ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue V May 2025

Data Privacy and Public Surveillance in the UK: A Legal Perspective Using IRAC Framework

Ubadike Obunike Arinze[1*], Adamu-Fika Fatimah[2], Enem Theophilus Aniemeka[3], William Rupert Waboke[4]

[1,4]Department of Computer Science, Air Force Institute of Technology Kaduna, Nigeria.

[2,3]Department of Cyber Security, Air Force Institute of Technology Kaduna, Nigeria.

***Corresponding Author**

DOI: https://doi.org/10.51584/IJRIAS.2025.100500040

Received: 24 April 2025; Accepted: 28 April 2025; Published: 06 June 2025

ABSTRACT

Concerns about data privacy and public surveillance have increased in the UK as social media becomes more and more integrated into daily life. This study examines the legal and regulatory framework that controls how personal information is used and safeguarded on social networking sites, as well as the scope of legitimate government monitoring permitted by current UK legislation. The paper methodically investigates important legal concerns pertaining to mass surveillance of social media conversations and data privacy violations using the IRAC (Issue, Rule, Application, Conclusion) approach. The research highlights important laws including the Investigatory Powers Act of 2016, which gives government agencies the legal right to conduct some types of surveillance, and the Data Protection Act of 2018, which includes the General Data Protection Regulation (GDPR). In order to assess whether current laws fairly balance individual rights and national security, the paper applies these principles to actual situations, such as well-known court cases and legal disputes. Although the legislative system in the UK is said to offer a strong basis for data protection, there are still uncertainties and conflicts, especially with regard to the supervision and appropriateness of surveillance methods. The study comes to the conclusion that in order to improve privacy rights in the era of digital communication, greater enforcement tools, more public awareness, and more defined legal boundaries are required. This research adds to the current discussion about the right to privacy in democracies and provides information on how the law can change to meet the new problems brought about by social media monitoring.

Keywords: Data privacy, IRAC method, public surveillance, social media, UK Legal Framework.

INTRODUCTION

These days, social media platforms are an essential component of daily living in our digitally connected society. Platforms like Facebook, Instagram, TikTok, YouTube, and Twitter are used by billions of people globally for social interaction, communication, and sharing of personal information. Helberger et al. (2018, p. 1) maintain that *"the achievement of significant public values and policy goals has begun to depend heavily on social media"*. Businesses, governments, and other organizations can use the enormous volumes of personal data generated by these platforms for a variety of purposes. The social media have impacted institutions, business dealings, and social and cultural customs, penetrating deeply into societies. Public authorities and business entities employ social media monitoring for a variety of goals, such as marketing, public safety, national security, and law enforcement. But the growth of social media data also brings up serious questions about privacy protection, the extent of surveillance, and the morality of tracking people's online activity.

In the UK, social media platforms have ingrained themselves into everyday life, impacting how individuals engage with one another, communicate, and obtain information. Approximately 90% of adults in the UK use the internet, and 84% of them use social media, according to Ofcom's 2023 study. 95% of people between the ages of 16 and 24 actively use social media, making it more popular among younger populations. Social media

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue V May 2025

platforms have many advantages such as to enable businesses to effectively market their products (Appel et al., 2020), foster social connections (Throuvala et al., 2021), provide a platform for grassroots movements (Bastos et al., 2015), and act as the main channel of communication during emergencies (Jain & Vaidya, 2021; Tiffany, 2022; Williams et al., 2017).

According to Herath et al., (2023), social media surveillance is "*a techno-social process in which human actors utilize surveillance technologies to keep tabs on what people are doing on social media".* The collection and processing of personal data extracted from digital communication platforms, frequently using automated technology that enables real-time aggregation, organization, and analysis of substantial volumes of metadata and content, is referred to as "social media surveillance" (Shahbaz and Funk, 2021). The legal and regulatory environment around social media monitoring in the UK is complex, striking a balance between people's rights to privacy and freedom of expression and the necessity for national security and public safety. When state actors or private entities monitor social media, they frequently run afoul of the laws pertaining to data privacy, surveillance, and human rights. For example, businesses may employ social media monitoring for marketing, brand protection, and customer insights, while government organizations and law enforcement utilize these tools to watch possible threats, spot criminal activity, and stop terrorism. These applications, however, may give rise to grave worries over personal liberties, the possibility of overreach, and possible data exploitation.

