Journal of Law, Policy and Globalization
ISSN 2224-3240 (Paper) ISSN 2224-3259 (Online)
Vol.149, 2025

Reconciling Personal Data Protection with Public Security Interests: Legal and Ethical Challenges in the Age of Surveillance

ZAMMY A. OWODUNNI
LL.B., B.L., LL.M. *Louisiana State University, Baton Rouge*
* E-mail of the corresponding author: owodunnizammy@gmail.com

ABSTRACT
The exponential growth of digital technology has introduced a critical and complex conflict between the state's compelling interest in maintaining public security and the fundamental right of individuals to the protection of their personal data and privacy. In an age characterized by mass digital surveillance and the weaponiation of personal data for malicious ends—such as targeted disinformation, terrorism, and political psyops—governments face the challenge of implementing effective security measures without infringing upon civil liberties. This article addresses this tension by examining the legal and ethical challenges inherent in balancing these two competing values. It explores the complexities of implementing public security measures that necessitate the collection and analysis of large datasets while simultaneously respecting individuals' privacy rights. Furthermore, the analysis critically evaluates existing legal provisions within US law intended to reconcile these interests, identifying key gaps and limitations. The article concludes that the collision between public security and privacy is inevitable but manageable. Consistent reconciliation requires continuously updated legal and regulatory guidelines that define clear scopes for data collection, mandate stringent transparency and accountability measures, and enforce the principles of necessity and proportionality. To bridge the identified legal gaps and adapt to accelerating advancements such as AI-driven surveillance, the article recommends the establishment of a dedicated multi-stakeholder oversight body to conduct independent compliance audits and proactively propose legislative amendments.
Keywords: Personal Data Protection, Public Security, Surveillance Law, Privacy Rights, Ethical Challenges, Necessity and Proportionality, Data Governance.
DOI: 10.7176/JLPG/149-14
Publication date: December 28th 2025

INTRODUCTION

The need to maintain public security and protect sensitive information has become more crucial in a modern world of digital and technological advancement.[1] However, this need for public safety must be balanced against the right to privacy and protection of personal data, which can be complex because it requires careful consideration of legal and ethical implications.[2]

The widespread use of the internet and digital devices has made lives easier, but it has also created new challenges, particularly in the area of public security and privacy. With an increasing amount of personal and sensitive information being stored online, the collection, processing, and protection of personal data has become a critical concern and challenge for governments.[3] The reason for this is that a vast amount of personal data online can be used for targeted messaging and disinformation, which can lead to terrorist attacks, mob actions, political psyops, or even mass economic loss.[4] There is therefore a need to reconcile personal data protection with public security interests because these two values often conflict with each other. For instance, implementing strong public security measures may require collecting and analyzing large amounts of personal data, which could infringe on an individual's privacy rights. Conversely, protecting individuals' privacy may require limiting the collection and use of personal data, which could compromise public security.[5]

[1] N Allahrakha, 'Balancing Cyber-security and Privacy: Legal and Ethical Considerations in the Digital Age' (2023) 4(2) Legal Issues in the Digital Age, 78-121.
[2] P Singer and M Tushman, *Understanding Cyber-Security and the Implications for National Security* (N.Y. Columbia University Press, 2021).
[3] N Kshetri, 'A Global Analysis of Data Breaches: focus on sensitive data theft' (2021) 133 Journal of Business Research, 326-334.
[4] E Luiijf 'Cyber-security and resilience: what are we talking about? In *Cyber Security: From Technology to Society* (Cham: Springer, 2019).
[5] P Rosenzweig 'Balancing Privacy and Security: The Ethical Dimension' in J Quigley and D Molnar (eds), *Routledge Handbook of Science, Technology and Society* (L. Routledge 2015).

Based on these observations, this article examines the legal position on the protection of personal data and the ethical considerations involved in balancing public security interests with privacy rights. Furthermore, the article explores the challenges of implementing effective public security measures while respecting privacy rights. Finally, the article critically evaluates extant provisions of US law that attempt to balance public security and privacy protections and makes suggestions and recommendations for reconciling both.

