The Scale of Modern Surveillance

and it’s Impact on Human Behavior

Atticus Emilsson

Interdisciplinary Theories and Concepts

IDS300W

Mar 03, 2025

Introduction

The human race and it's affinity towards progress has potentiated corporate greed and sowed distrust between governing bodies and their constituents (albeit unexpectedly). Among this progress lies technological advancements which perpetuate the in-place powers and rules of society. It is virtually impossible to sufficiently interface with modern technology and contemporary society without sacrificing one's privacy to some extent. Public roadways, residential homes, and shared properties are littered with security cameras, license plate readers, facial recognition tools, and other surveillance equipment. Digital services and applications monitor your activity to derive valuable data for advertising such as your browsing history, precise location patterns, relationships and acquaintances, and consumerist interests. Social media platforms are an inherent threat to privacy on a sociological basis, where sharing personal information and details has become the norm. No matter where one goes or what one does, a disconcertingly large majority of the population is under constant surveillance. Not only is this unsettling by nature of principle, but it also manipulates the manner in which constituents think and act. This is of course, advantageous to corporations and governments, where surveillance acts as a deterrence against bad actors; however, when does the deterrence end if surveillance exists virtually everywhere? To what extent does this deterrence influence how we operate in society, and does it stop when we are alone? These are the concerns that this research presents.

An Interdisciplinary Approach

The questions presented are very complex and controversial in nature. There have been one-off attempts to address instances like these; however, none of these endeavors amount to much. The technological advancement has skyrocketed at rates never before seen. Humans have not yet had enough time to adjust to the changing reality, an Orwellian one. The complexity of these issues demands insight from multiple disciplines, considering these technologies integrate with so many different facets of modern industry and society. It is incredibly important that one integrates insight from the corresponding disciplines in order to develop a more effective and refined product/solution. Failure to incorporate such insight would result in the deployment of a flawed solution, doing more harm than good.

Identified Disciplines

In the context of modern mass-surveillance, there are plenty of disciplines that could provide unique and valuable insights. Politicians hold the direct power, overseeing the laws and legislation that goes into effect. Policy analysis would provide valuable information pertaining to why these concerns often find themselves in limbo, without answer. This also applies to lawyers and attorneys, who have had first-hand experience with cases of this nature. Economists can also provide insight when developing policies, exploring solutions that also align with the for-profit landscape of the United States. Anthropology will also help in determining how human behavior contributes to the issues at hand. These are the primary disciplines that will be drawn on in the context of this interdisciplinary research. As aforementioned, failure to integrate such insight would be counter-intuitive considering the highly complex nature of the proposed issue. History has shown that flawed and rushed deployments of policy oftentimes either has no impact, strengthens the situation, or creates an entirely new situation. A rushed solution in this context would be a disservice, hence the call for integrating the Interdisciplinary Research Process (IRP).

The Scale of Surveillance

The concept of surveillance is not a new word, and has persisted as a concept for “more than two hundred years;" however, the scale at which surveillance technology has been advancing is simply too fast (Lyon, 2022). Older definitions and policies were likely effective for their corresponding time period, with the scale of surveillance equipment being much more *manageable*. This may have included cameras around banks, gas stations, and ATMs; conversely, surveillance equipment is virtually everywhere. Newer surveillance technologies are much harder to identify, and even more difficult to combat. With the advancement of consumer electronics, the space quickly caught wind of increased demand for surveillance. This spawned much innovation within the *Home Security* industry, where cost-effective, cloud-based solutions are now implemented at every door and under every eave. The dense deployment radius’ of these smart-home security systems creates a sort of mesh of surveillance equipment. Everywhere one publicly interfaces with urban/sub-urban society, will undoubtedly fall under some form of surveillance.

The Evolution of Surveillance

Surveillance is no longer limited to the confines of the physical world, where virtually every activity performed on the internet is being tracked. Your Google searches are being sold, your consumer interests are being tracked as you interact with social media, connections are made between you and others for identifying relationships and acquaintances. Much of this data is also willingly forfeited when interacting with social media. Not only do social media platforms invisibly track virtually everything you do in the context of the application, but individuals also willingly share intimate information to the public. Phones precise location history and habits, some devices extract voice data and use it for AI-training, and some devices collect your facial features for facial recognition purposes. The common phone now also serves as an incredibly high definition camera, meaning it is likely that you can be identified in photos being taken by other people. With the exponential progression of surveillance technologies and the incredibly concentrated integration we have with technology, it is virtually impossible to navigate society without forfeiting any personal information.

The Influence of Surveillance

It is inarguable that individuals are influenced by conventional, physical security controls and surveillance equipment; however, the more abstract surveillance being performed by big data is just as effective. One might not have concern regarding the collection and processing of their data, or may not understand the scale of the information collected. For example, the Facebook Privacy Policy defines four categories of private information that they collect: “Your activity and information that you provide,” “Friends, followers and other connections,” “App, browser, and device information,” and “Information from partners, vendors and other third parties” (Facebook, 2022). The first category lists multiple types of data collected, some of which are more directly concerning such as “messages that you send and receive, including their content” (Facebook, 2022).

