FILOZOFIA I NAUKA
Studia filozoficzne i interdyscyplinarne
Tom 10, zeszyt specjalny, 2022

Dustin Gray

MODERN FORMS OF SURVEILLANCE AND CONTROL

doi: 10.37240/FiN.2022.10.zs.9

ABSTRACT

In todays advanced society, there is rising concern for data privacy and the diminution thereof on the internet. I argue from the position that for one to enjoy privacy, one must be able to effectively exercise autonomous action. I offer in this paper a survey of the many ways in which persons autonomy is severely limited due to a variety of privacy invasions that come not only through the use of modern technological apparatuses, but as well simply by existing in an advanced technological society. I conclude that regarding the majority of persons whose privacy is violated, such a violations are actually initiated and upheld by the users of modern technology themselves, and that ultimately, most disruptions of privacy that occur are self-levied.

Keywords: philosophy of technology, data privacy, surveillance, autonomy.

1. INTRODUCTION

How much should we care about our right to privacy, and how much of a role does it play in the total amount of autonomy we experience? Does it make sense to believe that "privacy is a function of liberty" as some do (Rusbridger, MacAskill, 2014)? If we are to follow this line of reasoning, then we are bound to the presupposition that to experience liberty, we must also *have the option* to keep as much of our lives private as we deem appropriate. In doing so, we would be living by a specific self-determined rule and to that extent, have autonomy.

However, an important consideration to make regarding autonomy and privacy is that in virtue of having the former, the rational agent has the final say on how highly she values the latter. The mere exercise of choice as to whether one's privacy is important or not is in itself emblematic of autonomous action. The argument I want to make, however, is that the invasion of privacy that occurs by means of what I call *technological surveillance*—as administered to everyone who exists in today's advanced society—can be

regarded as impermissible. "Technological surveillance" should be recognized in its use throughout the paper as the unwarranted audio, visual, and or digital monitoring of a rational agent's affairs by another.

In this paper, I will aim to provide a greater understanding of what it means to have our privacy pilfered by means of surveillance in a variety of capacities. There will be a discussion on how surveillance is used to control persons within a given society and how this can be seen as a form of oppression that is—in many ways—*self-instituted*. I will argue that many seem to, without concern, place themselves in a position to be regulated in this manner. While some may be oblivious, others simply remain indifferent in regard to the numerous structures put in place to ensure that residents of this and many other countries are being watched, listened to, and otherwise monitored every day (Schwartz, 2017).

To be sure, many methods of surveillance are unavoidable, such as automated license plate readers, public space cameras, and audiovisual surveillance employed on public transportation. I argue, however, that all who use information devices such as mobile phones, computers, and even credit cards *place themselves* in a position to be monitored. Each time these devices are used to make calls, send texts, watch funny cat videos, interact on social media, purchase goods and services, send and receive emails, or conduct internet searches, what is said and heard, sent and received, viewed and posted, bought and sold, and taken interest in is monitored and scrutinized. The use of these devices inherently implies a self-imposed forgoing of one's autonomy. One who places even a shred of value on the retention of her privacy who, in turn, voluntarily discloses her personal information via modern technology could hardly be seen as living by rules set for herself. Not only are these data monitored, but they are stored as well. This retention of another's personal information without permission further demonstrates a loss of autonomy and I argue is deserving of just as much attention as might be given to the manner in which the data is collected. The collection and storage of one's data in this sense does imply a *taking*, but we must not be tempted to think that in collecting and storing our intellectual property it is modern technology that operates as the *taker*. No doubt, we are stripped of our autonomy by technological means, but the identity of the thief lies not in anything technological.

I want to suggest that, ironically, those who most enthusiastically adopt and integrate the modern technological advances that ultimately control them, tend to believe they experience the highest degree of freedom. Furthermore, I argue that the widespread adoption and use of modern technologies is precisely what facilitates the forms of surveillance I am critical of. I will consider those persons who use modern technological devices such as telephones (both standard landline and mobile), computers, "smart" home security systems to be what I call *users*. By integrating the regular use of

these contrivances, persons put themselves in a position to be surveilled by those who I will refer to as *sentinels*. The primary responsibility of the sentinel is to record as much information about the user as possible by means of surveilling her conduct and behavior. But simply monitoring the day-to-day activities of the user will not be enough. Also crucial to the mission of the sentinel is the *storage* of this data for later use, to have a continually growing surplus of information that can be referred back to at any time.