PUBLIC SECURITY INTERESTS Vs. PRIVACY RIGHTS

The journey of surveillance technologies began with rudimentary systems primarily focused on direct observation and basic recording devices.[1] The concept of surveillance was historically rooted in military and security contexts, where it served as a tool for gathering intelligence and ensuring public safety. As technological advancements accelerated, particularly in the 20th century, surveillance evolved significantly with the integration of electronic and digital technologies. The mid-20th century marked the onset of a technological revolution in surveillance with the introduction of CCTV systems.[2] Initially developed for security purposes in high-risk areas, CCTV rapidly became a mainstay in public and private spaces, significantly expanding the reach and efficacy of surveillance.[3] The digital age ushered in a new era with the development of advanced digital cameras and networked video capabilities, which allowed for real-time monitoring, recording on an unprecedented scale, and the integration of digital technologies into surveillance systems.[4] The proliferation of the internet and wireless communication technologies gave rise to digital surveillance tools that could monitor and analyze vast amounts of data. This era also saw the introduction of biometric technologies, which utilized unique physical characteristics such as fingerprints, facial recognition, and iris scans for identification and surveillance purposes.[5]

Today, surveillance technologies encompass a broad spectrum of tools and systems, from advanced biometrics and facial recognition to massive digital data collection and analysis frameworks supported by artificial intelligence (AI). These technologies are not only more pervasive but also more capable, with the ability to integrate data from multiple sources and analyze it with little to no human intervention. The implications of these capabilities extend far beyond traditional security concerns, influencing privacy rights, individual freedoms, and social dynamics.[6]

As surveillance systems become more embedded in everyday life, the dialogue around the ethical implications, privacy concerns, and regulatory requirements becomes increasingly significant because of a growing mainstream concern that public security and privacy rights are in a collision. This perception stems from the view that to maintain public safety, the government and its agents have to always be in advance of any activity, such as crime, terrorist attacks, conspiracies, mob actions, riots or mass psyops of any sort that endangers public security interests. To maintain foresight and forestall these threatening activities, the government often deploys surveillance systems to detect, classify, monitor, and track objects and persons of interest in real time.[7] Such surveillance process often ranges from intercepting phone calls, emails, text message, and digital chats to monitoring clicking behaviour on social media, flagging of web surfing to certain sites, active and passive video camera data gathering, electronic monitoring of personal conversations, deployment of CCTV or GPS tracking system to determine live location of subjects of interest, use of surveillance advanced drones, algorithms and high tech to provide predictive and diagnostic data from subjects of interest[8]. These surveillance systems, especially CCTV and digital monitoring, have proven effective in promoting public security interests such as deterring offenders and providing crucial evidence for prosecution.[9] However, they have also raised privacy concerns. In one case, for example, a CCTV camera installed for traffic monitoring inadvertently captured

[1] MC Wheatley, 'Ethics of Surveillance Technologies: Balancing Privacy and Security in a Digital Age' 2024 1 Journal of Data Science 1-8.
[2] Ibid
[3] C Norris and M Mchill, *CCTV in Britain: a social and political perspective on the emergence and development of public space surveillance* (University of Oxford Press, 2015).
[4] Wheatley (n6).
[5] I Ajunwa, K Crawford and J Schultz, 'Limitless worker surveillance' (2017) 105(3) California Law Review 735-76.
[6] BE Harcourt, 'Exposed: Desire and disobedience in the digital age' (2024) 1 Journal of Data Science 1-8.
[7] DJ Power, C Heavin and Y O'Connor, 'Balancing privacy rights and surveillance analytics: a decision process guide' (2021) 4:2 Journal of Business Analytics 155-170.
[8] Ibid.
[9] NG La Vigne and SS Lowry, 'Evaluation of Camera Use to prevent crime in commuter parking facilities: a randomized controlled trial' 2011 47(5) Urban Affairs Review 695-716.