Persisting Surveillance and Influence

The vast amount of data processed can be represented as the “digitization of the streams of our thoughts and actions,” resulting in an even more pervasive manner of influence and deterrence (Marthews & Tucker, 2018) This scale of mass surveillance not only deters potential bad-actors from participating in objectionable actions, but it also may influence the manner in which people think.

These mass datasets of personal information and behaviors is not only used for advertising, but also for curating content. These curation algorithms can be leveraged maliciously to skew what types of media one consumes. For example, one can observe how social media campaigns were able to successfully manipulate public opinion through the spread of misinformation/disinformation (University of Oxford, 2021). It was also discovered that more than 93% of 81 countries surveyed had deployed disinformation as “part of political communication” (University of Oxford, 2021). This effectively presents the manipulation capabilities and how they can be applied to certain populations at rates which fall under the Just Noticeable Difference (JND) threshold. These campaigns can be tailored to any need considering the scale and concerning accuracy of the datasets held by *Big Tech.* Alex Marthews and Catherine E. Tucker describe this manipulation of online behavior (as a result of mass surveillance) as “chilling” (Marthews & Tucker, 2018).

The incredibly complex landscape of this issue is further compounded by the political and ethical implications of certain, privacy-respecting solutions. For instance, another highly controversial topic, encryption is a privacy-enhancing tool that is used in all reaches of the internet. It is primarily used as a security measure to ensure user and operator information is kept secret from malicious actors listening in on traffic. Encryption is also used to send messages securely, ensuring that only the sender and recipient can view the message, and nobody in between. Many law enforcement agencies around the world have expressed concern about this. Due to the secure nature of these conversations, it is possible that criminals might resort to using them in attempt to evade law enforcement agencies. Since it is incredibly resource intensive to crack messages of this nature, LE agencies have started pushing for the implementation of “back doors” or “master keys” in secure encryption algorithms (Eoyang & Garcia, 2020). Unfortunately, the introduction of a “back door” would inherently weaken the overall security of the encryption algorithms, and introduce a potential vector for attack. These measures, with the goal of increased surveillance capabilities, would further “undermine national security” and should not be considered as viable alternatives (Eoyang & Garcia, 2020). This further highlights the complex nature of the policies and legal frameworks surrounding surveillance, and the constant push for more.

An absolute block on tracking is most certainly not a viable approach from an economic perspective for many reasons. The first of such is that advertising generates revenue for a company that is providing a service. This means that removing tracking/data collection would completely eliminate one source of revenue for said organization. It would also hamper the economy, as many companies rely on targeted advertising to actually gain business. Advertising has allowed for individuals to grow businesses and flourish. It has also enabled the kickstart of an entirely new industry, content creation. It allows creators of content to generate revenue on work that does not receive payment in a conventional manner (Miller, 2010). It also generates a colossal mount of earnings for the respective corporations, with Google making “more than 90 percents of its revenue from text search ads” and Youtube generating $450 million in revenue (2009-2010) (Miller, 2010). The impacts to the economy would be scale-able, and requires collaboration between disciplines. It will take lots of work and collaboration between all applicable disciplines to develop a solution that effectively addresses and resolves the issues at hand.

The issues were identified and analyzed through an interdisciplinary approach that highlights various concerns which impede timely and effective implementations that address the privacy concerns shared by the people. This research aims to clarify the problem with a mono-disciplinary approach to privacy concerns, and identify the boundaries at which the disciplines clash. We can observe historic instances of mass data collection, processing, and analytics used in a malicious manner. For example, the instance of Cambridge Analytica where data was maliciously used with the purpose of manipulating voter opinion. As dystopian of a concept it may sound, this reality is much closer than one might think.

References

Eoyang, M., & Garcia, M. (2020, September 9). Weakened Encryption: The Threat to America's National Security – Third Way. Www.thirdway.org. https://www.thirdway.org/report/weakened-encryption-the-threat-to-americas-national-security

Facebook. (2022, July 26). Meta Privacy Policy - How Meta collects and uses user data. Www.facebook.com. https://www.facebook.com/privacy/policy

Lyon, D. (2022). Surveillance. Internet Policy Review, 11(4). https://policyreview.info/concepts/surveillance

Marthews, A., & Tucker, C. (2017). The Impact of Online Surveillance on Behavior. 437–454. https://doi.org/10.1017/9781316481127.019

Miller, C. (2010). YouTube Ads Turn Videos Into Revenue. https://www.andrew.cmu.edu/user/lshea/Interesting_Articles/YouTube_Copyright.pdf

University of Oxford. (2021, January 13). Social media manipulation by political actors an industrial scale problem - Oxford report | University of Oxford. Www.ox.ac.uk; University of Oxford. https://www.ox.ac.uk/news/2021-01-13-social-media-manipulation-political-actors-industrial-scale-problem-oxford-report