

Fighting Fire with Fire: Surveillance vs Sousveillance

Tyson Shannon

CIS, Minnesota State University-Mankato

CIS202W: Computers in Society

February 11, 2026

Fighting Fire with Fire: Surveillance vs Sousveillance

Surveillance has been one of the largest talking points of the 21st century, making it into regular news cycles regarding various governments and corporations for about two decades. However, what has not been discussed to the same extent is how these technologies can be used by citizens to defend against surveillance. Since the early 2000's surveillance has become an ever-increasing reality for modern civilization. Major countries from the Five Eyes to adversarial nations like Russia and China have seen surveillance grow alongside technological advancement. With increased tensions both domestically and internationally, many governments are violating privacy in the name of greater security and control. At the same time companies with access to large amounts of personal data have surpassed oil companies in value and taken the crown as the most valuable industry in the world (European Parliament, 2020). This has made surveillance not only a form of control but a profitable enterprise. Surveillance is described as any collection of personal data for the purpose of influence or management of an individual or group (Dinev et al, 2008). The word stems from the French sur- "over" and veiller- "to watch" meaning "to watch over". In contrast, the concept of sousveillance utilizes the prefix sous- "below" meaning "to watch from below". Sousveillance is the practice of surveilled individuals filming surveillance activities and authority figures (Bakir, 2018). To simplify, sousveillance is a form of counter-surveillance using similar techniques used by many governments. With the rise of camera phones and the internet tools necessary for recording, communicating, and tracking is widely available to everyday citizens. The same technology used to track us every day can be pointed back at our authorities when privacy is uniquely

and exceptionally violated. The modern technological age has given governments and corporations unprecedented power to invade our privacy. However, that same power is in the hands of everyday citizens allowing us to keep these organizations in check. As we'll see, sousveillance is a necessary last resort for democratic societies in this new era.

Government and Corporate Surveillance

The dawn of the 21st century has brought many social benefits for the average person but has also created a new environment of risk for both governments and individuals. No moment looms a larger example of this than post 9/11 America. As a result, we as a society have accepted, willingly or not, a new social contract with less privacy in exchange for more convenience and safety. However, organizations continue to push the limits of how much people are willing to give up. Governments have learned they can gather detailed reports of individuals through online reconnaissance, information gathering by social engineering, phone and device tracking, camera/video tracking, and their online footprint (Shimonski, 2014). Only a few of these techniques require warrants making the question not if we are being tracked but what the government wishes to do with this information.

Corporations have also seen a shift in their attitude toward surveillance since 9/11. In 1996, the FBI and CIA said they were unable to protect enterprises from corporate spying (Boghossian, 2013, p. 38), and these activities became the norm among businesses. However, after 2001 there was a resurgence in the private espionage industry and many of these companies were praised for their efforts which now pointed away from other

companies and towards the public. These security firms also face little to no consequences for abuse of power, sometimes with even less oversight than government organizations. Among the thousands of companies that have arisen through the influx of US contracts, Google has become one of the most successful. In 2012 Google was fined a mere 7 million dollars for unlawfully logging unsecure Wi-Fi traffic across 37 states while running their Street View project (Boghosian, 2013, p. 44). In the 90's the government lacked the ability to stop corporations from spying, but today they simply lack the desire.

Sousveillance Tools and Methods

Although it can be nearly impossible to take back privacy, it has become incredibly easy to create transparency using the same tools used to spy on us. By pointing these digital powers at corrupt authorities, we can level the playing field and expose unjust behavior. Sousveillance is not a tool for solving abusive surveillance but a last resort for democratic societies to fight for constitutional rights against a higher power. Some examples of tools that can be used by everyday people for this purpose include screenshotting online evidence, filming with mobile cameras, social media live streams, crowd sourced tracking, and even hashtags for connecting similar posts (Jenkins & Cramer, 2022). Many make arguments discussing the ethical implications of utilizing surveillance to fight surveillance, citing the economic benefit for the companies who design these tools (Borradaile & Reeves, 2020). However, sousveillance is not a solution to any civil issues being experienced by a population but rather a necessary defense.