footage from private residences.[1] In another case, drones conducting aerial sweeps captured intimate images and videos of private gatherings of individuals in their private spaces.[2]

In this regard, scholars like Yoo argue that public security and privacy rights are headed for collision as there is no way to ensure public security in a modern world without surrendering certain protection of personal data, because overly strict privacy right protections will necessarily inhibit law enforcement and national security agencies from accessing important data to prevent threatening activities like terrorist attacks.[3] However, other scholars like Greenwald are of the view that surveillance systems aimed at public security are not necessarily in collision with privacy rights since surveillance is not necessarily evil. Rather, privacy rights protections aim to prevent governmental overreach. Greenwald, for instance, argued that the need for controlling the scope of surveillance is exemplified in the extent of the U.S. government surveillance activities, which were exposed through the reporting on the Edward Snowden leaks.[4] The leaks revealed how the government collected a vast amount of data on private citizens without their knowledge and consent.

It is hard not to agree with Greenwald since almost every reasonable person will agree that some level of surveillance is always necessary to ensure public security. Thus, it can be argued that privacy concern is not really about surveillance in itself but about the scope of surveillance deemed necessary and the level of transparency surrounding the development, deployment, and use of surveillance tools and the data gathered through it. The question over the lack of transparency on the use of surveillance systems is important because of the legitimate fear that the data collected through the surveillance systems might violate privacy boundaries by being used for purposes that have no public security interests, such as political or private blackmail, disinformation, or mass psyops.[5] This concern was exemplified in the Cambridge Analytica scandal in which a small London-based data analytics company harvested and compiled the personal data of more than 50million Facebook users and then deployed a series of targeted psychological messages to the compiled profiles for the purpose of influencing the 2016 United States Presidential elections.[6] Thus, the Cambridge Analytical scandal exemplifies that, aside from the legitimate concern of surveillance being used for governmental overreach, personal data is also a valuable commodity that can be traded in the marketplace and monetized by private businesses who may hand over such personal data to actors who will use it for mass disinformation or psyops.[7] It is thus clear why privacy concerns over a lack of transparency on the use of surveillance systems to gather personal data are legitimate. Especially because, rather than serving the goal of public security, surveillance systems, if not transparently implemented, can in fact harm public security by eroding public trust and limiting cooperation between citizens and law enforcement agencies.[8]

However, while the concern over a lack of transparency is legitimate, it is nevertheless problematic for a number of reasons. First, and as regards the scope of surveillance deemed necessary, it should be noted that activities that require surveillance for public safety are not abstract theoretical hypotheses but rather real-life cases with different, nuanced, and continuously developing contexts that will require the exercise of good-faith judgment in real time. Thus, only in hindsight will it be clear in many cases whether surveillance was justified or not. Second, and as regards transparency on the development and deployment of surveillance systems, it is hard to see how public security will still be served if the government becomes publicly transparent about the development and deployment of surveillance systems, since such disclosure will only aid hostile actors and subjects of interest in evading surveillance tools that have been developed for public security purposes. Thus, the potential collision between public security and privacy protections arises because both concepts have distinct goals that will often clash. While the public security surveillance system is focused on extracting, collecting, gathering, and sometimes exposing personal data for collective safety and security, privacy rights, on the other hand, are focused on ensuring that such personal data remains concealed from public scrutiny.

[1] L Roberts, 'Employee privacy monitoring: the pros and cons of workplace surveillance' 2021 160(2) Journal of Business Ethics 635-50.
[2] M Green, 'Balancing privacy and protection: the legal debates over drone surveillance' (2021) 134(4) 2023-41.
[3] C Yoo, 'Cyber-security and freedom on the internet' (2015) 38(1) Harvard Journal of Law & Policy 129-137.
[4] G Greenwald, 'The National Security Agency in the age of Cyber Surveillance' (2021) 237 Foreign Policy 78-86.
[5] S Zuboff, 'Big other: surveillance capitalism and the prospects of an information civilization' (2015) 30(1) Journal of Information Technology, 75-89.
[6] H Kuchler, 'Cambridge Analytica case highlights Facebook's data riches' *Financial Times* (San Francisco, 19 March 2018) <https://www.ft.com/content/c1f326a4-2b24-11e8-9b4b-bc4b9f08f381> accessed 9 July 2025.
[7] A Acquisti and J Grosslags, 'Economics and Privacy' (2013) 51(2) Journal of Economic Literature 1-32.
[8] R O'Harrow, 'Privacy vs. Security: A False Dichotomy' (2017) 9(1) Journal of National Security Law & Policy 95-113.