Generally, there are two ways in which the sentinel administers control via surveillance. The first is by way of *corporate* surveillance. The sentinels in this category are technicians and engineers at large and powerful tech companies such as Google, Amazon, and Facebook. The sentinels behind the veil of these entities—as motivated by an all-out perversion of the capitalist venture—have developed an ingenious method to influence the decision-making processes of the consumer. This is done in many ways, but among the most prevalent are the digital monitoring of users' internet searches and the audio surveillance via information devices of what is said by users in their day-to-day lives.

The second means by which users are controlled is what I refer to as *governmental* surveillance. Though specific processes vary, there are three primary methods. The first is simply the audio and visual recording of conduct by means of publicly installed video cameras and microphones. The second is done by the monitoring, recording, and storage of persons' telephone conversations. The third, and possibly most invasive method, is the continuous monitoring and storage of the user's internet activity. In these instances, it turns out that the sentinel is part of the very structure that was originally implemented to protect the rights of its people, yet instead now operates as a system designed to deny that which it promised to protect and uphold.

Notice here that one does not necessarily need to be a user of modern technology to be surveilled. In regard to the first method of governmental surveillance, one only need walk about and congregate in the public arena to become subject to monitoring of this type. This non-user I will refer to more generally as the *citizen*. Being perhaps the greatest minority in existence today, she is still not free from surveillance outside her own home. We might say that all users, too, fall into the category of citizen by existing in an advanced technological society and that one can easily go from user to citizen by way of the use or non-use of modern technology. It is this possibility of transition from user to citizen that implies a choice of degree to which one is controlled. There will be more to come on this toward the end of the paper.

2. CORPORATE SURVEILLANCE

So with a general understanding of the ways in which surveillance takes place, I will now move into the specifics of its operation. Let us begin with the corporate method. In her seminal book, *The Age of Surveillance Capitalism*, Shoshana Zuboff gives an extraordinarily detailed account of how corporate surveillance originated and is practiced today. As the title suggests, she argues that surveillance capitalism is the current standard for technological control over the purchasing practices of today's consumers.

> "Surveillance capitalism unilaterally claims human experience as free raw material for translation into behavioral data. Although some of these data are applied to product or service improvement, the rest are declared as proprietary *behavioral surplus*, fed into advanced manufacturing processes known as 'machine intelligence,' and fabricated into *prediction products* that anticipate what you will do now, soon, and later. Finally, these prediction products are traded in a new kind of marketplace for behavioral predictions that I call *behavioral futures markets*. Surveillance capitalists have grown immensely wealthy from these trading operations, for many companies are eager to lay bets on our future behavior." (Zuboff, 2020, p. 8)

From her definition of the term, we find that surveillance capitalism sees the experience of the consumer not as a *subject* to be studied for market research but rather as an *object*. The consumer's experience is considered as data to be compiled as a method by which the corporate sentinel can predict what the user will do next.

Though much could be said about Zuboff's overall analysis, for the purposes of this paper, I will keep a narrow focus on what she discusses concerning the two methods of corporate surveillance listed above: the monitoring of consumers' internet searches and the audio surveillance of consumers' speech. Maintaining that order, let us first explore the ways in which this particular sentinel derives information and makes suggestions based on our internet searches.

Each time you type something into a search engine and press enter, that which you query is captured and stored by, for instance, Google. Zuboff informs us that not only is the keyword itself noted but additionally "each Google search query produces a wake of collateral data such as the number and pattern of search terms, how a query is phrased, spelling, punctuation, dwell times, click patterns, and location" (Zuboff, 2020, p. 67). This collection of information is what Zuboff terms "behavioral data," those data that the user freely provides to Google—or any given search engine—which the sentinel then uses to predict future patterns. Behavioral data alone, though, are of little use to the search provider unless they are *stored*.

During Google's early stages of implementation in the late 90s, "these behavioral by-products were haphazardly stored and operationally ignored" (Zuboff, 2020, p. 67). In the beginning, Google itself did not see the immense potential value of these data; they were merely supplementary bits of information retained within the servers as a result of the users' searches. The original purpose of data collection was, as the company claimed then and still does today, to improve the user's experience by catering search results to the individual based on her search patterns. "Google's engineers soon grasped that the continuous flow of collateral behavioral data could turn the search engine into a recursive learning system that constantly improved search results and spurred product innovations such as spell check, translation, and voice recognition" (Zuboff, 2020, p. 68).

