mobile condition.

Artworks within the field of surveillance art that engage with sound surveillance enabled by smartphones and portable computers serve to raise awareness, denounce, and critically examine how such surveillance practices challenge notions of privacy or the lack thereof and reveal the power structures behind these technologies. One such example is *Evasion Score* (2021) [25], a project by artist Roslyn Orlando in which she develops an instructional score designed to help individuals evade the sound detection of words and phrases by their smartphones. The score, accompanied by a demonstrative video, teaches vocal modulation techniques that mask spoken language, thereby preventing detection by sound surveillance systems operated by corporations and tech companies, what the artist refers to as systems of power.

Another example is the artistic intervention *Conversnitch* (2013) by Kyle McDonald and Brian House [26], who developed a listening device disguised as a light bulb or lamp, which they installed in public places with Wi-Fi access, such as restaurants, libraries, and banks in New York City, Manhattan, and Washington, D.C. Fragments of conversations captured by the microphones embedded in these devices were recorded, transcribed, and posted to the social media platform Twitter (at present X). The transcription process was carried out using Amazon Mechanical Turk, a paid crowdsourcing service. Among the critical issues raised by this intervention, the artists highlight the ease with which illegal surveillance can be conducted with the aid of outsourced crowdsourcing services, as well as the concern over the loss of control individuals have over their own privacy. The work also requires reflection on potential illegal ways of using commercial products and services found online, particularly in relation to unauthorized audio surveillance.

The artistic works exemplified reveal the real potential for sound surveillance that can be managed by technology companies, highlighting how vulnerable we can be to this type of surveillance when using smartphones or gadgets. Practices of sound espionage through technology, as well as Internet of Things (IoT) devices like Amazon's Alexa or even the use of Facebook, have been increasingly discussed by researchers. Audrey Amsellem's recent study explores how this sound espionage is conducted via the Alexa virtual assistant and reflects on the experiences of users who notice signs that they are being spied on. Amsellem [4] clarifies that Amazon, the company behind Alexa, has been employing human workers to listen to fragments of voice commands from Alexa users in order to improve the machine's ability to better understand voice commands.

Although studies like Amsellem's confirm that Alexa users' voices are being monitored, these devices continue to be sold, with concerns about the potential for sound surveillance and privacy loss only arising when Alexa users encounter issues such as "bugs" in the device. These bugs include situations like receiving advertisements for products after talking aloud about needing the same product near the device or, for example, when Alexa unexpectedly starts laughing with a voice different from its own. When users lose control over the device, Amsellem [4] reflects that the fear of using this device, which users themselves have chosen to place inside their homes, creates a sense of anxiety and an uncanny encounter.

This leads users to question: Is this device constantly spying on me? Unplugging the device may result from this anxiety.

However, despite evidence confirming the presence of sound surveillance in the devices we constantly carry with us, we continue to use them. The question that remains is whether the privacy concerning sound data, especially our voice, will lose its relevance as sound surveillance becomes increasingly normalized in the name of AI development.

4 Final considerations

We can observe in the discussions presented in this article that the field of surveillance art refers closely to a form of technological art, as discussed by Andrea Brighenti. The artworks cited here are developed through the use of, or reference to, technological surveillance devices. These works provoke reflection on the relationship between the subject and the surveillance apparatus, the behavioral changes these technologies induce, and the power relations between the watcher or listener, who holds access to information, and the watched or heard body. They also address the ongoing enhancement of increasingly invasive surveillance technologies, which are central themes explored by the artists.

Within the specific domain of sound surveillance, a close connection to espionage practices emerges. Historically, audio surveillance has been employed in closed contexts such as criminal investigations, high-technology surveillance operated by specialized labor, and illegal monitoring. This dimension is evident in artistic practices that focus on acoustic surveillance as their primary conceptual axis. In these artworks, "bugs", microphones embedded in devices, as explained by Dörte Zbikowski, are emphasized as receptive apparatuses that eavesdrop on conversations in order to extract personal information, which can later serve to benefit individuals, institutions, or corporations. While image-based surveillance may also operate in espionage contexts, it has been normalized to the realm of banality, specifically due to the common practice of sharing personal images on social media platforms. In contrast, the perception of being acoustically surveilled still evokes associations with a nature of espionage, illegality, and monitoring of intimate information.

We are increasingly asked to accept AI as the defining technology of the future and adapt to a lifestyle where automated systems will be widely integrated into our daily routines. This tendency is already visible in the widespread use of tools such as ChatGPT, which exemplify the ability of AI systems to produce a broad spectrum of predictive and generative outputs. Accepting such mechanisms of automation implies accepting the mass surveillance currently implemented, as well as its intensification, in order to sustain the functioning of artificial intelligence, machine learning, and deep learning systems. This prompts reflection on the potential future dynamics of control and power shaped by machines operating through data surveillance and what implications these might hold in contexts such as economic and political crises, environmental collapses, or even armed conflict.

Acknowledgments

This work was supported by Fundação para a Ciência e a Tecnologia (FCT), I.P., under the project: CEECINST/00070/2021;

2022205CITAR022. Additionally, I am appreciative of the scholarship that CAPES (Coordination for the Improvement of Higher Education Personnel) has awarded me in order to pursue my doctoral studies.