In view of this, several legal provisions and safeguards have emerged in the United States to balance public security interests with the protection of privacy rights.

LEGAL PROVISIONS BALANCING PROTECTION OF PERSONAL DATA AND PUBLIC SECURITY INTERESTS

The jurisprudence that underpins the protection of personal data is rooted in the right to privacy, which refers to the social, moral, and legal understanding that certain personal information of people must be immune to public scrutiny.[1] The scope of what constitutes personal data varies by jurisdiction based on public policy. However, such scope often covers the privacy of person as well as the person's personal behaviour, personal communication, personal data, location, personal thoughts and beliefs etc.[2] Irrespective of the jurisdictional scope of personal data, the social, moral and legal norm in most jurisdiction is that information deemed personal by public policy must remain outside the remit of government and public scrutiny.

In the United States, the main legislation that attempts to reconcile public security interests with the protection of personal data is the Cybersecurity Information Sharing Act (CISA) 2015.[3] A community reading of Section 102(2) and Section 104 of CISA provides that the primary objective of CISA is the monitoring of private information systems for the purpose of discerning security vulnerabilities. The concern over a lack of transparency in the use and deployment of surveillance systems under the Act is most visible in Section 104 of CISA, which provides that communication or personal information obtained by law enforcement agencies in furtherance of activities regulated under CISA is exempted from disclosure under local freedom of information laws. However, to balance public security interests with personal data protections, Section 105(4)(b) of CISA required that public interim guidelines relating to privacy and civil liberties, which shall govern the receipt, retention, and dissemination of personal information obtained by a Federal entity in connection with activities under the Act, be formulated.

In view of the above requirement, the US Government issued the Privacy and Civil Liberties Final Guidelines: Cyber-Security Information Sharing Act of 2015 on June 15, 2018, to reconcile public security interests with privacy protections. To underscore the challenge of balancing transparency while obtaining personal data with public security interests, the 2018 Privacy Guidelines made pursuant to CISA provide in Article 4 that an individual whose personal information is directly related to security threats will not have the ability to consent or be involved in the process of information collection, as this will counter the utility of the threat indicator. The fact that the 2018 Privacy Guideline dispenses with the need for consent, a key principle upon which the concept of privacy rights is formulated, clearly re-reinforces the perspective that public security interests and privacy protections are in collision. Furthermore, Article 2 of the 2018 Privacy Guidelines permits Federal law enforcement agents to target threat indicators for information that would qualify as personal information of individuals or that identifies an individual, so long as the information is relevant to the objective of CISA. Again, this provision evidences how surveillance systems must sometimes be permitted to encroach on privacy rights if the goal of public security is to be perpetually maintained.

However, to balance the need for the maintenance of public security with the protection of personal data, the 2018 Privacy Guidelines enumerate certain General Principles which focus on defining the scope of collection and usage of personal information and mandating certain transparency measures that must be put in place in the collection, sharing, and usage of such personal information. Suppose a federal agency receives a threat indicator from a private sector partner: logs that include IP addresses, usernames, and email addresses, plus content that reveals personal data about some users. The partner believes that some activity is associated with a foreign-based intrusion attempt that is attacking U.S. infrastructure. Under the Guidelines, the agency can accept and share this indicator because it includes some identifying personal information, but only if that information is directly related to the threat, for example, email used by attacker, logs showing attacker behavior, and any unnecessary data like usernames that aren't relevant, personal biographical info is removed. Before sharing, the agency must ensure it follows the privacy & civil liberties principles: check whether the information is verifiable, remove or mask non-relevant data, only distribute to relevant entities, document the sharing, ensure policies are in place, and maintain audit logs.