It was not until Google found itself in need of additional revenue streams that behavioral data emerged as a vast untapped mine of profitability. During the first two years of its establishment in 1998, the founders of Google, Larry Page and Sergey Brin, maintained a "passionate and public opposition to advertising" (Zuboff, 2020, p. 74). But in December of 2000, a damning *Wall Street Journal* article incited concerns of future profitability in the company's investors. The article generally targeted many Silicon Valley startups by saying, "Simply displaying the ability to make money will not be enough to remain a major player in the years ahead" (Zuboff, 2020, p. 74). The article maintained that what would be required would be "an ability to show sustained and exponential profits" (Zuboff, 2020, 74). In response to investor anxiety, Page and Brin departed from their earlier convictions on advertising and set the then seven-person internal department, AdWords, on a project to find new streams of revenue. "Operationally, this meant that Google would turn its own growing cache of behavioral data and its computational power and expertise toward the single task of matching ads with queries" (Zuboff, 2020, p. 74). Put simply, the advertising would have to become "relevant" to users. More appropriately, as Zuboff remarks, "a particular ad would be 'targeted' to a particular individual" (Zuboff, 2020, p. 74). She terms this immense reserve of user information as "behavioral surplus." Not only is this what ultimately led to the "sustained and exponential" profits Google was after, it also served as the origin of the epoch of corporate surveillance or what Zuboff would call surveillance capitalism (Zuboff, 2020, p. 99).

Worth noting at this point is an argument made nearly 70 years prior to that of Zuboff's. Martin Heidegger maintained in *The Question Concerning Technology* that the goal of technology is to place that which is derived for modern technological purposing into "standing reserve." "Everywhere everything is ordered to stand by, to be immediately at hand, indeed to stand there just so that it may be on call for a future ordering" (Heidegger, 2013, p. 17). I argue that the collection and storage of user's search patterns on the internet by any means is fundamentally related to this claim.

This brings us sharply to Zuboff's claim that our conduct on the internet is *commodified*. This modern instantiation of human behavior is monitored, commandeered, and stored for the purpose of predicting future instantiations thereof by companies like Google so that they might turn a profit. She claims that what we do online is digitally *dispossessed*.

> "Today's owners of surveillance capital have declared a fourth fictional commodity expropriated from the experiential realities of human beings whose bodies, thoughts, and feelings are as virgin and blameless as nature's once-plentiful meadows and forests before they fell to the market dynamic. In this new logic, *human experience is subjugated to surveillance capitalism's market mechanisms and reborn as 'behavior*.' These behaviors are rendered into data, ready to take their place in a numberless cue that feeds the machines for fabrication into predictions and eventual exchange in the new behavioral futures markets." (Zuboff, 2020, p. 100)

In other words, we ourselves have become the resources mined for standing reserve. "Knowledge, authority, and power rest with surveillance capital, for which we are merely 'human natural resources' " (Zuboff, 2020, p. 100). Those who control the technological powers that be may claim to be monitoring our conduct online to cater their services to our individual wants and needs, but the true motivation has become profitability via appropriation of users' behavioral data (Viadhyanathan, 2011, pp. 21–23).

Another sentinel that has become a leading frontrunner in the use of corporate surveillance is Facebook. Nearly everyone today is aware of the "Like" button. This seemingly harmless digital apparatus is clicked on by Facebook users to express interest in or approval of other users' posts on the social media platform. However, there is a much deeper functionality behind the veil of congeniality proposed by the "Like" button. Each time you "like" a post, something called a "cookie" is installed into your computer, tablet, or smartphone. Not unlike a burrowing parasite, these tiny bits of code embed themselves into your device to establish and allow intersystem communication between Facebook and the end user. The information gained through this exchange is used by Facebook analysts to determine which ads will display based on your interests. Again, the user's behavior online has become a human resource to be exploited for the purpose of targeted advertising that will lead to profitability for the sentinel.

Some might say, however, that this degree of privacy invasion is to be expected. When one signs up for a Facebook account, she is required to read and agree to a lengthy terms and conditions document, which outlines all of this in the privacy section. All Facebook users are informed of the risk they are taking by clicking the "Agree" box. However, in an article published by privacy researcher Arnold Roosendaal, it was found that even non-users of Facebook's services were being monitored as well simply by viewing

webpages associated with Facebook data (Roosendaal, 2010). So as it turns out, even those who do not agree to Facebook's terms are possible targets of corporate surveillance.[1]

Perhaps this, and what was expressed in regard to the data mining tactics employed by Google could be seen as harmless. In fact, there are some who might say they enjoy these predictive features in that they are presented with ads for products they actually are interested in. With these persons, I cannot and will not argue. But I will present one more example that might change the mind of even the most tolerant user.

