

Queen Mary University of London

Privacy through History's Lens

Neverending Surveillance

Jaime Salmonson

A History of the Internet HST5618

Professor Chris Sparks

05. 06. 2025

"Perhaps in the long run the fight to preserve privacy [in the digital world] is a vain one. But, like the struggle to preserve life it must be continued while any shred of privacy remains."

- *New York Times* 1966

In the digital age, privacy can seem like it is an endangered species clinging to life amid the unchecked rise of surveillance creeps, data mining, and artificial intelligent intrusion. The 1966 quote seen above represents both a challenge and a rally cry. It asks us: if privacy is the pure soul of freedom, how much of it are we willing to give up for our convenience and/or security? We can turn to history to examine the landscape of such a struggle – a tale of defiance against the encroaching shadows of Orwellian oversight, from the birth of ARPANET to Edward Snowden's revelations. Through the lens of time, the fight for privacy is not just a battle against the inevitable; it is a testament to our refusal to be subdued, even by the never ending evolution of technology. In this essay, I will look to history and determine that it becomes clear that while the battle for privacy may seem vain, it remains an important defense of human freedom in the digital age.

Historical Context

In the beginning, the internet was an abyss of freedom – a vast uncharted territory where curiosity reigned supreme. But even in its earliest days, privacy and surveillance were quietly implemented. The ARPANET, the precursor to our modern day internet, was not designed for privacy as the number one priority. Instead, the focus was to connect and express adversity during the cold war. As networks grew, so did the potential for its misuse and monitoring. Governments and other large organizations quite quickly recognized the immense value of collecting data, turning a tool for communication into a powerful way to control. This tension

between protecting individual privacy and exploiting technology for oversight was baked into the internet's foundations, creating the infrastructure for decades of debates and struggles to come regarding who is watching, who is watched, and what is “fair” in the digital world. The seeds of surveillance were sown early, and their roots run deep.

Orwell’s Vision & the Fight for Privacy

I remember reading George Orwell’s *1984* in the 9th grade and dismissing his vision of the future as far-fetched. But as time went on, I realized just how wrong I had been. The novel, often regarded as a chilling prediction of authoritarian surveillance, portrays a world where the government oversees every action, with constant reminders like the ominous slogan plastered across Oceania: “BIG BROTHER IS WATCHING YOU”(Orwell, 1989, p. 06, 07, 204). In this dystopia, even the very concept of privacy is crushed under the weight of control and fear. This “futuristic” vision can easily be applied in the modern digital era, where systems like metadata archives and internet surveillance are eerily similar to Orwell’s warnings. In *1984*, surveillance was both obvious and invasive, forcing citizens to censor their behaviors. Modern surveillance systems, while they are more subtle, have a similar omnipresence through algorithms and security cameras that analyze our behavioral data. Programs like PRISM and XKEYSCORE revealed how governments can exploit private personal information under the guise of national security. The loss of privacy is not accidental or temporary, it is deliberately built into the structure of surveillance systems. As Tom Engelhardt (2014) describes, “They have constructed a system potentially riddled with what, in the Cold War days, used to be called ‘moles.’ However, these moles aren’t spying for a foreign power – they’re spying for us. Privacy has been obliterated, encoded into the very DNA of the surveillance apparatus they’ve built” (Engelhardt, 2014, p. 62).

As Orwell warned, privacy is not just a personal concern – it is the basis of freedom, and compromising it is nothing short of oppression. The similarities show us the timeless relevance of Orwell's warningful tale, as well as the need to defend our right to privacy while we combat modern threats to our autonomy.

Historical Case Studies

The Electronic Frontier Foundation:

The Electronic Frontier Foundation (EFF) is a non-profit organization devoted to defending civil liberties in digital society by making sure that technology is a force for empowerment and not oppression (EFF, n.d.). Since its establishment in 1990, the EFF has been an advocate for privacy and freedom online, winning battles against the government for their overreach in intrusive policies. One of its most important confrontations was the challenge to the Communications Assistance for Law Enforcement Act (CALEA) – legislation that's goal was to use surveillance systems within telephones (EFF, n.d.). Moreover, another important achievement was the role it played in the case of *ACLU v. Clapper*, which resulted in the 2015 ruling of the NSA's collection of phone metadata *unconstitutional* (ACLU, 2015). Through these important moments, the EFF went from just questions about the privacy ideals, to real tangible victories.