[1] PM Schwartz, 'Privacy and participation: personal information and public sector regulation in the United States' (1994) 80 Iowa Law Review, 553.
[2] DA Burton, M Yin, U Aceros and A Nurmikko, 'An implantable wireless neural interface for recording cortical circuit dynamics in moving primates' (2013) 10(2) Journal of Neural Engineering 1-25.
[3] Cyber-Security Information Sharing Act 2015 Act Pub. L. No.99. 508, 100 Stat.2242.

Transparency
A key general principle formulated under Article 4 of the 2018 Privacy Guidelines is the need for transparency in the collection, sharing, and dissemination of personal information obtained in furtherance of the objectives of CISA. The principle of transparency requires law enforcement agencies to be accountable to designated reporting lines about their receipt, retention, and use of personal information. It also requires them to periodically complete and publish privacy compliance documentation as a Privacy Impact Assessment (PIAs) as appropriate.[1]

Notification
Article 5.4 of the 2018 Privacy Guidelines provides that where personal information obtained has been used in an unauthorized manner and in contravention of CISA, the individual concerned must be notified promptly, and the notice shall contain the information used in contravention of CISA and any other relevant information.[2]

Purpose Specification
Article 5.5 of the 2018 Privacy Guidelines authorizes Federal entities to receive, retain, use, and disseminate personal information received as threat indicators for only authorized purposes. The authorized purposes include security purposes, identifying threats or security vulnerabilities, and for the purpose of responding to, investigating, or prosecuting an offense arising out of a threat.[3]

Sanctions
Under Article 6 of the 2018 Privacy Guidelines, sanctions are to be implemented for activities of officers, employees, or agents of the federal government that are knowingly and willfully in contravention of the privacy protection guidelines.[4] Such sanctions include training, loss of access to information, loss of access to security clearance, and termination of employment, depending on the severity of misuse.

Destruction of Information
Article 5.2 of the 2018 Guidelines mandates Federal entities to destroy in a timely manner, personal information of individuals that is known not to be directly related to any of the objectives of CISA.

Accountability and Audit
The final guiding principle on privacy protection extracted from Article 8 of the 2018 Privacy Guidelines is the requirement that Federal entities be accountable for complying with privacy and civil liberties guidelines and must ensure that audit capabilities are put in place around the receipt, retention, use, and dissemination of personal information received as security threat indicators under CISA.[5] The audit capabilities required to be maintained by Federal entities include:
(i) The number of threat indicators or defensive measures shared, and the process developed
(ii) An assessment of any personal information shared, which was not directly related to a security threat and was thus, in contravention of CISA and the 2018 Guidelines
(iii) The number of times personal information obtained was used by a Federal entity to prosecute an offense
(iv) Quantitative and qualitative assessment of the effect that sharing personal information has on privacy and civil liberties, including the number of notices issued with respect to a failure to remove personal information not directly related to a security threat
(v) The adequacy of any step taken by the government to reduce any adverse effect from activities carried out under the 2018 Privacy Guidelines.

While the 2018 Privacy guidelines attempts to reconcile public security interests with personal data protection by defining the scope of collection and usage of personal information and mandating certain transparency and accountability measures that must be put in place in the collection, sharing and usage of such personal information, there remains a few gaps and limitations in the guidelines that still need to be addressed to effectively balance both interests.

[1] Article 4 of the Privacy and Civil Liberties Final Guidelines: Cyber security Information Sharing Act of 2015, June 15, 2018.
[2] Section 103(b)(I)(f) of the Cyber-Security Information Sharing Act 2015.
[3] Section 105(d) of the Cyber-Security Information Sharing Act 2015.
[4] Section 105(3)(c) of the Cyber-Security Information Sharing Act 2015.
[5] Section 105(a)(3)(c) of the Cyber-Security Information Sharing Act 2015.