Zuboff tells of a particularly disturbing service offered by various companies referred to as "service-as-software" (SaaS). She more appropriately deems it as "surveillance as a service" (SVaaS). For example, app-based technologies are being used by financial lenders to monitor the digital and physical behavior of potential borrowers before deciding whether they will provide a loan. One particular app "instantly establishes creditworthiness based on detailed mining of an individual's smartphone and other online behaviors, including texts, emails, GPS coordinates, social media posts, Facebook profiles, retail transactions, and communication patterns" (Zuboff, 2020, p. 172). Not only are these digital data collected, but physical patterns of behavior such as phone charging frequency, whether a user returns calls and how long it takes her to do so, or the distance a user travels each day are also taken into account (Zuboff, 2020, p. 172). Though the common user of information devices might think that data mining for the purpose of targeted advertisement is permissible, this degree of privacy invasion can and will stand directly in the path between a user and her potential to achieve financial security. This instantiation of corporate surveillance entails not the common, "that's just the way it is" mentality. It brings to the forefront a much deeper element of control involved with the surveillance perpetrated by corporate sentinels on users requiring their services.

Thus far, we have explored the actualities of corporate surveillance relating only to the user's conduct online. There is, however, another important feature of this invasive oppressive force that I would like to explore. Much of modern technology today exists in the home, and this is where we its most intimate forms of use occur. Digital assistants such as Alexa and Nest are among the most popular. With these devices, a user can simply verbalize the desire to listen to a particular song or artist, change the temperature on her thermostat, turn lights on and off, lock and unlock doors, etc. These capabilities might seem to provide freedom within one's home but consider also that having these devices installed presupposes the remittance of one's con-

[1] Since Roosendaal's findings, much has transpired. See pages 158–161 of Zuboff's *The Age of Surveillance Capitalism* to learn more about the many allegations made against Facebook regarding its surveillance methods and the ways in which the company defended itself by claiming that these practices were merely a "glitch" or "bug" in the system.

trol to these functionalities. Also worth noting is that many of these devices are actively listening to your speech patterns in search of specific indicators of what you may desire as a consumer. "Pieces of your talk are regularly farmed out in bulk to third-party firms that conduct 'audio review processes' in which virtual scorers, tasked to evaluate the degree of match between the machines text and the original chunk of human speech, review audio recordings retained from smartphones, messaging apps, and digital assistants" (Zuboff, 2020, p. 262). So not only is this data used to provide targeted advertising of goods and services on any device connected to the home system, it is also collected by third party firms to perfect the devices' ability to match what is recorded to the individual user.

It is insisted upon by companies such as Amazon, Google, and Microsoft that these data are anonymous and cannot be linked to individual users, but Zuboff cites the findings of a freelance journalist, A. J. Dellinger, who discovered loopholes in these claims of anonymity.

> "Within the recordings themselves, users willingly surrender personal information—information that is especially valuable in these review processes because they are so specific. Uncommon names, difficult-to-pronounce cities and towns, hyperlocal oddities [...]. I heard people share their full names to indicate a call or offer up location-sensitive information while scheduling a doctor's appointment [...] the recordings capture people saying things they'd never want heard, regardless of anonymity [...]. There isn't much to keep people who are listening to these recordings from sharing them." (Dellinger, 2015)

Zuboff tells of one device in particular that arguably took these capabilities too far. Besides smartphones and digital assistants, Smart TVs are highly sought after by consumers of modern technology. But in 2015, it was found by privacy advocates that Samsung's line of these devices may have been too smart. Not only when instructed to do so, these particular Smart TVs were recording everything said within an earshot of the system. The TVs were capturing phrases such as "*please pass the salt; we're out of laundry detergent; I'm pregnant; let's buy a new car; we're going to the movies now; I have a rare disease; she wants a divorce; he needs a new lunch box; do you love me?*—and sending all that talk to be transcribed by another market leader in voice recognition systems, Nuance Communications" (Zuboff, 2020, p. 263). If we consider the fact that the unique individual fingerprint associated with our voices is something that many firms regard as their sole object of interest as Zuboff has suggested, having the intimate details of our lives recorded in this manner should be alarming at a minimum.

