University of Pisa
Department of Computer Science

The right to privacy

Mass surveillance in the digital age

June 27, 2022

Yohannis Kifle Telila
StudentID: 621821

Abstract

Since the beginning of democratic society, the right to privacy has been a pillar of a free and democratic society. Privacy was quite simple to safeguard centuries ago. If one wanted to do anything away from inquisitive eyes, it was done behind closed doors. It was easy to protect something from anyone. With the advent of digital technology, the definition of privacy has changed, and now it's not up to society to protect their information or privacy. In this work, I will be presenting a discussion on the importance of privacy and the constant surveillance of the government on citizens. Not only the government, but there is growing concern about how large corporations are exploiting user privacy, but I will not discuss this; instead, I will concentrate on the government side of the privacy issue. I will briefly discuss the two points, and I will assert my take on the importance of protecting the privacy of individual citizens and list out why it is so troublesome to allow the government to gain access and collect every little bit of data of its citizens. I then present the strategies that would help to fix these problems.

In this paper, I argue that the privacy of citizens should not be violated by any means and that the intrusion of government agencies into the private data or activities of citizens will not serve the public good. Furthermore, I will provide details on the importance of privacy and why the government should need alternative methods rather than collecting actions and activities of every citizen.

***Keywords**: Surveillance, Privacy, Technology*

1. Introduction

In recent years, federal government agencies have dramatically increased the quantity of personal data they gather from individual citizens through mass surveillance, including information about their political and religious beliefs, physical and mental health, and the identities of their family members and contacts. [4]. With the amendment of the act allowing the government to exert greater control over the lives of its citizens, technological advancements have raised the potential enormously for monitoring activities of citizens on the web [9]. The contemporary growth in large-scale government monitoring is often considered alarming, if not terrifying. Edward Snowden, a former national security agency(NSA) contractor, leaked data that shows that NSA was keeping and monitoring a huge amount of secret information about American people's phone calls, instant messaging, emails, documents stored in the cloud, contact lists, GPS data, etc. targeting everyone and anyone in the nation and community [8].

In addition to tracking information on other government officials, these surveillance techniques are also used to meddle in the affairs of other nations. However, I won't be discussing these in detail here. I will only focus on the surveillance of a government on its citizens.

At the same time, there remains arguments about the acceptability of surveillance in democratic societies. One of the main claims is security; to combat terrorism, violent crime, and foreign intervention, the government should have access to all of the instruments it requires [5][16]. I will be referring to [16] which basically argues that a state or a government is in principle morally permitted to place its citizens under constant surveillance. I challenge this claim and elaborate on the significance of each citizen's right to privacy and the denial of being watched without breaking the law.

This paper proceeds as follows: **Section 2** briefly addresses the main concerns and motives behind exploiting mass user data for surveillance. Next, **Section 3** provides an ethical analysis of surveillance and its impact on citizens of the nation. I will discuss more on the ethical side and the consequences of these acts. On the ethical side, more attention will be given to the moral and correctness of exploiting user data for the motives discussed in the previous section.

Finally, in **Section 4**, I will list out some of the main measures that could be taken to prevent the government's unnecessary mass surveillance without compromising national security.

2. Analysis of the problem.

The disclosure of questionable mass surveillance programs by intelligence and national security organizations in the government has sparked a global discussion over people's rights to be safeguarded from illegitimate or unwarranted private data collection and surveillance [13][12]. Some argue that, whether derived from individual rights to self-defense or via a social contract, a legitimate function of any government is to protect the rights of its citizens [11][16].

The author [11] contends that in times of national crisis, citizens are frequently asked to trade privacy for security. He further explains and argues that it is possible to promote both privacy and security by requiring judicial discretion when granting warrants, proving probable cause for an intrusion, and permitting public monitoring of the process and rationale involved. He pointed out two important reasons, national security and safety of citizens for the importance of putting security before privacy and suggested creating a balance between privacy and security.