First, Article 9 of the 2018 Guideline requires a 2-year periodic review of the measures and processes contained in the guidelines for the balancing of public security interests with privacy protections to ensure that they remain up to date. However, as technology continues to evolve at a rapid pace, a 2-year process guideline will be inadequate in keeping pace with technological advancement, which may contain innovative features that allow the collection of personal data in such a way that evades the processes and measures contained in an outdated guideline. For example, since the last guideline was issued, there has been a proliferation in the development of advanced Artificial Intelligence capabilities that allow for the analysis of vast quantities of data from public and private sources, potentially revealing personal information that individuals have not consented to share. Technological advancements such as this will inevitably lead to legal and regulatory gaps that may leave individuals vulnerable to privacy violations.[1] In view of this, it is suggested that the 2-year periodic review mandated under the 2018 Privacy Guidelines be reduced to a 6-month periodic review to allow for better up-to-date processes and measures reconciling public security interests with privacy rights.

Second, the highest form of sanctions under the 2018 Privacy Guidelines for officers, employees, or agents of the Federal Government who "willfully" and "knowingly" misuse private information in contravention of CISA is termination of employment. It can be argued that termination of employment might not be a sufficient deterren,t especially in a modern world plagued with leakage of classified information in furtherance of political objectives.[2] For example, in the last decade, the world has witnessed the wilful misuse and leakage of classified information by Federal officers, such as the Edward Snowden Leaks, the Pentagon Papers Leaks, the Iraq War Logs leaks, the Robert Hanssen's Sale of Classified Information, and the Ukrainian War Leaks.[3] It is hard to imagine that in each of the above cases, the officers concerned did not understand that they would lose their jobs and yet they still went ahead with it. This indicates that the misuse of classified informatio,n such as personal data, is a calculated risk, and the fear of termination of employment is not a sufficient deterrence for Federal officers motivated by political or other objectives to misuse such personal information. Consequently, it is suggested that criminal sanctions should be warranted where appropriate, for "willful" and "intentional" misuse of personal information in contravention of the 2018 Privacy Guidelines and CISA. Such criminal sanctions will serve as a more effective deterrent against the violation of privacy protections.

CONCLUSION

This article highlighted the importance and challenges of balancing public security interests with the protection of personal data in the age of surveillance. It also explored the legal provisions, attempting to reconcile both interests and the gaps and limitations contained in the legal provisions. Finally, it suggested ways in which the gaps and limitations in the legal provisions can be bridged.

Public security and privacy protections are two interests that will inevitably collide from time to time. However, with a continuously updated legal and regulatory guideline defining the scope of collection and usage of personal information and mandating certain transparency and accountability measures, both interests can be consistently balanced for the purpose of maintaining public security without compromising privacy protections.

To effectively implement these necessary legal updates, a multi-stakeholder oversight body must be established. This body should comprise legal scholars, technology experts, privacy advocates, and public security officials. Its mandate would be to perform regular, independent audits of data collection practices to ensure compliance with the principles of necessity and proportionality, and to proactively recommend legislative amendments to keep pace with rapid technological advancements such as AI-driven surveillance. Crucially, the legal framework must include a mandatory requirement for annual judicial review of the necessity of ongoing surveillance programs, ensuring that any intrusion upon fundamental privacy rights is temporary, strictly limited, and demonstrably essential to public safety.

[1] L Hickman and C Martin, 'The FTCs Unfulfilled promise: Revisiting the effectiveness of the FTC's Data Security Enforcement Program' (2022) 83(1) Ohio State Law Journal 73-132.
[2] P Beaumont, 'US Intelligence leak: What do we know about 'top secret' documents?' *The Guardian* (11 April 2023) <https://www.theguardian.com/world/2023/apr/11/us-intelligence-leak-what-do-we-know-about-top-secret-documents> accessed 11 July 2025.
[3] S Neukam, 'The 5 biggest US Intelligence Leaks', *The Hill* (04 October 2023) <https://www.theguardian.com/world/2023/apr/11/us-intelligence-leak-what-do-we-know-about-top-secret-documents> accessed 11 July 2025.

