Arushi Bandi and Cecelia Brower

A Phenomenological Approach to Life Under Surveillance[1]

Introduction

In this essay, we understand phenomenology as the study of "conscious experience as experienced from the subjective or first person point of view" (Smith, 2018, para 1) , or the study of the "lifeworld" as distinct from objective "worlds" of academia and natural sciences (Encyclopædia Britannica 2016) . Our main concern is with applying a phenomenological approach to surveillance and its ethicality. In order to do this, we adopt the view of technology and ethics outlined in the *Stanford Encyclopedia of Philosophy* by Introna (2017, sec 1.3) that:

> Technology and society … are each other's condition of possibility to be. Technology is not the artifact alone it is also the technological attitude or disposition that made the artifact appear as meaningful and necessary in the first instance … The task of ethics is … to open up and reveal the conditions of possibility that make particular technologies show up as meaningful and necessary (and others not). It seeks to interrogate these constitutive conditions (beliefs, assumptions, attitudes, moods, practices, discourses, etc.)

Additionally, we will make use of Don Ihde's phenomenology of human/technology relationships, which characterizes them as either 1. *embodiment*: technology taken as the very medium of subjective perceptual experience of the world (e.g. eyeglasses), 2. *hermeneutic*:

[1] Due to page limits of this essay and the extensive background that was necessary, we chose to focus most of our energy on the more interesting and novel work of analysing a few accounts of surveillance from a phenomenological point of view, rather than strongly maintaining an ethical or political stance. We examine the accounts under existing ethical theories along with phenomenology to determine how the two come to different conclusions and briefly state implications for possible new ethical stances at the end of this essay. We understand that this is not exactly what the assignment asked, but we hope this creative take on an issue discussed in class suffices to show our engagement with class material and concepts.

technology as an immediate referent to something beyond itself (e.g. maps, language), 3. *alterity*: technology experienced as a being that is otherwise, technology-as-other (e.g. smart robots), or 4. *background*: technology not directly implicated in a conscious process of engagement on the part of the human actor (e.g. air-conditioning, traffic lights) (Introna, 2017, sec 2.4). We will examine how human/surveillance relationships can shift between these categories, based on the context it is experienced in. We consider our phenomenological view of surveillance in relation to existing theories of surveillance and find that a phenomenological approach to surveillance discovers the constitutive conditions that allow surveillance to exist in its current form in addition to its direct impact on the lifeworld of surveillants. When discussing the ethicality of surveillance, we must then decide as a society what type of subjective experience to confer on individuals.

Brief Overview: Types of Surveillance and History of Surveillance

Surveillance has existed in forms such as prison guards for hundreds of years, but new settings for surveillance are becoming increasingly common. One of the most well-known uses of surveillance is public surveillance, by way of security cameras in public spaces. It is sometimes assumed that in public spaces, surveillance is less controversial because we are inherently observed by others. However, this is not the same phenomenon as surveillance because there is more permanence and consequence to modern surveillance than seeing other people as a temporary observer (Patton, 2000, p. 181-187).

Dataveillance, short for data surveillance, is the collection of data from personal devices and platforms in order to gain information about the persons using the device or application.

Dataveillance has mainly been used by two entities with different motivations. One is the government, under the guise of keeping citizens safe. The other is corporations, for the stated purpose of improving user experiences. The use of this data by the government has allowed it to keep tabs on innocent people through dataveillance in the name of stopping potential future crimes. This justification became much more prevalent shortly after September 11th, when the 2001 USA PATRIOT Act was passed to "identify and neutralize potential threats and the sources from which they emanate (Mace, 2009, p. 1)." The USA PATRIOT Act allowed for the data collection by the government at levels previously considered unlawful (Mace, 2009).

Corporate dataveillance by companies like Facebook and Google is often justified under the promise of improved user experience, but often the extent of data mining seems to go beyond what would be necessary simply for this purpose. As a result of these platforms' ubiquity, we are seeing higher amounts of information being collected, to the point that these companies have developed entire profiles of their users. These profiles are often unviewable and include data such as shopping history, credit card information, search history, and website clicks (Zimmer, 2008).

The last type of surveillance discussed in this article is interveillance, which is different because it exists largely as a form of entertainment and social life, rather than an assurer of safety. Interveillance refers to "the expanding prospects of mediated self-enclosure and self-disclosure," or in other words, watching others perform themselves and watching others watching you perform yourself. The main example of this is social media, where users see more of other users' curated lives that previously was not as immediately accessible (Christensen &Jansson, 2015, p. 1473-1491).

