

# Analyse the balance between security and privacy in the legislation concerning digital surveillance.

Aarini Gupta

Given the rapid technological growth of the 21st century, modern states face a dilemma: in guarding its citizens against unprecedented threats, it risks dismantling the freedoms that define democracy itself. The promise of digital surveillance is security, wherein its danger is the quiet erosion of liberty. In this essay, I will attempt to analyse the balance between security and privacy in digital surveillance legislation by first examining the arguments in favour of surveillance, then highlighting overreach and rights violations, and finally exploring how legal safeguards and oversight can engineer a successful balance.

The strongest defence of mass surveillance lies in its undeniable utility. The interception of Najibullah Zazi's 2009 New York subway bombing plot is believed to have been the result of a US PRISM programme that sifted through consumer information from tech giants (Hosenball, 2013). CCTV was also central to identifying the culprits of both the 2005 London bombings (Greenberger, 2006) and Boston Marathon attack (FBI, n.d.). When the stakes are literally life-or-death, surveillance is indispensable.

Yet security is not absolute. The Edward Snowden disclosures revealed that the NSA's bulk collection of phone metadata indiscriminately swept up millions of Americans' records, most with no links to crime (BBC News, 2014). Such practices do more than breach Article 12 of the Universal Declaration of Human Rights (United Nations, 1948): they sow distrust, invite misuse, and create what scholars call a "chilling effect" where citizens censor themselves out of fear of unseen eyes (Chadha, 2022), drawing eerie parallels to Orwell's 1984. Similarly, the UK's Investigatory Powers Act of 2016 authorised sweeping interception powers, later criticised in European courts for violating privacy rights (Siddique, 2021). By normalising indiscriminate monitoring, governments risk turning exceptional powers into permanent fixtures.

The supposed trade-off between security and privacy is a false binary. A state that monitors its citizens too broadly risks both being overwhelmed by useless data and also eroding the trust on which effective security depends. Approaches focused on high-risk individuals, judicial warrants, and external monitoring of intelligence agencies not only protect rights but also render intelligence more precise. (Deeks, 2015) The USA Freedom Act of 2015, which restricted bulk data collection, is one example of how oversight can be restorative (Forsyth, 2015). The EU's GDPR, meanwhile, reframed privacy as a proactive obligation rather than an afterthought (gdpr.eu, n.d.).

In conclusion, while surveillance is undoubtedly necessary for ensuring security, it is rendered legitimate not by clandestine mass and indiscriminate monitoring, but by transparency, trust, and above all, the recognition that citizens are not merely data points to be managed but rights-bearers to be respected. Liberty and security are not opposing forces, but interdependent ones. Thus, the real danger lies not just in the sacrifice of too much privacy in the name of security, but also that in doing so, we forget what we were trying to secure in the first place.

## References:

- BBC News. (2014). Edward Snowden: Leaks that exposed US spy programme. Available at: <https://www.bbc.com/news/world-us-canada-23123964> (Accessed: 17 September 2025).
- Chadha, V. (2022). Balancing the Privacy v Surveillance Argument. Dialnet. Available at: [https://www.researchgate.net/publication/360632235\\_Balancing\\_the\\_Privacy\\_v\\_Surveillance\\_argument\\_a\\_perspective\\_from\\_the\\_United\\_Kingdom](https://www.researchgate.net/publication/360632235_Balancing_the_Privacy_v_Surveillance_argument_a_perspective_from_the_United_Kingdom) (Accessed: 17 September 2025).
- Deeks, A. (2015). An International Legal Framework for Surveillance. Available at: <https://ssrn.com/abstract=2490700> (Accessed: 17 September 2025).
- FBI. (n.d.). Boston Marathon bombing. [online]. Available at: <https://www.fbi.gov/history/famous-cases/boston-marathon-bombing> (Accessed: 17 September 2025).
- Forsyth, B. (2015). Banning Bulk: Passage of the USA FREEDOM Act and Ending Bulk Collection, 72 Wash. & Lee L. Rev. 1307. Available at: <https://scholarlycommons.law.wlu.edu/wlulr/vol72/iss3/9> (Accessed: 17 September 2025).
- GDPR.eu (n.d.). What is GDPR, the EU's new data protection law?. Available at: <https://gdpr.eu/what-is-gdpr/> (Accessed: 17 September 2025).
- Greenberger, M. (2006). The need for closed circuit television in mass transit systems. Law Enforcement Executive Forum, pp.151. University of Maryland Legal Studies Research Paper No. 2006-15. Available at: <https://ssrn.com/abstract=900414> (Accessed: 17 September 2025).
- Hosenball, M. (2013). U.S. NSA Internet spying foiled plot to attack New York subways: sources. Reuters. Available at: <https://www.reuters.com/article/technology/us-nsa-internet-spying-foiled-plot-to-attack-new-york-subways-sources-idUSBRE956171/> (Accessed: 17 September 2025).
- Siddique, H. (2021). GCHQ's mass data interception violated right to privacy, court rules. Available at: <https://www.theguardian.com/uk-news/2021/may/25/gchqs-mass-data-sharing-violated-right-to-privacy-court-rules> (Accessed: 17 September 2025).
- United Nations. (1948). Universal Declaration of Human Rights. Available at: <https://www.un.org/en/about-us/universal-declaration-of-human-rights> (Accessed: 17 September 2025).