Undergraduate Research Journal

Issue 18, Volume 2 May 2026

Beneath The Watchful Eyes

Sofia Solorio

In the 1970s, French philosopher Michael Foucault brought the design of a hypothetical prison into the public eye. This prison, first conceived by Jeremy Bentham, was circular in shape, the cells facing a central guard tower capable of observing any of them at any time. The guards could not watch every prisoner at once, but the possibility that they *could* be observed at any time was meant to deter them from misbehaving. It was called the panopticon. Foucault used the panopticon as a metaphor, reasoning that in modern society, the threat of surveillance had replaced corporal punishments. He argued that society's need for discipline had long since outpaced its technological advancement, and when it became possible to observe in all places;school, work, hospitals, surveillance emerged as a new sort of punishment.

Foucault's theory of punishment and surveillance is more relevant than ever in the age of technological advancement in electronic surveillance. Technology, of course, is defined as inventions of the purpose to assist in a task-in this case, surveillance. The definition of surveillance is trickier to pin down but can be encapsulated as the observation of an individual's or group's activities. Surveillance has taken many forms over the course of its history; human operatives, listening devices (bugs), and more recently, observation over electronic devices such as mobile phones and computers. Surveillance is justified by its proponents for a variety of reasons; preventing terrorism, ensuring national security, tracking down criminals, etc. With the increase of the ease of surveillance, it would be easy to assume that society has advanced from previous states of law enforcement and benefitted accordingly.

However, the advancements made in electronic surveillance technology have in fact caused society to regress. Society has normalized and complied with the authority of surveillance technology, entirely at the mercy of those who watch.

In today's age, everyone is being watched by someone, though they rarely acknowledge it. Being on the internet in the first place requires one to parse through lengthy agreements to surrender personal data and agree to monitoring. Surveillance, active or passive, has become so completely standardized in the online world that there is simply no way to opt out. Lecturer at John F. Kennedy School of Government and cybersecurity professional, Bruce Schneier, in his chapter "How We Sold Our Souls–and More-To the Internet Giants", posits that electronic surveillance, including but not limited to that on the internet, has become increasingly normalized and harder to avoid. Increasing reliance on technology and the internet has made it nigh impossible to avoid subjecting oneself to surveillance, and as it currently stands, it's not feasible to simply forgo the technology. Those who are unaware of surveillance subject themselves to it, and the knowing have no real choice but to follow.

Though many are under the opinion that they are not actively being observed under suspicion, they would no doubt find it surprising how much personal data is stored and utilized by corporations and governments. The privacy of the average internet user is non-existent, thanks to electronic surveillance. Nearly every account on many sites are required to be registered under an email and legal name, and may also require a birthdate or location. Perhaps one may not have anything to hide. However, the data collected from unaware citizens may lead to misdrawn conclusions and unforeseen consequences for the

surveilled. Schneier emphasizes that surveillance data is accumulated tremendously, including location, search history, and biometric data, stressing that "corporations gather, store and analyse this data, often without our knowledge and typically without our consent", pointing out that the conclusions drawn from this data can have profound effects on people's lives (335). Information gathered without one's awareness or compliance could be used against them. Law enforcement may draw incorrect conclusions or be misled by someone's seemingly suspicious data, wasting investigation time and subjecting an innocent person to scrutiny, all based on surveillance data collected in ignorance. Being surveilled is no small matter-but as of now, there is no true option other than to comply.

As technology has blossomed into widespread use in society, so has electronic surveillance alongside it. Processing speed and capabilities of computers have led to them becoming a staple in not only schools and workplaces, but human lives in general. In the background of the daily emails, internet searches, and online purchases, third parties are quietly accumulating data from the unaware and using them for their own purposes. Author and military historian, Yuval Noah Harari, in his chapter "Big Data, Google, and the End of Free Will", contends that society has become over-reliant on algorithms to the point that authority is now shifting to Big Data systems. Electronic surveillance has embedded itself so firmly into society that it is able to disguise itself as a benefit while selling personal data collected from its users without their knowing consent. A positive response to recommendations given with the aid of surveillance reinforces the idea that surveillance is not only harmless, but even beneficial. People like the ease of use that comes with being watched; this great eye that knows them can draw from its immense pool of information to

show them what they would like-information, which, of course, comes from the surveillance of others.

The ouroboros of surveillance is ingrained into the internet experience to such an extent that it does not seem to be a cause for alarm or even notice. The expectation that data is collected for corporations to do as they choose is endured by nearly all. This only makes it more difficult to resist the gaze of the watchers; no one seems to take issue with it. En masse, society is placated by electronic surveillance's capabilities to regurgitate others' data back at it. Harari corroborates this notion, elaborating that, "dataists believe that given enough biometric data and computing power, this all-encompassing system could understand humans much better than [they] understand [themselves]" (342). In theory, many would object to being surveilled on a near constant basis, but those very same dissenters can be distracted by this enormous system of algorithms and eyes flattering them with recommendations made possible by their continued compliance. Users enjoy being told who they are, what they like or would like, who has similar tastes. When presented with their data, there is a tendency of the Watched to become drawn to their reflections. Like it or not, people have given this system a stamp of approval, long before they were endeared to it.

Society has made an unspoken agreement to be surveilled. To reiterate Foucault, this is due to the public's need for discipline exceeding the speed at which technological advancement can make it possible. Fear of terrorism, crime, and disorder have all been factors in continued amenability toward being surveilled. Instructor at the University of Montevallo, Levi Pulford, in his article, "'All Watched Over By Machines,' or AI Ethics, Surveillance, and Pluralism", asserts that people have willingly subjected themselves to

increasingly invasive surveillance while in pursuit of order. Visibility has become the norm, privacy obsolete. Society has lifted the veil over the private lives of the masses in the name of security, with little to no concern regarding who watches the watchmen. The question of who to surveil and how to navigate the mistakes that will inevitably be made remains unanswered.