Snowden Revelations

Now to talk about one of the most influential names of the privacy age: Edward Snowden. Snowden was a former contractor for the U.S National Security Agency who leaked *thousands* of classified documents regarding global surveillance programs – some viewed him as a hero

while others a traitor. Programs like PRISM and XKEYSCORE (secret surveillance programs), once hidden in the shadows, were suddenly thrust into the glaring light of public scrutiny (Bamford, 2013). His 2013 revelations swept across the globe like a digital tsunami, altering the grounds for privacy debates forever. And these were not just programs – they were embodiments of a surveillance structure so large it bordered on dystopian fiction. These programs became the starting point for major discussions, completely changing privacy from an abstract concept into an *urgent global priority*. The public demand that followed brought about many meaningful legislative changes, such as the USA FREEDOM Act of 2015, which sought to control some of the NSA's surveillance practices (114th Congress, 2015). But beyond legislation, Snowden's actions were a powerful reminder that even in an age of unprecedented surveillance, people could challenge the status quo and be a part of *real change*.

Wiretapping & Protocol Design

The early days of the internet was really just a mix of experiments, where the wonderful potential of web-based connection battled with the realities of government oversight. In the 1990s, the Internet Engineering Task Force (IETF) was at the intersection of privacy and surveillance, debating whether to integrate wiretapping capabilities into internet protocols. At first, “Many early Internet protocols reflected an environment in which security and privacy were not crucial or immediate concerns” (DeNardis, 2015). The stakes were quite high: Was the internet to be a safe haven for innovation, or would it become yet another tool for control? Advocates for surveillance pointed out its necessity for law enforcement, but critics said that such mechanisms could be weaponized by malicious intent. In the end, the IETF chose privacy, emphasizing its value in shaping the internet as a space of trust. These debates were not just

technical, but philosophical, reflecting a commitment to shaping the internet as a space where privacy actually could prevail.

Surveillance Abuse & Misuse

Historically, the practice of Charivari, a village custom for enforcing social rules through *collective shaming*, expressed the power of community driven surveillance – “The Charivari was turned against anything the community found unnatural, [they] are reactive, offering no constructive plan beyond humiliating and shaming the offender, and [they] die away as quickly as it flares up” (Brunton, 2013 p. 103). If we take this and apply it to the online world, this cultural phenomenon takes a new form of mediated structures where violations of the norm are met with collective punishment. In 1988, Rob Noha overwhelmed USENET (a platform for online discussions) with an excessive amount of posts. This messed with the platform's normal flow and annoyed its users, which of course led to an outlash from the other users. Rather than turning to the creators, users identified his internet service provider (ISP) and organized community action to publicly shame him (Brunton, 2013, p. 44). This bottom up approach expresses the potential of surveillance systems to enforce accountability, but it also exposes the risks of collective judgment as a weapon. Shame, while maybe a potent tool, has its limits – it may enforce the norm but most definitely lacks the sophistication to address systemic issues.

The WELL (Whole Earth [e]lectronic Link), an early online discussion forum, is an example of the tension between surveillance and the digital frontier's ideals. WELL members envisioned a new culture built on “openness and countercultural values”, yet hacking incidents tested the boundaries of their vision. Figures like Acid Phreak and Phiber Optik engaged in activities that revealed the darker sides of surveillance, using their skills not to foster community but to exploit

people's vulnerability. The raid on Acid Phreak's home in 1990, following accusations of causing a crash in AT&T's network, showed us the government's crackdown on hacking. John Perry Barlow's reflections on these events explain the idealistic world versus the realities of surveillance. For Barlow, cyberspace was a chance to form new, free, communities, but his ideas were often met with the issue of managing security and misuse (Turner, 2008).

As digital surveillance systems became more prevalent, abuses became more complex, from financial exploitation to spam schemes to the illegal collecting of user data. Governments, put to task with overseeing these systems, often found themselves treading dangerous waters. Finding a balance between protecting national security *and* preserving individual rights proved to be an enduring challenge. For example, the NSA's surveillance programs expressed the potential for overreach, where the lines between protection and intrusion aren't quite clear. To lessen the risks, policy emphasizing transparency, accountability, and "privacy first" design should be prioritized.

Age of Encryption

Encryption is both a shield, as well as a battlefield in the fight for privacy. "Encryption is an essential tool in providing security in the information age. Properly implemented encryption allows sensitive information to be stored on insecure computers or transmitted across insecure networks" (Abelson et al., 1997). At its heart, it transforms data into unreadable, confusing, code, a safe to protect sensitive information. However, this shield has brought about philosophical questions. As Laura DeNardis (2015) so perfectly put it in the title, encryption embodies the "design tension between surveillance and security." On one side, it defends people

who expose wrongdoing and who oppose authoritarian governments; on the other, it is exploited by criminals to conceal their crimes.