In most cases, I am sensitive to the possible objections that may arise to my claims. But regarding what has been said in this example, I simply will

not concede. Technologies of this nature make possible an inexcusable degree of privacy invasion, and it is my contention that the manner by which these sentinels monitor and store our speech, thoughts, and actions is unquestionably oppressive. We are given no access to check and balance the capabilities of such contrivances, and short of absolute boycott, the oppression will not stop.[2]

As mentioned early on, these instances of corporate surveillance involve the manifestation of an oppressive force that is *self-levied*. We can sit here all day reveling in our accusations that Google, Facebook, and Amazon are wrongfully dispossessing us of our innermost thoughts and feelings, but the truth of the matter is that we are fundamentally the ones to blame, for we, the users, seem unable to live without the various technologies that the sentinels provide. Sure, tech giants such as the ones we have looked at thus far make a convincing case for the necessity to buy what they are selling, and most do. But it must be remembered that in all of this, we do have a choice. And if I am correct, then one will have a difficult time arguing against the oppression imposed by something that one refuses to live without.

3. GOVERNMENTAL SURVEILLANCE

It is generally accepted that while in public, our actions and activities are subject to monitoring by both audio and video surveillance equipment. Some of these methods are employed by private companies and some by law enforcement (Gomez, 2019). Some might say that being monitored while in public is just indicative of the world we live in today.[3] It could be argued that the modern advantages associated with existence in a technologically advanced society fundamentally come at the cost of our privacy. But just as we have seen with corporate surveillance, I will show that governmental surveillance is just as—if not more so—oppressive.

Consider the fact that deeply intimate and private aspects of your life are being regularly recorded and stored each time you make a phone call, send an email, or use a search engine. Put simply, when you communicate via telephone or on an internet connected device, *you are being monitored*. But in this case, the deployment of surveillance stems not from capitalist profit motive. In what is to be discussed for the remainder of the paper, I will uncover the aggressive tactics employed by our own government to observe and control its populace.

On October 26, 2011, President George W. Bush signed a piece of legislature known as the USA PATRIOT ACT (Uniting and Strengthening America

---

[2] More will be discussed on this in the conclusion.

[3] Arguably, there is much to be said about audio/visual surveillance of the common citizen, but for the purposes of this project, I adhere mainly to those systems of governmental surveillance involving the monitoring of telephonic and internet communications.

by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism) (USA PATRIOT ACT, 2011). This enabled the National Security Agency (NSA) to monitor and record the phone calls and digital communications of every U.S. citizen.

In June of 2013, a former NSA contractor, Edward Snowden leaked thousands of classified documents to the press revealing the NSA's methods and abilities to intercept all Americans' phone calls and internet traffic (Gellman, Blake, Miller, 2014). Subsequently, President Barack Obama addressed public concerns by describing plans to reform NSA spying. He stated, "They're not abusing authorities in order to listen to your private phone calls, or read your emails" (Ackerman, Roberts, 2014). The original phrasing of the Patriot Act was drafted explicitly in its primary intention to seek out and stop the spread of terrorism. In his speech, President Obama was intending to make the case that the common, law-abiding American need not be concerned and would not be directly affected by the conduct of the NSA.

Upon hearing this speech, one might assume that effective measures would be enacted to protect the privacy of Americans' tele/data communications. However, more recently in 2018, *The New York Times* reported that the NSA had tripled its data collection from U.S. phone companies (Savage, 2018). So though there was a changing of the guard in terms of presidential leadership, the NSA not only continued to monitor residents of the United States but actually increased its efforts in doing so three-fold.

Within the philosophy of technology, there is rising concern for digital privacy and the ethics of data collection. As the emphasis of this paper is on the ethical implications of governmental surveillance and data collection, I call upon our old friend, *utilitarianism*, to better understand the consequences of governmental surveillance and decide whether it can be justified.

Typically, Jeremy Bentham is associated with "act" utilitarianism. An example of such would be a Marine jumping on a hand grenade and thus taking the brunt of its force to ensure the safety of his squad.

> "An action then may be said to be conformable to [the] principle of utility, or, for shortness sake, to utility, (meaning with respect to the community at large) when the tendency it has to augment the happiness of the community is greater than any it has to diminish it." (Bentham, 2000, p. 15)

For Bentham, an act is good when its consequences increase the happiness of the community at large. In following the language used by Bentham and the broader logic of language, we could—at the very least, generally—call the American public a community.

In slight variation, John Stuart Mill brought about what is commonly known as "rule" utilitarianism. An example of this would be a given company's policy that if an employee is feeling ill that she not come into the office,

for to do so would create the possibility of getting others sick. "All action is for the sake of some end, and rules of action, it seems natural to suppose, must take their whole character and colour from the end to which they are subservient" (Mill, 2001, 6). Mill suggests that rather than actions, we should focus on which rules will promote the highest degree of happiness for those who fall subject to them.