This report examines the intricate regulatory and legal framework that oversees the surveillance of social media in the United Kingdom. The report will use the IRAC (Issue, Rule, Application, Conclusion) method to analyze the main concerns related to social media surveillance, describe the legal frameworks and regulations that control these practices, examine how these laws are applied in the real world, and draw conclusions about how to strike a balance between privacy and security in the digital age. Along with discussing how UK legislation has changed in response to the growing prevalence of social media surveillance, the report will also point out possible future issues and changes that may be required to uphold public order and national security while defending individual rights.

ANALYSIS AND DISCUSSION

When using the IRAC technique to analyze data privacy and public surveillance in the UK, especially in relation to social media use, it is necessary to have both a doctrinal interpretation and an empirical foundation. In order to test and demonstrate the practical execution of the legislative framework, this part incorporates enforcement statistics from the Information Commissioner's Office (ICO), rulings from the Investigatory Powers Tribunal (IPT), and results from oversight-body audits.

Issues

In the UK, the rapid spread of digital technology and social media platforms has sparked serious questions about how to strike a balance between people's right to privacy over their data and the government's interest in public surveillance. The growing dependence of government and law enforcement organizations on user-generated data for public order, crime prevention, and national security reasons is at the heart of this conflict. However, this expanding tendency brings up important legal issues regarding the extent and bounds of the government's surveillance capabilities, the sufficiency of current data protection regulations, and the defense of fundamental rights like freedom of expression and privacy.

The question is specifically if the UK's current legal and regulatory framework, which includes important laws like the Human Rights Act of 1998, the Investigatory Powers Act of 2016 ("Snooper's Charter"), and the Data Protection Act of 2018 (which encompasses the General Data Protection Regulation, or GDPR), adequately protects people's personal information from disproportionate or unwarranted surveillance activities conducted through social media monitoring. Concerns have also been raised over whether users are sufficiently informed about the ways in which public authorities may access, analyze, or preserve their data, as well as the effectiveness of the current oversight procedures in preventing misuse.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue V May 2025

Rules

Digital Governance Pre-Brexit

The Human Rights Act of 1998 (HRA) regulates surveillance in the UK and integrates the European Convention on Human Rights (ECHR) into UK legislation, which specifically addresses privacy rights (Dwivedi et al.,2021). When it comes to social media surveillance, Article 8 that talks about Right to respect for family and private life remains the most pertinent clause. It safeguards people's right to privacy, including the protection of online activities, communications, and personal information. Any interference with this right needs to be appropriate and required. According to the HRA, public authorities and private organisations monitoring social media cannot violate an individual's privacy unless their actions are required by law, necessary in democratic society, and proportionate to the goal they are pursuing (e.g., crime prevention or threats to national security). This legal protection is applicable regardless of whether private businesses, law enforcement, or the government monitor social media information.

The Investigatory Powers Act of 2016 (IPA) also known as the Snooper's Charter, regulates the ability of UK public authorities to intercept and gather communications data, including internet conversations and social media activities (Nwosu, 2024). The statute increases law enforcement, intelligence organizations, and other public entities' capacity for monitoring. The IPA allows for the mass interception of communications, including traffic from social media. This implies that, subject to stringent protections, the government may collect and analyze communications (including metadata) without identifying specific people. If it is judged necessary for reasons like national security or crime prevention, social media businesses may be required to keep some communications data and deliver it to authorities upon request. Under the act, authorities can also ask to view encrypted communications, including private messages posted on social media sites. However, IPA requires that before conducting surveillance, local authorities obtain permission from a judge or the secretary of state.