References

- [1] Michel Foucault. 1978. *The History of Sexuality, Volume I: An Introduction*. Pantheon Books, New York.
- [2] Antoinette Rouvroy and Thomas Berns. 2015. Governamentalidade algorítmica e perspectivas de emancipação: o dispar como condição de individualização pela relação? *Revista Eco-Pós: Tecnopolíticas e Vigilância* 18, 2 (2015), 36–56. <https://doi.org/10.29146/eco-pos.v18i2.2662>
- [3] Steve. Wright. 2005. The ECHELON: An Illegal Vision. *Surveillance & Society*, 3(2/3). <https://doi.org/10.24908/ss.v3i2/3.3501>.
- [4] Audrey Amsellem. 2024. Machine aurality: uncanny resonances and the sonic anxieties of surveillance capitalism, *Sound Studies*, 10:1, 26–40. <https://doi.org/10.1080/20551940.2023.2286769>
- [5] Dimitrios Pavlounis. 2016. *Sound Evidence: An Archaeology of Audio Recording and Surveillance in Popular Film and Media*. PhD dissertation. Screen Arts and Cultures, University of Michigan, Ann Arbor.
- [6] Andrea M. Brighenti. 2010. Artveillance: At the crossroads of art and surveillance. *Surveillance & Society* 7, 2 (2010), 137–148. <https://doi.org/10.24908/ss.v7i2.4142>
- [7] Michel Foucault. 1999. *Vigiar e Punir: nascimento da prisão*. (20a ed.). Vozes, Rio de Janeiro.
- [8] Zygmunt Bauman and David Lyon. 2014. *Vigilância líquida: Diálogos com David Lyon*. Zahar, Rio de Janeiro.
- [9] Gary T. Marx. 1985. The Surveillance Society: The Threat of 1984-Style Techniques. *The Futurist* (July 1985), 21–26. https://web.mit.edu/gtmarx/www/futurist_surv_soc.pdf
- [10] Dörte Zbikowski. 2002. Bruce Nauman. In Levin, Thomas Y; Frohne, Ursula; Weibel, Peter (eds.). *CTRL [SPACE]: Rhetorics of Surveillance from Bentham to Big Brother*. MIT Press, Cambridge, MA.
- [11] Jill Magid. 2002. *System Azure Security Ornamentation*. <https://www.jillmagid.com/projects/system-azure-security-ornamentation>
- [12] Heather Dewey-Hagborg. 2013. *Stranger Visions*. <https://deweyhagborg.com/projects/stranger-visions>
- [13] Trevor Paglen and Kate Crawford. 2019. *Training Humans [Exhibition]*. Fondazione Prada. [https://www.fondazioneprada.org/project/training-humans/?lang=\\$en](https://www.fondazioneprada.org/project/training-humans/?lang=$en)
- [14] Thomas Y Levin, Ursula Frohne, and Peter Weibel (Eds.). *CTRL [SPACE]: Rhetorics of Surveillance from Bentham to Big Brother*. MIT Press, Cambridge, MA.
- [15] Paula Sibilia. 2005. El hombre postorgánico: Cuerpo, subjetividad y tecnologías digitales. *Fondo de Cultura Económica*, Buenos Aires.
- [16] Shoshana Zuboff. 2015. Big other: surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology*, (30). 75 - 89. <https://doi.org/10.1057/jit.2015.5>
- [17] Krzysztof Sliwinski. 2024. Artificial intelligence and international military conflicts – The case of war in Ukraine. *World and New World Journal*. [https://worldnewworld.com/page/content.php?no=\\$3970](https://worldnewworld.com/page/content.php?no=$3970)
- [18] Al Jazeera. 2023. The Gospel: Israel turns to a new AI system in the Gaza war. *The Listening Post*. December 9. <https://www.aljazeera.com/program/the-listening-post/2023/12/9/the-gospel-israel-turns-to-a-new-ai-system-in-the-gaza-war>
- [19] Marie Sester. 2005–2007. *Threatbox.us*. Retrieved June 28, 2025. <https://sester.net/threatbox-us/>
- [20] Julie K. Petersen. 2001. *Understanding Surveillance Technologies: Spy Devices, Their Origins & Applications*. CRC Press.
- [21] Dimitrios Pavlounis. 2016. *Sound Evidence: An Archaeology of Audio Recording and Surveillance in Popular Film and Media*. PhD dissertation. Screen Arts and Cultures, University of Michigan, Ann Arbor.
- [22] Duncan Campbell. 1988. They've got it taped. *New Statesman Society*. Aug. 12. <https://www.duncancampbell.org/menu/journalism/newstatesman/newstatesman-1988/They%20got%20it%20taped.pdf>
- [23] Steve Wright. 2005. The ECHELON: An Illegal Vision. *Surveillance & Society*, 3(2/3). <https://doi.org/10.24908/ss.v3i2/3.3501>
- [24] Dörte Zbikowski. 2002. The Listening Ear: Phenomena of Acoustic Surveillance. In Levin, Thomas Y; Frohne, Ursula; Weibel, Peter (eds.). *CTRL [SPACE]: Rhetorics of Surveillance from Bentham to Big Brother*. MIT Press, Cambridge, MA.
- [25] Roslyn Orlando. 2021. *Evasion Score*. Retrieved June 28, 2025 from <https://firstdraft.org.au/soft-power-pages/evasion-score-roslyn-orlando>
- [26] Andy Greenberg. 2014. *An Eavesdropping Lamp That Livetweets Private Conversations*. *Wired*. Retrieved June 28, 2025. <https://www.wired.com/2014/04/coverstitch-eavesdropping-lightbulb/>