Atticus Emilsson

SOC-205S (21079)

Data, Technology, Society

November 26, 2024

The Critical Growth of Mass Surveillance

Introduction

As time progresses, society migrates into a world where technology is prevalent in every facet of daily life, from advanced/modern warfare to the automatic brewing of coffee. These technological advancements can be found virtually everywhere due to their benefits towards quality of life, specifically convenience. These advancements are not just for the individual, but also organizations and industry. Critical service providers such as healthcare facilities, government buildings, and prisons/penitentiaries all employ modern technology to strengthen their workflows and enhance their services. Some of these critical technologies exist with one sole purpose, and that is to place constituents under surveillance. In Vita Peacock's entry, _Surveillance_, they define this act as "watching over through human and/or non-human technologies for an intended purpose," which could be the protection of assets (including both tangible and intangible), overseeing employee activity, and/or ensuring proper behavior within a correctional facility (2023). This progression into such a highly interconnected world comes with unprecedented consequences, blurring the lines between surveillance technologies and technologies not intended for surveillance.

With the incredibly fast progress regarding technological advancements, there have been pitfalls in development that have contributed to insecure technologies. These commonly insecure technologies are typically embedded systems and/or smart systems that have a single purpose, as opposed to a computer or other desktop system which typically serve multiple purposes. These systems are referred to as IoT (Internet of Things) devices. Their incredibly rapid development and advancement have led to a vast oversight of security assessments and implementations, as they "do not usually support strong security mechanisms" that one can observe in non-IoT devices (Meneghello, 2019). When such insecure systems are networked, a door is opened for

adversaries to take advantage of. Consumer security cameras and surveillance equipment are also oftentimes considered IoT devices.

The implementation and integration of insecure security equipment alongside officially deployed surveillance equipment introduces unprecedented opportunities for mass surveillance. Insecure surveillance equipment can also pose a threat to individual privacy being taken advantage of by non-governing/non-enforcing bodies such as predators and nation-state actors. This research paper will analyze the different threats of digital surveillance and its ever-growing prevalence, how it may impact privacy and social behavior, and how it may reinforce existing power structures.

Increased Surveillance Presence

Previously, surveillance relied solely on the physical presence of cameras installed by an institution, building manager, or other individual with authorization and funding to implement such equipment; however, the rise of IoT devices and consumer security equipment has lowered the bar for entry. Further technological advancement has also enhanced existing surveillance technologies and led to the development of more accurate and invasive observation.

Older implementations of security cameras and other audio/visual recording devices were intended to minimize drive utilization whilst being able to store a plethora of data. These factors, coupled with the simple, infantile capabilities of recording equipment led to poor-quality video that was not sufficient for prosecution and other legitimate purposes. As time progressed, the quality of the recordings increased, and drive capacity and compression algorithm efficiency skyrocketed. These advancements are further compounded by "cutting-edge applications of

artificial intelligence and big data for surveillance purposes," granting new surveillance equipment with facial recognition capabilities (Mobilio, 2023).

With the growth in the development of IoT devices, a new market has also been introduced which entails the introduction of consumer surveillance equipment. These devices are network-enabled, incredibly cheap, and allow consumers to integrate cameras, motion detectors, and other "smart" surveillance equipment for relatively cheap. One incredibly common implementation is the Ring doorbell camera, which can be observed by the door of many businesses, homes, apartments, and other dwellings. Although these implementations may be cheap, they do further contribute to a competitive surveillance market. This leads to the enhancement of capabilities, cost, and stealth in enterprise-grade surveillance equipment.

Prior to these advancements, cameras were oftentimes only observed in critical or high-value areas such as banks and penitentiaries; whereas now, both consumer and professional surveillance equipment is present everywhere. Not all surveillance, however, revolves around the direct recording of audio and visuals. Surveillance can also include internet browsing behaviors, social media usage and interactions, location history, and any other network traffic. These activities can be actively transmitted by the IoT devices or maliciously extracted from the device/traffic by an adversary. IoT devices may also capture and transmit other non-network related activities such as "sleeping-patterns, exercise routines, child behaviors, medical information, and sexual activity" (Apthorpe, 2017). Just because a device does not have a lens does not mean that said device is not actively participating in surveillance.

Potential for abuse and other implications

Although security equipment can certainly present benefits to one's own safety and well-being, there are security concerns that must be considered. As mentioned, many IoT security devices are insecure with various vulnerabilities. Putting this aside, however, the constitutional nature of this networked equipment introduces an avenue for the illicit surveillance and/or spying of an individual. Networked security cameras require a method for a legitimate, authorized user to access and review recorded content. Similar to many web logins, this typically consists of a username/email and password. In many cases, "many cameras use default passwords" which gives a user the opportunity to set the password to their liking (Herodotou, 2023). Unfortunately, users oftentimes do not change the default password which grants attackers easy access to security systems. In the case that a user does change the default password, they are also oftentimes not sufficiently strong/complex for today's standards. It is possible to "perform an online brute-force attack to uncover the camera's password," where less complex passwords are discovered much quicker compared to more complex passwords (Herodotou, 2023).