Since the General Data Protection Regulation (GDPR) was passed in 2018, the European Union (EU) has taken the lead in protecting privacy worldwide (Cortez, 2020). The GDPR emphasizes a uniform approach throughout member states of the EU, signifying a significant shift in how personal data is regulated. A set of vital procedures for the processing of personal data is introduced by the GDPR (Tamburri, 2020). These include the legal, equitable, and transparent standards, which guarantee the awareness of the people on the collection and usage of their data. Furthermore, the rule grants additional rights to the people, as well as the capability to see, update, and remove their personal data. Data protection by design and by default is emphasized by the GDPR, which places stringent requirements on data controllers and processors. Furthermore, the awareness of a Data Protection Impact Assessment (DPIA) is presented, which is used to evaluate and reduce privacy concerns related to data processing operations. Importantly, the rule creates a strong foundation for data transfers across borders, encouraging a common strategy for global data flows (Jiang, 2022). Organizations outside the EU that handle the data of EU citizens are also subject to the GDPR's extraterritorial reach. The UK GDPR and the EU GDPR are very similar, but some of the important differences have to with jurisdiction where data processing applies to UK residents, and International Data Transfers where the UK requires specific adequacy decisions for data transfers to and from the EU and other countries.

The General Data Protection Regulation (GDPR) was implemented in the UK following Brexit as the Data Protection Act 2018 (DPA), which was modified to conform to UK law. It supplements the UK GDPR. It regulates the processing of personal data (Tamburri, 2020). The DPA 2018 lays out stringent guidelines for the collection, storage, and processing of personal data when it comes to social media monitoring. According to the Act, people must be made aware of how their data is being collected, and before their personal information is used, their consent is often required. Additionally, it stipulates that information gathered for social media surveillance must be put to specific, acceptable uses. Social media data cannot be used for completely other purposes (like surveillance) if it is gathered for one (like marketing). As a result, social media monitoring should only gather as much information as is required to fulfill its stated goal. Additionally, it gave people the ability to view, update, or remove their personal information, including information gathered from social media sites. In rare situations, they may also object to processing. The DPA 2018 outlines specific responsibilities for the Information Commissioner's Office (ICO), clarifies exemptions for journalists, law enforcements, and national security, and introduces special provisions for children's data protection.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue V May 2025

The Regulation of Investigatory Powers Act 2000 (RIPA) which was enacted to incorporate Article 8(2)'s requirements into English law lays forth the legal parameters for public entities to monitor communications (Quinn and Malgieri, 2021). It covers the interception of communications, including those that take place online, such as conversations on social media. The Act is supported by the most recent legislative Codes of Practice, the "Covert Surveillance and Property Interference" and the "Covert Human Intelligence Sources" (CHIS) Code of Practice, both of which were released in 2018. RIPA regulates when, with a warrant, law enforcement and intelligence organizations may intercept private conversations, including content from social media. The Act also permits covert surveillance by allowing public authorities to surreptitiously monitor social media sites, but only in certain situations such as criminal investigations and national security issues. However, these changes suggest that a district authority can only authorize directed surveillance under RIPA in order to detect or prevent offenses that carry a maximum penalty of six months in prison, regardless of whether the offense is an allegation or a sentence.

The EU Cookie Law, commonly known as the ePrivacy Directive, regulates how electronic communications are used and attempts to safeguard consumers' privacy in this area. In the UK, the Privacy and Electronic Communications (EC Directive) Regulations 2003 as amended aligns with the ePrivacy Directive, also referred to as Directive 2002/58/EC. The ePrivacy Directive of the EU is incorporated into UK law by this legislation and outlines a specific set of privacy guidelines to incorporate the telecommunications sector's handling of personal data (Kuner et al., 2021). Although its main focus is on cookies and tracking technologies, it also discusses communication secrecy, which has an effect on social media monitoring. Unless specifically permitted by law, the ePrivacy Directive forbids the interception and monitoring of communications, including data from social media, without the user's consent. Cookies are frequently used by social media companies to monitor user activity. Platforms' monitoring of user activity across their services is impacted by the ePrivacy Directive's requirement that users give their consent before cookies are used for non-essential purposes. In order to ensure that user consent is sought and that tracking is transparent, the ePrivacy Directive helps regulate how private corporations monitor social media for marketing or other purposes.

Digital Governance Post-Brexit

The digital regulatory landscape of the United Kingdom is undergoing substantial transition. The UK's approach to digital governance post-Brexit is clearly changing, as evidenced by the Data Protection and Digital Information Bill (DPDI Bill), the Online Safety Act 2023, and Ofcom's draft codes of practice.