How might we apply these variations of utilitarianism to the Patriot Act considering that though it was ostensibly put in place to protect all Americans from the threat of terrorist infiltration and attack, it also necessitates the unwarranted audio and digital surveillance of all American citizens? The Patriot Act operates as a piece of legislation that involves specific circumstances and persons. By its own language, we are led to believe that the intended targets of surveillance are those suspected to be involved with terrorist organizations and capable of committing acts of terrorism upon innocent civilians. However, as has been shown, the focus is not centralized in this manner. *All* Americans must be monitored in order to weed out those that might pose a threat. As a matter of policy, it is a matter of rule. The NSA has made the implicit claim that *as a rule*, it should retain the ability to monitor everyone in search of radical terrorists. Framed this way, I am inclined to think that what we are dealing with is rule utilitarianism, at least *prima facie*. The aim of the Patriot Act may very well be to protect the lives of the American people, but I argue that it carries with it the consequence of innocent Americans being monitored in a way that limits their autonomy. It denies the right to privacy of those it is supposed to protect.

Whether viewed as action or rule, one could argue that the consequences of the Patriot Act do promote the greatest degree of happiness or pleasure—or in this case, security—for the majority of those impacted. An advocate of this variety could take the stance that if her autonomy must be limited by monitoring her phone calls and internet traffic in order to gain protection from terrorist threat, so be it. Besides, she has nothing to hide, right? For this particular user, the ends justify the means.

In support of utilitarianism, Peter Singer offers a formulation that attempts to ameliorate both of the accounts previously mentioned. He suggests that when making any ethical decision, we must take ourselves out of the picture. We must consider it as applying to everyone collectively and, in so doing, we must never allow our specific individual desires to influence or intrude upon this process. "In accepting that ethical judgments must be made from a universal point of view, I am accepting that my own interests cannot, simply because they are my interests, count more than the interests of anyone else" [Singer 1979, 12]. Singer argues that whether we are looking at acts or rules, we must consider the consequences for those impacted *above and beyond* our motivation for their creation. Let us look at the issue from this perspective and see what comes about.

One could clearly speculate ulterior motives, but for the moment, I will grant that the singular motive behind the creation and implementation of the Patriot Act was to identify terrorist threats via telephonic and internet surveillance. Those involved in the creation and execution of the Patriot Act—the NSA and the U.S. federal government—enjoy the benefit not only of having unfettered access to all Americans' tele/data communications and patterns of online conduct, but they also have the benefit of referring back to any specific data of their choosing as all that is monitored is stored. This is an actual consequence of the actions allowed by the Patriot Act. With this in mind, recall that the aim of the Patriot Act is to identify terrorist threats, and the method is mass surveillance of all persons in this country. The employment of this process certainly makes possible the identification of terrorists, for if you are watching everyone all the time, the chances that you will be able to locate the bad apples are good. Speaking literally, this is how bad apples are found. From this, we can correctly surmise that dragnet governmental surveillance can amount to the possibility of identifying terrorist threats, but what can we say of *actual* discovery?

On June 18, 2013, NSA Director General Keith Alexander testified before the U.S. House Select Intelligence Committee that governmental surveillance programs authorized by the Patriot Act "had helped prevent 'potential terrorist events over 50 times since 9/11'" (Nakashima, 2013). Though by their very description, these events were characterized as being merely potential, their identification did, in fact, seem to be actual. On October 16, 2013, it was reported that Alexander would be stepping down as NSA Director. This likely came in the wake of Snowden's exposing the agency's indiscriminate sweeping surveillance of American's telephone and internet data. It is also likely that Alexander's resignation came as a result of his admission that the actual number of potential terrorist events was an over exaggeration (Live Leak, 2020). Though the number of terrorist threats identified via governmental surveillance programs turned out to be lower than Alexander's original declaration, we could grant that at least some degree of terrorist threat was actually identified. In making an argument for utility, however, we must consider the *entire* scope of consequence.

Besides the consequence of identifying terrorist threats, I have demonstrated another that comes in the form of widespread and indiscriminate surveillance of American's telephone calls and their conduct online. Returning to the question concerning utilitarianism posed earlier, let us not think in terms of pain or pleasure, but rather in those of security and risk. I argue that ubiquitous governmental surveillance authorized by the Patriot Act does not follow an act model of utilitarianism. This is because the act does not promote a higher degree of security than is justified to eliminate risk of terrorist attack. We could imagine such adherence only if it were the case that once identified as a terrorist threat—by having compelling reasons to

believe so—surveillance was then implemented to gain further intelligence. Only surveillance of *known* terrorist threats would meet the necessary conditions of act utilitarianism. The individual act of surveillance would be permissible because the ends would justify the means.