In society's endless scrabble for law and order, it has surrendered its privacy. Convenience and fear have created a perfect storm for the tightened grip of electronic surveillance. If the people do not consent with being under oversight for easiness' sake, more will comply under the possibility of crime prevention. Pulford offers that, "With the rise of personal smart devices and personalized social media feeds, we have traded the Panopticon for a labyrinth of echo chambers", adding that new technological advances have made surveillance infinitely more feasible (1). Perhaps the majority feels that surveillance is harmless, even beneficial at times, but this is far from the case.

Electronic surveillance's prevalence in today's society is directly harming the masses while the surveilling benefit. Some may say that if one has nothing to hide, they have nothing to fear from surveillance-whereas in reality, society directly experiences the consequences of constantly being observed. Surveillance is a tool that is directly utilized against the watched. Professor of Law at Washington University, Neil M. Richards, in his journal article in *The Harvard Law Review,* explores how governmental and private surveillance erode civil liberties and intellectual privacy. Any free society should allow its citizens some modicum of privacy to think, loose from the ever-present eye of the surveilling overseer. The concept of surveillance is intrinsically opposed to freedom. If

surveillance is not being used by the government to excessively monitor, enforce, or blackmail, then it is being used by corporations in order to persuade consumers to buy more via their recommendations. In either scenario, surveillance is ultimately being used to control behaviour, and any moment surveillance is not being used is a moment when that control slips. Richards attests that surveillance creates a power dynamic between the *watcher* and *watched* via information, elaborating that "[it] gives the watcher increased power over the watched that can be used to persuade, influence or otherwise control them", going on to explain that this can happen even if the watched doesn't know they're being surveilled (1956). Electronic surveillance is so facile that it has likely already begun to shape society's behaviours; their wants, likes, and dislikes all decided and echoed to each other by the omniscient digital panopticon.

Electronic surveillance's proponents often argue that it is a necessary evil for law enforcement, making it all the more ironic that surveillance actively undermines several aspects of the legal system. Typically, law enforcement requires a warrant to search someone's person, vehicle, or residence; warrants that must be issued by a ruling that there is reasonable suspicion. Electronic surveillance, however, bypasses these procedures to directly observe a person's workplace, home, or personal messages without any reasonable suspicion of a crime. Former Deputy Assistant Secretary of Defence for Cyber Policy and founder of Third Way's Cyber Enforcement Initiative, Mieke Eoyang, and National Security Fellow at think tank Third Way, Gary Ashcroft, in their research report, *Why Electronic Surveillance Reform Is Necessary,* assert that legal corrections regarding electronic surveillance are needed in order to respect civil liberties. It is unlawful for law enforcement

to search someone's home, pockets, or car without the approval of a court, however, electronic surveillance monitoring a person's messages, internet searches, and location is-as of now-perfectly legal.

Surveillance has enabled the average person to have every action, written message and search engine query scrutinized for illegal activity without any suspicion that they were committing a crime in the first place. This can be also utilized in order to discover if said user is a member, or even agrees with the ideals, of a political group that the government is keeping an eye on. Surveillance has provided a window into the overlapping real and digital lives of the public for governments and corporations alike to peruse with impunity; a window that has no blinds to draw shut. Eoyang and Ashcroft point out that electronic surveillance allows for loopholes to laws preventing unlawful search and seizure, making emphatic that "without [the warrant requirement], law enforcement is given a blank check to subject Americans to intrusive, unjustified invasions of private life" (8). Given the obvious corrosion of legal procedure, the justification for surveillance as a tool of law and order falls quite flat.

Surveillance's inescapable grasp on society is facilitated by apathy, fear and convenience; a want to be safe, to not have to worry, for things to be easy. The promises spouted by electronic surveillance and its proponents are nothing but weak justifications for grotesque violations of privacy and civil rights. Surveillance functions as a tool of control, one that aims to dictate what people do, buy, and say in their daily lives. As technological capabilities increase, surveillance will as well. But it is not a hopeless fight. Some states have already proposed legislation to discourage or prevent surveillance and the sale of

personal data, such as the California Privacy Rights Act. If the public realized the extent of the harmful effects of being watched and overcame their apathy to demand legislation, society may very well be freed from its panoptic watchers.

Works Cited

Eoyang, Mieke, and Gary Ashcroft. *Why Electronic Surveillance Reform Is Necessary*. Third Way, 2017. *JSTOR*, http://www.jstor.org/stable/resrep02523. Accessed 23 Nov. 2025. Harari, Yuval Noah. "Big Data, Google, and the End of Free Will." *Rereading America: Cultural Contexts for Critical Thinking and Writing*, Twelfth edition, Bedford Saint Martin, 2021, pp. 341–347

Pulford, Levi. "'All Watched Over By Machines,' or AI Ethics, Surveillance, and Pluralism." *Computers & Society*, vol. 52, no. 2, 2024, pp. 28–28, https://doi.org/10.1145/3656021.3656032.

Richards, Neil M. "THE DANGERS OF SURVEILLANCE." *Harvard Law Review*, vol. 126, no. 7, 2013, pp. 1934–65. *JSTOR*, http://www.jstor.org/stable/23415062. Accessed 23 Nov. 2025.

Schneier, Bruce."How We Sold Our Souls–and More-To the Internet Giants." *Rereading America: Cultural Contexts for Critical Thinking and Writing*, Twelfth edition, BedfordSaint Martin, 2021, pp. 334–340