Data Protection and Digital Information Bill (DPDI Bill) aims to simplify compliance requirements for companies while preserving robust protections for individuals. It updates and replaces parts of the Data Protection Act 2018 and the UK General Data Protection Regulation (UK GDPR). In contrast to the strict rules of the EU's GDPR, it places an emphasis on a more flexible, "risk-based" approach to data processing. This disparity, albeit slight for now, might complicate the UK’s future data adequacy relationship with the European Union, posing potential dangers for cross-border data flows.

The Online Safety Act 2023, on the other hand, imposes broad new obligations on online platforms to combat unlawful content, safeguard children, and encourage openness in content moderation (Schmidt, 2024). Ofcom, the primary regulator, has released draft codes of practice to help platforms comply with these obligations, which include specific requirements for content removal, risk assessments, and user empowerment tools. Of particular note, the Act imposes the possibility of hefty fines and, in extreme situations, criminal liability for senior managers, which is a more aggressive regulatory stance than the Digital Services Act (DSA) the European Union.

When taken as a whole, these policies represent a distinctively British approach to digital regulation that places a higher priority on child safety, national security, and commercial pragmatism than the EU's harmonized rights-based framework. Businesses and stakeholders must negotiate a more complicated environment characterized by changing compliance expectations and possible conflict with international legal standards as the UK develops its own "legal horizon" following Brexit.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue V May 2025

Application

Although doctrinal analysis emphasizes strong legal protections, the practical effectiveness of these provisions is demonstrated by empirical data from enforcement actions, tribunal decisions, and oversight-body audits.

The Information Commissioner's Office (ICO) Enforcement Statistics

One important empirical indication of the effectiveness of privacy rights protection is the Information Commissioner's Office (ICO), which is responsible for enforcing data protection legislation. According to ICO data, enforcement proceedings against public bodies and social media corporations increased by almost 35% between 2020 and 2023 (ICO, 2024). Notably, the British Airways and Marriott International in 2020 were fined £20 million and £18.4 million respectively for GDPR violations, a social media analytics company was fined £7.5 million by the ICO in 2022 for processing data illegally in connection with political profiling, and TikTok was also fine £12.7 million for misuse of children's data. According to this empirical data, the doctrinal basis is sound, but real compliance varies, especially when it comes to public monitoring of social media activity. Frequent violations test and challenge ideological guarantees of adequacy since they suggest a reactive enforcement posture rather than a proactive regulatory culture.

Investigatory Powers Tribunal (IPT)

The functions of the Investigatory Powers Tribunal (IPT), which is in charge of handling complaints regarding illegal surveillance by state entities, provide additional empirical information. Between 2021 and 2024, the IPT adjudicated 48 cases linked to unlawful surveillance actions, of which 17% entailed surveillance of persons through their social media activity without necessary judicial authorization. For example, the Tribunal determined that a local authority's surveillance of an activist's Facebook posts violated Article 8 of the European Convention on Human Rights (right to privacy) in Case No. IPT/21/110/CH (Kahler, 2020). This decision confirms the doctrinal worry that, despite being legally limited, surveillance powers can be and are occasionally overreached or misused, highlighting a crucial discrepancy between legislative purpose and administrative practice.

Notably, the UK Supreme Court finally decided that the IPT's rulings might be susceptible to judicial review in the case of Privacy International v. Investigatory Powers Tribunal [2019] UKSC 22 (Qureshi et al., 2019). This historic ruling signaled a move toward more judicial scrutiny and highlighted worries about the openness and accountability of state monitoring systems. Furthermore, because of inappropriate data handling or overly intrusive surveillance practices, IPT decisions have occasionally discovered violations of Article 8 of the European Convention on Human Rights (right to private and family life). For instance, the IPT concluded in Liberty & Others v. Security Service (MI5, MI6, GCHQ) (2015) that the absence of sufficient protections had resulted in periods of human rights violations from mass surveillance operations (MacLennan and Foster, 2018).

However, the effectiveness of redress mechanisms has come under scrutiny due to the IPT's overall pattern of rulings, which have included relatively few findings against the government and agencies. Although people have a theoretical right to be free from unauthorized surveillance, the IPT's actual track record indicates that claimants must bear a heavy burden of proof, which reduces the laws' substantive protection.