Can we then say that governmental surveillance meets the conditions necessary to conform to the precedent of rule utilitarianism? Well, considering that the overarching and indiscriminate surveillance taking place as I type these very words does operate as a rule, we might be inclined to think so. But when we consider that all Americans—innocent or otherwise—as well as possible terrorist organizations are targeted, the methodology attracts more intuitive scrutiny. Surveillance on a scale this massive creates a situation in which the entire civilian population enjoys a disproportionately lower level of benefit than is promised by the means. Therefore, it is not clear that governmental surveillance can be justified under a rule model of utilitarianism. It is not clear that the level of security promised justifies the degree of privacy relinquishment required to fulfill it.

Finally, consider that the monitoring of private affairs and especially the retention of collected data involves the unabashed denial of Americans' 4th Amendment right to be secure in their persons, houses, papers, and effects. Governmental monitoring, collection, and storage of telephone call transcriptions and internet traffic equates simply to illegal search and seizure of one's intellectual property. Considering this, it seems that even outside the scope of utilitarianism governmental surveillance entails a legitimate violation of rights that are supposed to be guaranteed by those laid out in the U.S. constitution. Whether it is viewed under a consequentialist lens or simply considered using general ethical reasoning, I argue that surveillance of this nature is both unwarranted and unjustified.

I have also suggested that surveillance of this nature involves a loss of autonomy suffered by anyone who uses a telephone or computer, which turns out to be a vast majority of persons in this country. Again, we can presume the objection will be made that if one has nothing to hide, then surveillance of this kind is of no consequence and, therefore, poses no threat to one's autonomy. I will, however, ask this brand of objector to consider the way she conducts herself in private as opposed to in public. Before a date, many try on a number of outfits in private for the sole purpose of selecting the only one they want to be seen in by their partner in public. Those who tremble in fear at the mere idea of singing a song in front of an audience might do so emphatically in the shower alone. It is no secret that many people "pleasure themselves" sexually on a regular basis and feel there should be no stigma attached to such a practice as it serves as a healthy method of satisfying one's urges and relieves stress. Would such a person feel comfortable doing this in front of a group of NSA agents? I wager not.

The point here is that there are any number of strange and normal things we do in private *because* we are in private. An actual consequence of the Patriot Act is that one has to consider that she is being monitored as she researches birth control methods, seeks out divorce lawyers, and diagnoses strange rashes online. These intimate affairs are ones I am inclined to think that most would wish to remain private, but the Patriot Act removes the possibility for privacy in such conduct and in so doing disallows the possibility of one's retention of autonomy. In considering these autonomy limiting factors in conjunction with the utilitarian analysis provided above and the fact that this policy effectively authorizes unlawful search and seizure on a blindingly massive scale, I argue that the Patriot Act and its subsequent authorization of NSA spying on innocent civilians follows no principle of utility or morality whatsoever.

4. SURVEILLANCE AS A FORM OF CONTROL

For those who cherish our constitutionally guaranteed right to privacy, much of what I have said here is troubling. Of those who contend that NSA surveillance is unproblematic in that they "have nothing to hide," we might ask why they have blinds in their windows or doors on their bathrooms. We might ask if they are aware of the NSA's surveillance of pornography viewing habits, would they draw the same conclusion (Greenwald, Grim, Gallagher, 2017)? In deciding how to respond to the implications of NSA surveillance, I offer the words of philosopher Robert Paul Wolff as cited by Singer:

> "The defining mark of the state is authority, the right to rule. The primary obligation of man is autonomy, the refusal to be ruled. It would seem, then, that there can be no resolution of the conflict between the autonomy of the individual and the putative authority of the state. Insofar as a man fulfills his obligation to make himself the author of his decisions, he will resist the state's claim to have authority over him." (Singer, 1979, p. 293)

The point Wolff is making here is that inherently, the state and its people will always be at an impasse due simply to his declaration that the state demands authority and its citizens demand autonomy. What all of this really amounts to is *control*. Governmental surveillance is nothing more than the latest technological method to ensure that control of its citizens remain in the hand of the state. It is no secret that we civilians vastly outnumber the total amount of both police officers and military, yet government officials fear not any uprising or power shift of any kind. This is because shrewdly they have taken control by technological means to ensure that the teenagers will never throw a party because the parents will never leave town.