2.1 National security

The government collects information in the name of national security to strengthen the protection of national security and protect institutions and markets from external invasion, plagues, and terrorism. This was the main focus of [11].

Glen Sulmasy [15] argued in an op-ed piece that in today's world, the government should be equipped with all of the latest technologies and methods of gathering information to ensure the nation's safety. He further explains that the threats from different terrorist organizations have put the country in need of using aggressive intelligence collection and effort.

He pointed out some of the incidents of terror attacks like the Boston marathon bombers[1] and the New York subway bombers[2] to strengthen his point of view on the importance of constant surveillance and monitoring of user communication. He argued that, as an open society, using technology to protect the constitution and the security of the nation is what the government should do considering the current global dynamics.
The paper published by Taylor, James Stacey [16] even goes further to argue that the government should monitor all of its citizens under constant surveillance at any time and any place, including what they are doing in their bedroom. The paper argues that the government is legally and morally permitted to place its citizens under constant surveillance. He pointed out two important arguments.

[1] https://en.wikipedia.org/wiki/Boston_Marathon_bombing
[2] https://en.wikipedia.org/wiki/2017_New_York_City_Subway_bombing

- It is morally acceptable for the government to keep track of historical occurrences.
- Importantly, he stated surveillance devices are ethically permissible for the government to utilize.

In his defence, Taylor argue that the government doesn't know what information is needed or will be important in the future. So, a system that is complete and able to record and store all the information possible should be permitted.

2.2 "Just Trust Us"—Trading Civil Rights for Security

Many contend that citizens shouldn't worry when the government gathers private activities and expands surveillance programs [3]. They argue that everyone should trust the government stating "If you have nothing to hide, you have nothing to worry about." "You should only be concerned if you're doing anything bad, and then you don't deserve to keep it secret"[9][5]. According to this reasoning, we should weigh the security advantages of recognizing and thwarting terrorist threats over privacy issues. People who claim that they are not important enough to warrant spying on or that, by doing so, the other party, or the government in this case, would receive no significant benefit because they are nobody. I will comeback to the ethical analysis of this argument on **section 3**.

Recent empirical research based on social surveys show a positive correlation between trust in public institutions and consent to government surveillance [7][14]. According to these findings, trust is a strong predictor of favorable sentiments about monitoring. As a result, trustworthy citizens consent to state surveillance, or, to put it more formally, trustworthy citizens give the government's legitimacy. Instead of hidden surveillance, these investigations primarily focus on open monitoring.

A common view is that we should assume the best about individuals in authority and that they won't violate individual rights without good reason. We should have faith in public officials because they often run for office to further the common good and are generally excellent individuals who want to do the right and fair thing. On this basis, people in positions of authority should decide how to strike a balance between privacy and security in light of the pertinent considerations. Government officials may utilize Internet packet-sniffers to look for suspicious content in chat rooms or private e-mail accounts where terrorists are using them to plot attacks.

3. Ethical analysis

At this point, it's reasonable to question whether it is morally and ethically correct to keep every individual under the radar. To begin with, let me counter the first argument pointed by [16] on section 2.1, I argue that monitoring every movement, action, and online activity 24/7 is ethically wrong and pointless. It is a good example of information overload, in which there is so much information that it's difficult to process and alert the authorities before something wrong happens. For instance, it's quite common to see security cameras on every street nowadays. Despite the fact that it's unlikely anybody would be viewing all these footage, this level of surveillance is logistically impossible and would be useless unless the intention was to dissuade crime by making criminals aware that their actions are theoretically being recorded.

Numerous instances show how this type of surveillance does not stop crime, as shown in these papers[10][2]. The conclusion of the study, [2] is that although preliminary studies in the US "suggest little to no beneficial

influence on crime," cameras in the UK had "no statistically significant impact" on crime. Furthermore, I am more certain that such a technology would eventually be exploited. In times of emergency or catastrophe, well-intentioned government officials have been and will continue to be tempted to disregard reasonable protections.