REFERENCES

Acquisti A and Grosslags J, 'Economics and Privacy' (2013) 51(2) Journal of Economic Literature 1-32.

Ajunwa I, Crawford K, and Schultz J, 'Limitless worker surveillance' (2017) 105(3) California Law Review 735-76.

Allahrakha N, 'Balancing Cyber-security and Privacy: Legal and Ethical Considerations in the Digital Age' (2023) 4(2) Legal Issues in the Digital Age, 78-121.

Beaumont P, 'US Intelligence leak: What do we know about 'top secret' documents?' *The Guardian* (11 April 2023) <https://www.theguardian.com/world/2023/apr/11/us-intelligence-leak-what-do-we-know-about-top-secret-documents> accessed 11 July 2025.

Burton DA, Yin M, Aceros U and Nurmikko A, 'An implantable wireless neural interface for recording cortical circuit dynamics in moving primates' (2013) 10(2) Journal of Neural Engineering 1-25.

Green M, 'Balancing privacy and protection: the legal debates over drone surveillance' (2021) 134(4) 2023-41.

Greenwald G, 'The National Security Agency in the age of Cyber Surveillance' (2021) 237 Foreign Policy 78-86.

Harcourt B.E, 'Exposed: Desire and disobedience in the digital age' (2024) 1 Journal of Data Science 1-8.

Hickman L and Martin C, 'The FTC's Unfulfilled Promise: Revisiting the effectiveness of the FTC's Data Security Enforcement Program' (2022) 83(1) Ohio State Law Journal 73-132.

Kshetri N, 'A Global Analysis of Data Breaches: focus on sensitive data theft' (2021) 133 Journal of Business Research, 326-334.

Kuchler H, 'Cambridge Analytica case highlights Facebook's data riches' *Financial Times* (San Francisco, 19 March 2018) <https://www.ft.com/content/c1f326a4-2b24-11e8-9b4b-bc4b9f08f381> accessed 9 July 2025.

Luiijf E 'Cyber-security and resilience: what are we talking about? In *Cyber Security: From Technology to Society* (Cham: Springer, 2019).

Neukam S, 'The 5 biggest US Intelligence Leaks', *The Hill* (04 October 2023) <https://www.theguardian.com/world/2023/apr/11/us-intelligence-leak-what-do-we-know-about-top-secret-documents> accessed 11 July 2025.

Norris C and Mchill M, *CCTV in Britain: a social and political perspective on the emergence and development of public space surveillance* (University of Oxford Press, 2015).

O'Harrow R, 'Privacy vs. Security: A False Dichotomy' (2017) 9(1) Journal of National Security Law & Policy 95-113.

Power DJ., Heavin C and O'Connor Y, 'Balancing privacy rights and surveillance analytics: a decision process guide' (2021) 4:2 Journal of Business Analytics 155-170.

Roberts L, 'Employee privacy monitoring: the pros and cons of workplace surveillance' 2021 160(2) Journal of Business Ethics 635-50.

Rosenzweig P 'Balancing Privacy and Security: The Ethical Dimension' in J Quigley and D Molnar (eds), *Routledge Handbook of Science, Technology and Society* (L. Routledge 2015).

Schwartz PM, 'Privacy and participation: personal information and public sector regulation in the United States' (1994) 80 Iowa Law Review, 553.

Singer P and Tushman M, *Understanding Cyber-Security and the Implications for National Security* (N.Y. Columbia University Press, 2021).

Yoo C, 'Cyber-security and freedom on the internet' (2015) 38(1) Harvard Journal of Law & Policy 129-137.

Wheatley MC, 'Ethics of Surveillance Technologies: Balancing Privacy and Security in a Digital Age' 2024 1 Journal of Data Science 1-8.

Zuboff S, 'Big other: surveillance capitalism and the prospects of an information civilization' (2015) 30(1) Journal of Information Technology, 75-89.