As far as the use of modern technology, however, I fear that the convictions expressed by Wolff have gone the way of the buffalo. In a society so infatuated with modern technology, its residents have become convinced—whether they know it or not—that unwavering adherence to the rules decreed by another are acceptable under any conditions, even when they remove the ability to live by those we might give ourselves.

As users of modern technology, we have voluntarily succumbed to the allure of modern digital existence. It is unlikely that many users would even consider the possibility of being what I referred to in the beginning of the paper as a mere citizen. There may be those rare few who refuse to participate, and to them I am more or less in accord. But for the masses—for that overwhelmingly disproportionate majority of persons who make the ritualistic use of modern technology requisite for their daily patterns of existence—there is no freedom from the bondage of corporate nor governmental surveillance.

REFERENCES

J. Bentham, Laurence J. Lafleur, *An Introduction to the Principles of Morals and Legislation*, Batoche Books, Kitchener, Ontario 2000.

A. J. Dellinger, *I Took a Job Listening to Your Siri Conversations*, *Daily Dot*, March 25, 2015; accessed May 28, 2020; https://www.dailydot.com/debug/siri-google-now-cortana-conversations/

B. Gellman, Blake A., Miller G., *Edward Snowden Comes Forward as Source of NSA Leaks*, The Washington Post, June 9, 2013; https://www.washingtonpost.com/politicsintelligence-leaders-push-back-on-leakers-media/2013/06/09/fff80160-d122-11e2-a73e-826d299ff459_story.html

L. Gomez, *Cameras on Nearly 3,000 Street Lights all over San Diego, Police Take Interest in Video*, The San Diego Union-Tribune, March 19, 2019; https://www.sandiegouniont ribune.com/opinion/the-conversation/sd-san-diego-street-light-sensors-camera-for-law-enforcement-use-20190319-htmlstory.html

G. Greenwald, Grim R., Gallagher R., *Top-Secret Document Reveals NSA Spied on Porn Habits as Part of Plan to Discredit 'Radicalizers'*, Huffington Post, Updated December 6, 2017; https://www.huffpost.com/entry/nsa-porn-muslims_n_4346128?13855 26024=

M. Heidegger, *The Question Concerning Technology and Other Essays*, William Lovitt (trans.), Harper Perennial, New York 2013, 17.

L. Leak, *Snoop Flies Coop: NSA Head to Quit After Lying, Failing to Explain Spy Overreach*, LiveLeak.com; accessed June 23, 2020; https://www.liveleak.com/view?i=2b8_1382134733

Mill, John Stewart. *Utilitarianism,* Batoche Books, Kitchener, Ontario 2001.

A. Roosendaal, *Facebook Tracks Everyone: Like This!* Tilburg Law School Legal Studies Research Paper Series, 3 (November), 2010, 1–10; https://papers.ssrn.com/sol3/papers. cfm?abstract_id=1717563

A. Rusbridger, Ewen MacAskill, *Edward Snowden Interview—The Edited Transcript*, *The Guardian*, July 18, 2014; https://www.theguardian.com/world/2014/jul/18/-sp-edward-snowden-nsa-whistleblower-interview-transcript

Ch. Savage, "N.S.A., *Triples Collection of Data from U.S. Phone Companies*, The New York Times, May 4, 2018; https://www.nytimes.com/2018/05/04/us/politics/nsa-surveillance-2017-annual-report.html

S. Schwartz, *9 Ways You're Being Spied on Every Day*, Huffington Post, updated December 6, 2017. https://www.huffpost.com/entry/government-surveillance_n_5084623? utm_campaign=share_email&ncid=other_email_063gt2jcad4

P. Singer, *Practical Ethics*, Cambridge University Press, Cambridge, England 1979.
A. Spencer, D. Roberts, *Obama Presents NSA Reforms with Plan to End Government Storage of Call Data*, The Guardian, January 17, 2014; https://www.theguardian.com/world/2014/jan/17/obama-nsa-reforms-end-storage-americans-call-data
U.S. Government Printing Office, *USA PATRIOT ACT*, accessed March 27, 2022; https://www.govinfo.gov/content/pkg/PLAW-107publ56/html/PLAW-107publ56.htm
S. Vaidhyanathan, *The Googlization of Everything: (and Why We Should Worry)*, University of California Press, Berkeley, 2011; http://ebookcentral.proquest.com/lib/ucsc/detail.action?docID=656365.
S. Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, Public Affairs, New York 2020.

ABOUT THE AUTHOR — Master of Arts, University of California, Santa Cruz, 1156 High Street, Santa Cruz, CA 95064, U.S.
Email: dugrayucsc@protonmail.com