This polarity brings about debates; governments call for backdoors, arguing that “it might be useful in the future to search through anyone’s calling history to see if that person had been in contact with a suspected terrorist, the agency should be able to collect everyone’s records and store them for five years,” (Cole, 2014). Though privacy advocates warn that such backdoors could be detrimental, echoing Finn Brunton's (2013) insights on the unintended consequences of networked systems – if exploited, they would compromise the integrity of encryption for all users, leaving most people, if not everyone, vulnerable.

Despite these risks, the argument for strong encryption continues: encryption is not just a technical tool but a philosophical one. James Bamford (2013) reminds us that privacy “is a condition for freedom,” and without it, democratic values may falter. While encryption could offer sanctuary to some malicious people, its broader role as a defense against surveillance outweighs its dangers. In a world where metadata alone is a dangerous weapon, encryption is a necessary protective fortress – a silent, but important, advocate for autonomy.

Conclusion

The fight for privacy is like the struggle to preserve our life; it is what seems like a never-ending battle that *must continue*, no matter the amount or intensity of obstacles. History has shown us in obvious ways that while threats to privacy evolve along with our technological evolutions, so too do the efforts to defend it. From the early debates over wiretapping protocols to the modern dilemmas of encryption and surveillance, one lesson remains clear: privacy is not a fleeting standard but is a definition of freedom.

Yes, the path is marked by misuse, overreach, and the tension between security and liberty, but our commitment to safeguarding privacy is important for the digital age to survive. Each step forward, whether that be legal victories, safe technological innovations, or community resistance, reinforces this truth: the preservation of privacy is not just a fight worth waging, but is essential for the protection of our autonomy, dignity, and democratic values.

Reference Page

114th Congress (2015) *H.R.2048 - USA FREEDOM Act of 2015*. [Online]. Available at:
<https://www.congress.gov/bill/114th-congress/house-bill/2048/text> (Accessed: 5 April 2025).

Abelson, H., Anderson, R., Bellovin, S.M., Benaloh, J., Blaze, M., Diffie, W., Gilmore, J.,
 Neumann, P.G., Rivest, R.L., Schiller, J.I. and Schneier, B. (1997) 'The Risks of Key Recovery,
 Key Escrow, and Trusted Third-Party Encryption', *World Wide Web Journal*, 2(3), pp. 241-257.
 Available at: https://www.schneier.com/academic/archives/1997/04/the_risks_of_key_rec.html
 (Accessed: 5 April 2025).

ACLU (2015) *ACLU v. Clapper - Challenge to NSA Mass Call-Tracking Program*. [Online].
 Available at:
<https://www.aclu.org/cases/aclu-v-clapper-challenge-nsa-mass-call-tracking-program> (Accessed:
 5 April 2025).

Bamford, J. (2013) 'They Know Much More Than You Think', *The New York Review of Books*,
 60(13), pp. 4-8.

Brunton, F. (2013) *Spam: A Shadow History of the Internet*. Cambridge, MA: MIT Press.

Cole, D. (2014) 'We Kill People Based on Metadata', *The New York Review of Books*, 10 May.
 Available at: <https://www.nybooks.com/daily/2014/05/10/we-kill-people-based-metadata/>
 (Accessed: 8 April 2025).

DeNardis, L. (2015) 'The Internet Design Tension between Surveillance and Security', *IEEE
 Annals of the History of Computing*, 37(2), pp. 72-83.

EFF (n.d.) *Electronic Frontier Foundation*. [Online]. Available at: <https://www.eff.org/>
(Accessed: 8 April 2025).

Engelhardt, T. (2014) *Shadow Government: Surveillance, Secret Wars, and a Global Security State in a Single-Superpower World*. Chicago: Haymarket Books. Available at: ProQuest Ebook Central, <http://ebookcentral.proquest.com/lib/gmul-ebooks/detail.action?docID=1649310>
(Accessed: 10 April 2025).

Orwell, G. (1989) *Nineteen Eighty-Four*. London: Penguin Books.

Turner, F. (2008) *From Counterculture to Cyberculture: Stewart Brand, the Whole Earth Network, and the Rise of Digital Utopianism*. Chicago: University of Chicago Press.