The ability of a malicious individual to remotely access security equipment introduces a vast array of threats. One such threat is disabling/manipulating said equipment to allow for an individual to physically enter the premises undetected. A threat more akin to the subject at hand, however, is the ability for an individual to leverage preexisting equipment to remotely spy on activities that occur on premises. These capabilities allow anyone, whether it be a stalker, a government agency, or a nation-state actor, to participate in surveillance in an individual's home with ease.

Impacts on Social Behavior

With the advent of big technology has come a new industry, and that is the collection, processing, and marketing of personal information. Oftentimes referred to as "big data," organizations collect information relating to individual activities. These activities are similar to those previously described by Francesca Meneghello, including networked activities such as internet history and shopping habits, as well as "offline" activities such as sleeping behaviors and sexual activities (2019). This data is typically intended to be used for targeted advertising, product development, and the enhancement of user experiences. Unfortunately, this data is also used to enhance surveillance activities. As previously mentioned, surveillance equipment now includes capabilities such as facial recognition. Extracting facial features and referencing this information with the datasets presented by big tech enables incredibly invasive surveillance capabilities such as individual identification, tracking eye movements, and even analyzing the probability that an individual may commit a crime. These capabilities coupled with the massive development and integration of surveillance equipment around the globe lead to what has been described as mass surveillance.

Mass surveillance describes the government's act of "spying on the entire population or a significant component of it," which is further exacerbated by the integration of cheap security equipment on many premises (Siniša, 2024). This is certainly a cause for political and ethical concern, due to the invasive nature of constant surveillance. Although there are more "direct" intents of surveillance such as protecting high-value assets like a bank, many of its results are less so. Vita Peacock describes this premise, where "surveillance is often intended to produce effects on the affective and mental life of the surveilled" (2023). In the setting of a bank, for example, this may deter criminals from attempting to participate in a heist or other related crime; however, the presence of mass surveillance has introduced a "self-regulated conformity to established rules" which may pose a threat to individual freedoms and result in the reinforcement

of existing power structures (Peacock, 2023). A notable term introduced by Michel Foucault is the Panopticon, "a series of architectural designs by English reformer Jeremy Bentham for controlling the behaviour of their occupants through the suggestion that they were being observed," which is now colloquially used in reference to the population under mass surveillance (Peacock, 2023). Due to the previously mentioned prevalence of surveillance equipment and other equipment capable of indirect surveillance, uncertainty has been introduced to the population where one may not know if they are being observed (Peacock, 2023). This forces individuals into a state of self-regulated conformity, even in their own homes. This induces fear and impedes an individual's ability to operate authentically, even if within the bounds of the law.

Conclusion

It is inevitable that as time progresses, society will further integrate itself with technology. This will further exacerbate the issue of mass digital surveillance, especially with the observed failures to pass legislation on technology and its interaction with the populous in a timely and sufficient manner. With these increases in inter-connectivity and surveillance, it is of critical importance to address the political and societal implications of mass surveillance. Failure to properly address this issue will certainly contribute to the reinforcement of existing power structures and will force constituents further into the state of self-regulated conformity.

Works Cited

Apthorpe, Noah, Dillon Reisman, Srikanth Sundaresan, Arvind Narayanan and Nick Feamster. 2017. “Spying on the Smart Home: Privacy Attacks and Defenses on Encrypted IoT Traffic.” arXiv. https://doi.org/10.48550/arXiv.1708.05044

Herodotou, Samuel and Feng Hao. 2023. “Spying on the Spy: Security Analysis of Hidden Cameras.” Network and System Security, vol. 13983: 345-62, doi:10.1007/978-3-031-39828-5_19.

Meneghello, Francesca, Matteo Calore, Daniel Zucchetto, Michele Polese and Andrea Zanella. 2019 "IoT: Internet of Threats? A Survey of Practical Security Vulnerabilities in Real IoT Devices," in *IEEE Internet of Things Journal*, vol. 6, no. 5: 8182-8201, doi: 10.1109/JIOT.2019.2935189.

Mobilio, G. 2023. “Your face is not new to me - Regulating the surveillance power of facial recognition technologies.” *Internet Policy Review*, 12(1). https://doi.org/10.14763/2023.1.1699

Peacock, Vita, Mikkel Kenni Bruun, Claire Elisabeth Dungey, and Matan Shapiro. 2023. “Surveillance”. *The Open Encyclopedia of Anthropology*. http://doi.org/10.29164/23surveillance

Siniša, Domazet, Marković Darko M. and Skakavac Tatjana. 2024. “Privacy under threat: The intersection of IoT and mass surveillance.” *Pravo - teorija i praksa*, *41*(3): 109-124. https://doi.org/10.5937/ptp2403109D