A Review of Surveillance Theories

The first stage of surveillance theory began with Bentham's idea of the "prison Panopticon" and Foucault's expansion on it. The "prison Panopticon" was an idealized circular prison where a guard in a watch tower in the center watched over the prisoners, to make the prisoners feel as though they were continually surveilled, despite this being infeasible in actuality. Bentham presents the guard to be "all-seeing, omniscient and omnipotent (Galič et al., 2017, 12)" from the prisoner perspective, to show that full surveillance was not only unnecessary, but also undesirable because of the extra resources it required. This system was effective because the feeling of being constantly watched in itself would prevent most wrongdoing. In the case that wrongdoing was committed and discovered, the prisoner would be punished, and consequently feel like the guards were always watching. Bentham was of the opinion that surveillance was only ethical when apositive impact is achieved as a result, such as preventing moral infractions by prisoners in this example (Galič et al., 2017, 9-37).

Foucault took Bentham's ideas and expanded them to theorize this system in broader society. Foucault explored "disciplinary societies" in which power is widely distributed among and surveillance can come from many directions, so the watcher is often unseen by the watched. These societies allow systems of power to shape the individual by enforcing "norms" through implied surveillance. When people feel as though they are always seen by "norm" enforcers (e.g. the government) at all times, they feel increased pressure to ascribe to it to avoid disciplinary action. Foucault's theory has implications particularly for public surveillance. In theory, if the

government encourages certain public norms and deploys public surveillance cameras, then these cameras encourage that behavior (Galič et al., 2017, 9-37).

Deleuze has yet another theory on how surveillance can be used to manage societies. He introduces the "control society" where in place of a single omnipotent and unseen watcher, there are multiple players consistently watching all aspects of society, with emphasis on capitalism and corporations. He concentrates on "short-term results" achieved through the surveillance of the current markets and changes made in the markets based on that. Deleuze's ideas are summarized in the statement "the point is no longer making bodies docile, but to mould consumers, whose data-bodies become more important than their real bodies (Galič et al., 2017, 20)."

The last of the traditional approaches to surveillance is the Marxist approach. This approach led to the idea of "surveillance capitalism" which similarly molds individual behavior for the purpose of maximising capital gain. Surveillance capitalism is motivated by the rising amount of data in capitalistic societies. The more information corporations have about people, the more they can both predict what people want and shape people to want new things. This theory is still in development, as the practice of surveillance capitalism is relatively new (Galič et al., 2017, 9-37).

A Phenomenological Approach: Sartre's "The Look", Interveillance, and Dataveillance

In this section, we examine several first-hand accounts of experiencing surveillance, from a range of authors and contexts. For each account, we point out the intricacies of the resulting human/surveillance relationship, the categorization of this instance of surveillance under one of Ihde's classifications, and the "constitutive conditions" that allow such a relationship to take

place. Identifying these constitutive conditions allows us to examine the justification of such surveillance, and whether they would hold if these conditions were to change or to be proven inadequate.

First, we will briefly discuss the thoroughly examined "The Look," by Sartre, a phenomenological account of the experience of observing people in a room through a keyhole, then hearing footsteps behind you, indicating someone is watching you spying. The shift of the narrator from watcher to watched parallels the shift of the narrator from "subject to object" where "lived relation is now largely determined by the objectifying gaze of a second observer" in the latter case (Friesen et al., 2009, 86). This is significant because it points out the difference between living with and without an 'objectifying gaze' - that of experiencing yourself' through the eyes of another, with different motives, beliefs, and values. This account is applicable to the case of mass surveillance in public areas, where someone observing their surroundings, or simply living, is in turn being watched by CCTV cameras, consistent with the experience of being under an 'objectifying gaze.' However, this experience is markedly different by the fact that the watcher is not a person who can be confronted and whose footsteps can be heard, rather a silent watcher. A phenomenological account of this modern experience of surveillance is more akin to the *background* human-technology described by Ihde, whereas the narrative in "The Look" would lead to an *embodiment* relationship. This difference is due to the fact that the pervasiveness of CCTV cameras numbs our active response to them: "when everybody can potentially be under surveillance, people will internalise control, morals and values—discipline is thus a type of power, a strategy and a kind of technology" (Galič et al, 2016, p. 16). In other words, an *embodiment* relationship with surveillance shifts to a *background* relationship as we