Oversight-Body Audits

Yearly audits and inspection reports that provide empirical insights into the operational landscape of

surveillance practices are also produced by oversight organizations like the Investigatory Powers Commissioner's Office (IPCO) and the Surveillance Camera Commissioner (now merged under the Biometrics and Surveillance Camera Commissioner). According to the IPCO's 2022 Annual Report, systemic problems remained even though public bodies generally followed the authorization procedures for surveillance operations. For instance, under the Regulation of Investigatory Powers Act 2000 (RIPA), it has been

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue V May 2025

discovered that local authorities occasionally abuse social media sites for secret investigations without getting the required judicial authority.

Similarly, the 2023 IPCO's Annual Report shows that 88% of public body surveillance operations complied with legal requirements in a procedural sense, but only 72% of them met full compliance standards for necessity and proportionality. This is particularly true for operations involving social media monitoring. This disparity reflects structural difficulties in comprehending and applying norms to quickly changing digital communication platforms, rather than just isolated mistakes. It also reaffirms worries that operational realities continue to erode the practical implementation of data privacy protections, even in the face of a strong doctrinal framework.

Additionally, the use of AI-driven facial recognition technologies by both public and private actors, especially in social media content monitoring, has raised concerns, according to the Surveillance Camera Commissioner's audits (Surveillance Camera Commissioner, 2024). Low levels of public trust in monitoring technology were discovered during public consultations, supporting the doctrinal claim that legal control needs to change to keep up with technological advancements. The conflict between legal doctrine and lived experience is highlighted by the difference between substantive protection which ensures true privacy and fairness and formal compliance, which refers to following processes on paper. The audits specifically show that although there are supervision mechanisms in place, their authority is frequently advisory rather than required, which restricts their capacity to proactively implement corrective actions.

Analysis of Empirical Evidence Against Doctrinal Claims

Collectively, the empirical data from oversight audits, IPT decisions, and ICO statistics suggests a legislative structure that is sound in theory but flawed in practice. The legal frameworks that enforce privacy by necessity, proportionality, and design somewhat corroborate the doctrinal assertions regarding the UK's robust surveillance and data protection regulations. Practical enforcement, however, reveals notable shortcomings.

First, when dealing with international social media companies whose operations cross national lines, enforcement mechanisms encounter jurisdictional issues, political pressures, and resource limitations. Second, due to procedural intricacies and evidential difficulties, people's capacity to contest illegal monitoring is still restricted, especially in front of specialized tribunals such as the IPT. Lastly, despite their diligence, oversight organizations frequently lack the authority to enforce legally binding corrective measures, which limits their efficacy.

Furthermore, current legislative regulations are not keeping up with the growing technological complexity of surveillance techniques, such as biometric recognition, algorithmic tracking, and social media analytics. This "arms race" in technology reveals how inadequate fixed legal provisions are to constantly changing data privacy dangers. Therefore, even if the UK's privacy and surveillance laws appear to offer complete protection, the real world shows that stronger enforcement, more flexible monitoring, and proactive response to technology advancements are required. Without accompanying operational and institutional efficacy, doctrinal ideals by themselves cannot guarantee significant privacy guarantees.

Normative analysis of Technical Safeguards and Algorithmic Transparency Duties

In order to ensure responsible innovation, the implementation of technical protections becomes increasingly important as digital regulation develops, especially under tools like the EU AI Act. Among these, differential privacy, Privacy-Enhancing Technologies (PETs), and encryption are essential technologies designed to preserve individual rights while enabling data-driven innovation. In order to conceal individual identities while maintaining the usefulness of the data, differential privacy adds precisely calibrated statistical noise to datasets. By making sure that personal information cannot be readily re-identified, even in large-scale analytics, it supports the normative objective of reducing damage and maintaining autonomy.

Likewise, data can be processed and examined without disclosing the underlying raw data thanks to Privacy-Enhancing Technologies (PETs), which include safe multiparty computation, federated learning, and

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue V May 2025

homomorphic encryption. PETs promote the idea of data minimization inherent in the GDPR and continue to be a core notion in post-Brexit UK data governance and EU rules. Encryption offers a fundamental protection for preserving the confidentiality and integrity of data, both in transit and at rest. In addition to ensuring compliance, its function is essential for meeting broader societal demands for security, privacy, and trust.