Real World Sousveillance Examples

In the winter of 2026 Minnesotans stormed the frigid streets, phones up and cameras rolling. As federal officers took over cities and as numerous claims of abuse rolled in, Governor Tim Walz had one request to his constituents, “Help us create a database not just to establish a record for posterity but for future prosecutions.” (Loria, 2026). So, every step federal immigration officers made was tracked by the public, as family vehicles chased unmarked government vans. Every arrest, every misstep, every shooting was caught in real time from multiple directions. This event perfectly demonstrates the power of sousveillance. In an unprecedented event the US federal government used surveillance technology for targeted attacks on immigrant communities. As a result, videos were filmed, crowd sourced tracking apps were made, and social media was utilized to spread messaging rapidly. Due to international backlash towards the information that was being gathered by citizens, much of the immigration crackdown was scaled back, however not yet removed entirely, and some individuals were even freed from custody. Although it remains too early to know the full outcome of this event, we have learned the true power inside every pocket on the planet. Minneapolis has become a perfect example of how sousveillance can counter authoritarian action and allow the average person to become a government watchdog.

Conclusion

In conclusion, the use of surveillance has never been higher, and governments and corporations get away with violating our privacy in increasingly intricate ways. However, the same technology that has infiltrated our lives can be used to keep these great powers in check. Although not a complete solution, sousveillance makes a powerful and proven

last defense against surveillance states overstepping their constitutional rights. It is necessary to acknowledge the new world order we find ourselves in where excusing yourself from the system is no longer an option. Embracing technology and utilizing civilian ingenuity gives citizens everywhere a fighting chance in an ever-changing world.

References

- Bakir, V. (2018). Sousveillance. In B. A. Arrigo (Ed.), *The SAGE encyclopedia of surveillance, security, and privacy*. SAGE Publications. <https://sk-sagepub-com.ezproxy.mnsu.edu/ency/edvol/the-sage-encyclopedia-of-surveillance-security-privacy/chpt/sousveillance>
- Boghosian, H. (2013). *Spying on democracy: Government surveillance, corporate power, and public resistance* (1st ed.). City Lights Books. <https://ebookcentral-proquest-com.ezproxy.mnsu.edu/lib/mnsu/detail.action?pq-origsite=primo&docID=1321759>
- Borradaile, G., & Reeves, J. (2020). Sousveillance capitalism. *Surveillance & Society*, 18(2), 272–275. <https://www.proquest.com/docview/2427315079?accountid=12259&parentSessionId=f5Oa8tnPR0HBU17ZY5Zcv0NLARjG124R4hjdNt1Oez8%3D&pq-origsite=primo&sourcetype=Scholarly%20Journals>
- Dinev, T., Hart, P., & Mullen, M. R. (2008). Internet privacy concerns and beliefs about government surveillance: An empirical investigation. *The Journal of Strategic Information Systems*, 17(3), 214–233. <https://www-sciencedirect-com.ezproxy.mnsu.edu/science/article/pii/S0963868707000492>

European Parliament. (2020). Is data the new oil? Competition issues in the digital economy (Briefing). European Parliamentary Research Service.

[https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/646117/EPRS_BRI\(2020\)646117_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/646117/EPRS_BRI(2020)646117_EN.pdf)

Jenkins, B. M., & Cramer, E. M. (2022). Capturing injustice: The screenshot as a tool for sousveillance. *Howard Journal of Communications*, 33(4), 412–433. <https://www-tandfonline-com.ezproxy.mnsu.edu/doi/full/10.1080/10646175.2022.2032884#d1e202>

Loria, M. (2026, January 14). Walz to Minnesota: Use your phones to record ICE injustices. *USA Today*. <https://www.usatoday.com/story/news/nation/2026/01/14/walz-calls-on-people-to-record-ice-for-future-prosecutions/88187191007/>

Shimonski, R. (2014). *Cyber reconnaissance, surveillance and defense* (1st ed.). Elsevier Science & Technology. <https://ebookcentral-proquest-com.ezproxy.mnsu.edu/lib/mnsu/detail.action?pq-origsite=primo&docID=1820202>