adapt to accommodate the new norms necessary to live with a constant watcher, so much so that we become unaware of it. Thus our adaptation to the point of unawareness is the constitutive condition that allows for mass surveillance in public spaces to permeate. If instead, however, we were in a state of constant awareness of an "objectifying gaze" as in Sartre's account, the condition allowing for such ubiquitous surveillance to present itself as meaningful would no longer exist, calling into question its ethicality. This has implications for a Foucaltian model of surveillance, as we see that Foucalt's "disciplinary" surveilling power operates via an *embodiment* relationship with its surveillants. Once, this *embodiment* relationship has shifted to a *background* relationship, however, the surveillants cease to actively feel an "objectifying gaze" as noted by Sartre. If such surveillance is no longer sufficiently "disciplinary," as has been the case in several cities deploying surveillance in the hopes of deterring crime (Porter & Hirsch, 2009, paras. 1, 5), its necessity is unjustified and the question regarding mass public surveillance then becomes: what type of subjective experience, or "lifeworld" do we want our society to maintain in public spaces?

In "The Spy Is a Camera," by the magazine *Real Life,* Coleman outlines the nuances around personal privacy that many people have around social media, or the act of engaging in interveillance. A subjective account from Coleman (2016, para 19) is:

> When my friend admits with delight how he loves to look at others looking at him, maybe he's really loving how novel it feels to know you're being surveyed: to be a sub who's really in control. It's hot to imagine yourself being seen, being watched, when you're controlling the terms — when you're three taps away from "Hide from My

Profile." That submission is a choice, but control is a given, is the fantasy your tagged photos encourage.

Applying a phenomenological view of the human-technology relationship to this account, we see that interveillance presents itself not only as the capacity to share pictures and life updates with friends and family and reach a wider audience (Rainie, 2018, para 5), but also as the newfound ability to experience what was previously impossible - to see yourself as others see you in real time and control what they see. In a phenomenological account of interveillance, the particular relationship between humans and their social media platform creates an ongoing mode of "routinized social monitoring" consisting of 1) watching and judging others, 2) watching others watching oneself, and 3) watching one's "data double.", or their curated self presented on the Internet (Friesen, 2009, p. 1480). Although "routinized social monitoring" has always been a natural facet of human life, the current technologies allow for this to occur at significantly larger scale and detail. This phenomenological analysis of interveillance lends itself to categorize the human-interveillance relationship in its most mainstream forms as an *embodiment* relationship. In more concrete terms, the medium of interveillance (Facebook, Instagram, etc.) becomes a part of the perceptual experience of the "lifeworld", indistinguishable from its place as a technology, where such a distinction might exist under other approaches to the human/interveillance relationship. The constitutive condition for such a vast network of interveillance to exist is that we often accept constant updates, pictures, and connection as objective and with approximately the same weight as we would have previously considered equivalent "in-person" interactions. The implication of this for the ethicality of issues surrounding social media (such as the limits of freedom of speech and press, social media as a potential military weapon) is the questioning of

this condition. Specifically, if we were to reject the notion that the act of interveillance holds the same weight as similar actions in the physical world, how might we redefine freedom for individuals use of social media and the dataveillance of these platforms? One issue regarding such corporate dataveillance is the use of targeted ads and surveillance capitalism. These practices exist because consumers have integrated social media platforms so deeply into their lives, a result of the constitutive condition described above. Additionally, these corporate systems operate on the notion that the products they are selling us are what we want, because we have supplied them with such accurate data. When we call the latter condition into question, it becomes apparent that these companies follow closely to Deleuze's theory of consumer-moulding, but also that such a market is not necessarily inevitable. Specifically, surveillance capitalism only thrives when we seek to replicate our "real world" data (such as health and financial data, personality traits) on these social platforms and buy into the claim that we are being sold what we want, which sometimes isn't actually the case, as noted by the New York Times report on e-commerce's advertising measures blurring the lines between persuasion and manipulation (Valentino-DeVries, 2019). Additionally, we see that a phenomenological approach to interveillance reveals that no prevailing popular theory of surveillance accounts for this new breed of surveillance deeply intertwined with entertainment and social life, thus an altogether new theory of interveillance must be created. A Deleuzian take on interveillance accounts only for the corporate oversight of it, leaving out the subjective experience of using these social platforms, which can often bring feelings of joy and power to the individual, as noted in the account.