Coming to the second argument of [16] on section 2.1, I would like to draw the following scenario to explain why the government should not be allowed to use any surveillance technologies to silence anyone who is exercising their basic human rights. Let's consider, for instance, people who are protesting the onerous restrictions that the government has put in place that restrict access to free information and the media. The person is peaceful, nonviolent, and demonstrating in a large group in accordance with the law. However, the government disapproves of this and considers the demonstration a danger to their authority. They believe that demonstrations like these signify dissent and disturbance in society. Then the authorities give the police orders to locate everyone and apprehend them. In these cases, anyone who participated in the demonstration would face a prison sentence for doing what the government refers to as "unwanted conduct." No one now challenges the government because they are afraid that the government will be able to locate them on every corner of the city. Additionally, they worry about the potential consequences of even being connected to demonstrating.

I understand some might argue that "well, this might be true in an authoritarian government but not in a democratic society." my response to that would be that even governments that are called democratic misuse their power in the name of democracy[3]. Let me explain it better. If this perspective is founded on the conviction that the government is essentially ethical and does not (and will never) misuse unchecked authority over its population, I can understand the point of view. However, there are enough historical evidences that exists to show that governments would abuse their unchecked power in a way that endangers our democratic way of life.

3.1 "Nothing to hide..."

I argue that the claim "If you have nothing to hide, then you have nothing to worry about." is a false dichotomy. It offers a misleading choice: you either have a reason to hide your privacy because you did something illegal, or you don't have a reason to hide anything since you didn't do anything wrong. Its foundation is the "false" idea that privacy exists only to hide wrongdoing, and thus eliminates the notion that someone can be completely innocent but still desire to hide their activities.

It's intriguing to think about how the "nothing to hide..." perspective seems in light of the Wikileaks campaign. If the situation were reversed, I highly doubt that any government would find such a viewpoint to be persuasive. If this is not convincing enough, I would like to leave them with a question: why would governments be outraged by leaks if they have nothing to hide?.

Moreover, we all legitimately hide certain sensitive personal information from others, not because it suggests criminal conduct but rather because others shouldn't have access to it. Think about a person's sexual or medical background. Imagine someone going online or to a library to study unconventional, socially unaccepted lifestyles. Think about being watched as you discuss political and social topics by reading, thinking, and

[3] https://www.aclu.org/other/top-ten-abuses-power-911

conversing(chatting, emailing) with others. Such intellectual monitoring is particularly dangerous because it can deter individuals from experimenting with unorthodox, divisive, or different ideas, which completely violate the values of democratic society.

The negative effects of the surveillance society are numerous, some of which are severe, and maybe irreversible [1]. If people feel like they are being watched and their movements are being recorded at any given moment, people will start to behave accordingly to this expectation. This could account for manipulating people's behavior and intimidating them which is effectively psychological abuse. People will question their every action. It makes no difference if you have something to hide. It matters that your psychology and behavior are being controlled.

I argue that any discussion of surveillance in public should take into account how it affects people's rights to privacy, ethics, and human rights; how it affects social inclusion and exclusion; how levels of choice, power, and empowerment change; whether those in charge of such systems will ever be held accountable; and whether or not surveillance procedures are transparent.

4. Discussing strategies.

The issue is not the privacy issue at its core. The key concern is how we interpret the purposes of state surveillance and what is required and appropriate to accomplish these purposes. This entails, among other things, debating the nature of the threat that terrorism genuinely poses to national security and the existence of a fundamental difference between regular citizens and actual people that are threat to the national security. Although the answers to these questions will establish the scope of privacy protection, they are not privacy-related.

I will propose three strategies to what we could do to prevent the government from collecting citizens data, thus violating privacy and suggest what the government should instead focus.

4.1 Stronger Constitutional privacy rights

Despite the fact that we have laws that protect citizens from unreasonable searches and seizures without a warrant, secret government initiatives cannot be challenged until they are discovered by whistle-blowers. The current surveillance and privacy law provides only the bare minimum of safeguards. The idea that simple monitoring causes no damage is commonly used by courts to reject challenges to these programs for lack of standing.