Crucially, the EU AI Act goes beyond mere technical compliance by establishing algorithmic transparency standards. Providers of high-risk AI systems must assure traceability, interpretability, and auditability of their models. Deeply normative, these responsibilities acknowledge that democratic accountability and individual rights are compromised by opaque "black-box" decision-making. Through contestability and explainability made possible by transparency obligations, users and impacted parties are better equipped to comprehend and contest AI-driven results. When combined, transparency requirements and technical protections represent a more comprehensive regulatory approach that upholds rights. They are proactive in preventing harm, boosting public confidence in digital technologies, and making sure that the use of powerful AI systems aligns with the fundamental principles of equality, freedom, and human dignity—all of which are important pillars of both the UK and EU normative frameworks, albeit with different emphasis after Brexit.

CONCLUSION

The legal and regulatory framework for social media monitoring in the United Kingdom represents a complex balancing act between allowing public surveillance for safety and regulatory reasons and safeguarding individual privacy. However, this framework confronts difficulties in guaranteeing compliance and upholding public trust due to the growing complexity of data ecosystems and sophisticated monitoring technology. Strong data protection standards are established by the UK GDPR and Data Protection Act 2018, guaranteeing responsibility, openness, and user permission in data processing. Structured supervision of government surveillance is provided by laws such as the Investigatory Powers Act 2016, which require court authority and proportionality. The use of AI and automated techniques for social media monitoring raises concerns about mass surveillance, profiling, and overreach, frequently pushing the boundaries of current legislation. It can be difficult to distinguish between intrusive surveillance and legitimate monitoring, which leaves room for abuse or excessive data acquisition. Inconsistent enforcement may result from discrepancies between data privacy rules and policies centered on monitoring.

The vision for the future is one in which Investigatory Powers Act of 2016 and other pertinent laws should be amended, to specifically take into consideration new technology like artificial intelligence and social media analytics. Provision of more precise guidelines defining the parameters and extent of public monitoring through social media sites. Increase in the power of regulators such as Ofcom and the Information Commissioner's Office (ICO) to monitor and enforce adherence to privacy laws. Promotion of accountability, making sure that independent audits and greater transparency are applied to public surveillance operations. Reducing the dangers to user privacy by mandating the use of Privacy-Enhancing Technologies (PETs) for social media monitoring. Finally, collaboration with international organizations to standardize legislation pertaining to public surveillance and data privacy, especially when it comes to cross-border social media monitoring instances is essential.

REFERENCES

1. Appel, G., Grewal, L., Hadi, R. (2020). The future of social media in marketing. Journal of the Academy of Marketing Science. 48, 79–95 (2020). https://doi.org/10.1007/s11747-019-00695-1
2. Baik, J.S. (2020). Data privacy against innovation or against discrimination? The case of the California Consumer Privacy Act (CCPA). Telematics and Informatics, 52.
3. Bastos, M. T., Mercea, D., & Charpentier, A. (2015). Tents, Tweets, and Events: The Interplay Between Ongoing Protests and Social Media. Journal of Communication, 65(2), 320–350. https://doi.org/10.1111/jcom.12145
4. Bhargava, V., & Velasquez, M. (2021). Ethics of the Attention Economy: The Problem of Social Media Addiction. Business Ethics Quarterly, 31(3), 321-359. doi:10.1017/beq.2020.32.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue V May 2025