The last phenomenological account of surveillance presented in this essay pertains to dataveillance, specifically the subjective experience of living in the authoritarian surveillance state of China. In "Feeling Safe in the Surveillance State" Jianan Qian (2019, para 9) writes about her experience returning to the country after living abroad for several years:

> Entering train stations felt like crossing border control at an international airport — my identity was confirmed not only by someone checking my documents, but also by one of the ubiquitous facial recognition cameras. One day, while a friend was driving me home after a reading in Shanghai, I saw one of them ahead of us on the highway. Well, we can no longer do "bad" things, he said, noticing my discomfort. It was supposed to be a joke, but we fell into a long, dead silence. Many people in China seem to be happy about the physical security promised by the surveillance network. Our mind-set, long ago, was wired to see safety and freedom as an either-or choice.

This portrayal of life in China reveals the mental tact involved in accepting life under dataveillance. The '"bad" things' mentioned by Qian's friend is a stand-in for all things that might draw attention to someone under the government's sprawling facial recognition and tracking system. Her statement that their minds were "wired to see safety and freedom as an either-or-choice" unveils the beliefs that must be accepted by a people in order for states to convince them of the justness and necessity of such a system. If we were to question this belief - that safety and freedom are mutually exclusive - the ethicality of such widespread and comprehensive surveillance would come into question as well, as we would consider a world where both are simultaneously possible. Such systems form a Deleuzian "control society," with the defining feature that "control societies not only exercise a different method of governing and

as such form a fault-line in thinking about surveillance and the types of societies that surveillance creates" (Galič et al, 2016, p. 18). In other words, someone who has conformed to a control society may not be able to publicly question its ethicality due to the "normation and internalisation of 'doing good'" under that society, which is in turn defined as not standing out from the rest of the population, by abiding by all norms (Galič et al, 2016, p. 18). The human/dataveillance relationship in such a situation then becomes one of *alterity*, where the omnipresent cameras refer to something other than oneself, specifically the likewise omnipresent oversight of the government. Each camera is a reminder not simply of the fact that you can no longer do '"bad" things', but also that whatever you do is seen by those above you and can be seen by all if you do wrong. In some sense, your behavior is not owned only by you, and this deal is presented as the price to pay for safety. The Foucaultian "disciplinary" model of surveillance that this operates is reliant on the constitutive condition established by the surveiller that safety and freedom are mutually exclusive. However, if citizens are to reject this notion, then the ethicality of government dataveillance comes into question, putting pressure on the surveiller to find a new justification for their surveillance measures rather than putting pressure on the surveillants to psychologically accommodate for stripped freedoms.

Conclusion

In the previous section, we uncovered the constitutive conditions that allow our relationship with various types of surveillance to exist in the current form, and allow these types of surveillance to present themselves as meaningful and necessary in their respective contexts. Mass surveillance has been adopted so widely because of our acclimation to it to the point that

we are no longer aware of its existence. Interveillance thrives because we accept it as an accurate representation of the "real world" and corporate dataveillance because we believe that we are being sold what we want by companies, who in turn base this claim on ours of accurate representation. Government dataveillance is accepted by a society almost solely under the belief that safety and freedom are mutually exclusive. A change or complete removal of these constitutive conditions would cause our relationship with these systems to change at the least, and in more extreme cases the necessity of these systems are no longer justified, since their ethicality is likewise based on these constitutive conditions. Additionally, no prevailing theory of surveillance accounts for all of the new strands of surveillance which are routinely encountered in modern times and must be dealt with formally. From this we see that modifications to both the philosophy and ethicality of various types of surveillance is required, as a result of a phenomenological framing of modern instances of surveillance.

Due to page limits on this essay, we will not detail the specifics of a new ethical theory based on our findings here. We previously mentioned that following a phenomenological approach towards surveillance guides us to consider what type of subjective experience to confer on individuals of the society. Thus, we will outline a few takeaways from this analysis that serve as guidelines to follow when shaping subjective experiences under surveillance. First, we hold that when creating systems of surveillance, it is necessary to consider the implicit values embedded in such systems, and explicitly state and question those. This follows from our finding that safety and freedom were accepted as mutually exclusive by some under the country of China, despite a lack of evidence supporting this. Additionally, when people inadvertently believed this proposition they had no incentive to question the existing surveillance state,

because they doing so would equate to questioning their safety which is illogical. An ethical theory of surveillance systems must account for such obstacles in the basic questioning of such systems - in other words, if a system cannot be analyzed and questioned by the people who live under it due to its presentation in society, it is potentially unethical in some aspect. Second, we maintain that an ethical theory of surveillance systems that are in practice involuntary on behalf of the individual experiencing them must address the ethicality of the question "who holds the power to surveil?" in addition to the surveillance itself. Through the analyses of mass public surveillance and corporate dataveillance (which are only escapable by going completely off the grid and being unidentifiable in public, which is not an option for most acting members of society), we saw that the power to surveil was held by the government and large tech corporations. This power reinforces their existing control over members of society, and this fact must be considered from an ethical stance when considering the surveillance they maintain. It is often unethical for those in power to hide the constitutive conditions on which they are justifying their use of surveillance. For example, the PATRIOT Act was justified based on the idea that safety comes from citizens relinquishing their privacy, but this was simply assumed to be the case, which led to alternatives not being explored, and a lack of clarity on why this was the case. This lack of transparency from the surveiller to surveillant is what crosses the line into unethicality.