The role of law in the regulation of state surveillance and the possibility of developing regulatory structures that ensure check and balance between government bodies can effectively protect individuals from unnecessary surveillance. Clearly, the law has a central role to play in defining the limits of individual privacy and in setting the standards that both private and public sector actors must meet when they engage in any form of surveillance.

The GDPR was promoted as the industry benchmark for data protection, providing the most robust data rights available. We now have the right, thanks to the GDPR, to request any data that is kept on us to be deleted. Again, this places the responsibility for doing the task on us, not on the big companies or the

government. However, the GDPR could have simply addressed this by making privacy the default setting and requiring our consent if we wanted our data to be gathered, thereby limiting how much data governments or companies could collect about us, predict our behavior, and exert control over us. The GDPR is not preventing the development of a surveillance society; in fact, it may potentially make it legal.

I strongly believe that as a democratic society we need constitutional legislation that addresses the collection of data, not only the protection of data after the data has already been collected without the consent of the people. Any form of surveillance is against human rights. Only in very specific circumstances that are intended to stop the most heinous crimes do we permit lawful monitoring. Regardless of who does it, spying on peaceful citizens and protesters, journalists, judges, or political opponents should be prohibited by law.

4.2 Building trust between society and gov't

Trust is arguably very important when it comes to surveillance, but the connection between trust and surveillance is more nuanced than it appears. Trust is about responding to society favorably with benign expectations. whereas surveillance is driven by a lack of such confidence. In general, surveillance is a very invasive activity that, among other things, affects people's privacy and undermines their sense of confidence. On the other hand, in democratic regimes, trust is essential for effective state monitoring. People will be hesitant to grant the state a mandate to watch them if they don't trust the government.

The legitimacy of democratic institutions rests on the basis of trust. Many governmental initiatives depend on the public's behavioral responses. Therefore, trust is essential to their success. However, as I mentioned earlier, surveillance erodes trust. Governments must work to restore public confidence in their institutions. Some of the actions the government could take to build trust in society include building transparency(sharing information and communicating with the public); valuing and respecting everyone regardless of background, identity, and belief.

I believe we can all agree that the trillions spent on "preventing terrorist plots" represents a very poor value in terms of lives saved relative to the amount of money spent. If the only purpose of spending trillions on surveillance was to save lives and safeguard the lives of the populace, then how many fatalities could have been avoided with only a fraction of that amount of money had it been used for things like food banks, homeless shelters, mental health care, and research into illnesses that kill a lot of people every year instead of investing in mass surveillance, which is not effective in preventing attacks.

The core causes of violence are frequently sustained by institutional injustices. Policies, social structures, and norms imposed by the institutions in power that hinder people living in impacted communities from having equal access to opportunity. Developing and supporting programs that promote structural equality between communities in raising healthy children, the opportunity to have equal healthcare and an education system are the first steps in violence prevention.

4.3 Alternatives for keeping people safe

Studies have shown how mass surveillance is ineffective in preventing domestic attacks [6]. Instead, focusing on targeted surveillance of people known to be connected to terrorism is the best way to find terrorists.

However, it is critical to distinguish between "targeted surveillance," which should be based on whether the targeted person or organization has a prior existence of evidence that places them under suspicion. Intelligence agencies need more resources to better investigate the evidence that they already have and more effectively discharge their responsibilities.

Any threat must be fully understood in order to be properly addressed. The analysis and in-depth research on domestic terrorist threats or violence prevention should be expanded and improved by the federal government. This work is crucial given the current, diversified, and dynamic domestic terrorist threat. Like I mentioned previously, collecting huge amounts of data wouldn't have any value in protecting against danger. Carrying out this type of research that promotes violence reduction strategies would rather help track, assess, and develop violence prevention strategies.

Conclusion

In this paper, I have discussed the importance of individual privacy over mass and extended surveillance by the government. In the ethical analysis, I stated that these mass surveillance programs are ineffective and put the citizens under the fear of their own elected government.

The government shouldn't have the power to spy on and force its citizens to obey its will. The government should focus on building trust between citizens and should give regular information on how the citizens participate in keeping national security so they do not need to be spied on[4].

We need to safeguard individual privacy and freedom to express themselves by introducing regulations and strong checks and balances that prevent the government from gaining unwarranted access to the private data of citizens.

Finally, I would like to say that terrorizing our own citizens is far more dangerous and achieves the overriding fear and societal breakdown that terrorists seek to accomplish themselves. We do not need to bring the hand of government into each and every one of our pockets and handbags. We do not need to disrupt our current way of life. We do not need to create a society that is emotionally manipulated and docile. No one will be safer through further constant and extreme government surveillance. Building trust between society and the government is the ultimate solution to building a better and safer society.

[4] This is a good example of transparent government.

Bibliography

[1] Louise Amoore et al. “A Report on the Surveillance Society”. In: (Jan. 2006).

[2] Noam Biale. “Expert Findings on Surveillance Cameras: What Criminologists and Others Studying Cameras Have Found.” In: (Jan. 2008).

[3] Fredrika Björklund and Ola Svenonius. “Legitimising Surveillance in Low-Trust Postcommunist Societies”. In: *Europe-Asia Studies* 0.0 (2022), pp. 1–26.

[4] Kees Boersma et al. *Histories of State Surveillance in Europe and Beyond*. May 2014. ISBN: 978-0-415-82946-5. DOI: 10.4324/9780203366134.

[5] Michelle Cayford and Wolter Pieters. “The effectiveness of surveillance technology: What intelligence officials are saying”. In: *The Information Society* 34.2 (2018), pp. 88–103. DOI: 10.1080/01972243.2017.1414721. eprint: https://doi.org/10.1080/01972243.2017.1414721. URL: https://doi.org/10.1080/01972243.2017.1414721.

[6] Jennifer Stisa Granick. *Mass spying isn't just intrusive—it's ineffective*. Mar. 2017. URL: https://www.wired.com/2017/03/mass-spying-isnt-just-intrusive-ineffective/.

[7] *How Americans have viewed government surveillance and privacy since Snowden leaks*. https://www.pewresearch.org/fact-tank/2018/06/04/how-americans-have-viewed-government-surveillance-and-privacy-since-snowden-leaks/. Accessed: 2022-06-23.

[8] Leon R Kass et al. *Government secretes: The public's misconception of the Snowden's disclosures*. 2004.

[9] Peter Königs. “Government Surveillance, Privacy, and Legitimacy”. In: *Philosophy Technology* 35 (Mar. 2022). DOI: 10.1007/s13347-022-00503-9.

[10] Gill Martin et al. “The impact of CCTV: fourteen case studies”. In: (Jan. 2005).

[11] Adam Moore. “Privacy, Security, and Government Surveillance: Wikileaks and the New Accountability”. In: *Public Affairs Quarterly* 25 (Apr. 2011).

[12] Bryce Newell. “Mass Surveillance, Privacy, and Freedom: A Case for Public Access to Information About Mass Government Surveillance Programs”. In: Dec. 2015. ISBN: 9781783484768.

[13] P. Perri. “The mass surveillance and the human rights' defense under the European convention of human rights”. In: *Notizie di Politeia* 33 (Jan. 2017), pp. 92–100.

[14] Elvira Santiago Gómez, Sara Degli-Esposti, and Vincenzo Pavone. *Key Factors affecting public acceptance and acceptability of SOSTs*. Jan. 2014.

[15] Glenn Sulmasy. *Opinion: Why we need government surveillance*. June 2013. URL: https://edition.cnn.com/2013/06/10/opinion/sulmasy-nsa-snowden/index.html.

[16] James Stacey Taylor. “In Praise of Big Brother: Why We Should Learn to Stop Worrying and Love Government Surveillance”. In: *Public Affairs Quarterly* 19.3 (2005), pp. 227–246. ISSN: 08870373. URL: http://www.jstor.org/stable/40441413 (visited on 06/20/2022).