These are just a few examples of how phenomenology can aid in better examining the ethicality of issues surrounding technology. As the systems of surveillance continue to grow daily, it is important to revisit these issues from a phenomenological perspective to understand their effect on the human psyche and make more informed decisions regarding their ethicality.

References

Christensen, M., & Jansson, A. (2015). Complicit surveillance, interveillance, and the question of cosmopolitanism: Toward a phenomenological understanding of mediatization. *New Media & Society, 17(9)*, 1473-1491. https://doi.org/10.1177/1461444814528678

Coleman, L.M. (2017). *The Spy is a Camera.* Real Life Magazine. https://reallifemag.com/the-spy-is-a-camera/

Friesen N., Feenberg A., Smith G. & Lowe S. (2012). *Experiencing Surveillance.* (A. Feenberg & N. Friesen Eds.) SensePublishers.

Friesen N., Feenberg A., & Smith G (2009). Phenomenology and Surveillance Studies: Returning to the Things Themselves, T*he Information Society, 25(2)*, 84-90, https://doi.org/10.1080/01972240802701585

Galič, M., Timan, T. & Koops, B. (2017) Bentham, Deleuze and Beyond: An Overview of Surveillance Theories from the Panopticon to Participation. *Philos. Technol. 30*, 9–37. https://doi.org/10.1007/s13347-016-0219-1

Hongladarom, S. Rafael Capurro, Michael Eldred and Daniel Nagel. (2017) Digital Whoness: Identity, Privacy and Freedom in the Cyberworld. *Minds & Machines, 27*, 259–263 . https://doi.org/10.1007/s11023-016-9391-4

Introna, Lucas. (2017). Phenomenological Approaches to Ethics and Information Technology. *The Stanford Encyclopedia of Philosophy.* (Fall 2017 Edition). https://plato.stanford.edu/archives/fall2017/entries/ethics-it-phenomenology/.

Mace R.R. (2009) Intelligence, Dataveillance, and Information Privacy. In: Gal C.S., Kantor P.B., Lesk M.E. (eds) Protecting Persons While Protecting the People. ISIPS 2008. Lecture Notes in Computer Science, 5661. Springer, Berlin, Heidelberg.

Patton, J.W. (2000) Protecting privacy in public? Surveillance technologies and the value of public places. *Ethics and Information Technology 2*, 181–187. https://doi.org/10.1023/A:1010057606781

Porter, H. & Hirsch, A. (2009). *The truth outs - CCTV doesn't cut crime.* The Guardian. https://www.theguardian.com/commentisfree/henryporter/2009/may/19/cctv-reduce-crime

Qian, J. (2019) *Feeling Safe in the Surveillance State.* The New York Times. https://www.nytimes.com/2019/04/10/opinion/china-internet-surveillance.html

Rainie L. (2018) *How Americans feel about social media in an era of privacy concerns.* Pew Research Center. https://www.pewresearch.org/fact-tank/2018/03/27/americans-complicated-feelings-about-social-media-in-an-era-of-privacy-concerns/

Smith, D. W. (2018). Phenomenology, *The Stanford Encyclopedia of Philosophy. (*Edward N. Zalta Ed.). https://plato.stanford.edu/entries/phenomenology/

The Editors of Encyclopaedia Britannica. (2016). Life-world. In *Encyclopædia Britannica.* Encyclopædia Britannica, inc. https://www.britannica.com/topic/life-world

Valentino-DeVries, J. (2019) *How E-Commerce Sites Manipulate You Into Buying Things You May Not Want*. The New York Times. https://www.nytimes.com/2019/06/24/technology/e-commerce-dark-patterns-psychology.html

Zimmer M. (2008) The Gaze of the Perfect Search Engine: Google as an Infrastructure of Dataveillance. In: Spink A., Zimmer M. (eds) Web Search. Information Science and Knowledge Management, vol 14. Springer, Berlin, Heidelberg