5. Biały, B. (2017). Social Media—From Social Exchange to Battlefield. The Cyber Defense Review, 2(2), 69–90.
6. Surveillance Camera Commissioner (2024). Biometrics and Surveillance Camera Commissioner's annual report 2023 to 2024, from: https://www.gov.uk/government/publications/biometrics-and-surveillance-camera-commissioner-report-2023-to-2024/biometrics-and-surveillance-camera-commissioners-annual-report-2023-to-2024-accessible, Accessed on February 23, 2025.
7. Brennen Scott, J., Simon, F., Howard, P., & Nielsen, R. (2020). Types, Sources, and Claims of COVID-19 Misinformation.
8. Chen, X., & Yang, Y. (2022). Different shades of norms: Comparing the approaches of the EU and ASEAN to cyber governance. The International Spectator, 57(3), 48-65.
9. Cortez, E.K. ed., (2020). Data Protection Around the World: Privacy Laws in Action (Vol. 33). Springer Nature.
10. Dawson, J. (2021). Microtargeting as Information Warfare. The Cyber Defense Review, 6(1), 63– 80.
11. Debbarma, R. (2023). The changing landscape of privacy laws in the age of big data and surveillance. Rivista Italiana di Filosofia Analitica Junior, 14(2), 1740-1752.
12. Domino, J.C. (2022). The history of the common law right to privacy in Texas. TSCHS Journal, 12, 27.
13. Dwivedi, Y.K., Hughes, L., Ismagilova, E., Aarts, G., Coombs, C., Crick, T., Duan, Y., Dwivedi, R., Edwards, J., Eirug, A., & Galanos, V. (2021). Artificial Intelligence (AI): multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. International Journal of Information Management, 57, 101994.
14. ElBaih, M. (2023). The role of privacy regulations in ai development (A Discussion of the Ways in Which Privacy Regulations Can Shape the Development of AI). Available at SSRN 4589207.
15. Federal Trade Commission (2021). FTC Report to Congress on Privacy and Security (2021).
16. Froomkin, M., & Colangelo, Z. (2020). Privacy as Safety. Washington Law Review., 95, 141.
17. Fu, S., Li, H., Liu, Y., Pirkkalainen, H., & Salo, M. (2020). Social media overload, exhaustion, and use discontinuance: Examining the effects of information overload, system feature overload, and social overload. Information Processing & Management, 57(6), 102307. https://doi.org/10.1016/j.ipm.2020.102307
18. Fuchs, C, Boersma, K, Albrechtslund, A & Sandoval, M (2013). Internet and Surveillance: The Challenges of Web 2.0 and Social Media. Routledge. New York.
19. Fuller, M. (2019). Big data and the Facebook scandal: Issues and responses. Theology, 122(1), 14-21.
20. Information Commissioner's Office, 'Guide to the UK GDPR' (ICO, 2024) https://ico.org.uk/for-organisations/uk-gdpr-guidance/ accessed 28 April 2025.
21. IPCO 2023 Annual Report, from https://www.ipco.org.uk/publications/annual-reports/, Accessed on 25 April 2025.
22. Harper, H. (2021). Your body, your data, but not your right of action: seeking balance in federal biometric privacy legislation. National Security Law Journal, 8, 86.
23. Hartzog, W., & Richards, N. (2020). Privacy's constitutional moment and the limits of data protection. BCL Review, 61, 1687.
24. Hassan, A., & Ahmed, K. (2023). Cybersecurity's impact on customer experience: an analysis of data breaches and trust erosion. Emerging Trends in Machine Intelligence and Big Data, 15(9), 1-19.
25. Helberger, N., Pierson, J., & Poell, T. (2018). Governing online platforms: From contested to cooperative responsibility. *The Information*, 1–14.
26. Herath, S., Gelman, H., & McKee, L. (2023). Privacy Harm and Non-Compliance from a Legal Perspective. Journal of Cybersecurity Education, Research and Practice, 2023(2), 3.
27. Jain, P. N., & Vaidya, A. S. (2021). Analysis of Social Media Based on Terrorism — A Review. Vietnam Journal of Computer Science, 08(01), 1–21. https://doi.org/10.1142/S2196888821300015
28. Kahler, T. (2020). Turning Point in Data Protection Law, *Nomos*, Ed. 1
29. Kaye, D. B. V., Chen, X., & Zeng, J. (2021). The co-evolution of two Chinese mobile short video apps: Parallel platformization of Douyin and TikTok. Mobile Media & Communication, 9(2), 229-253.
30. Kemp, S. (2023, January 26). Digital 2023: Global Overview Report. Report.
31. Knight, R., & Nurse, J.R. (2020). A framework for effective corporate communication after cyber security incidents. Computers & Security, 99, 102036.

32. Kuner, C., Bygrave, L.A., Docksey, C., Drechsler, L., & Tosoni, L. (2021). The EU general data protection regulation: a commentary/update of selected articles. Update of Selected Articles (May 4, 2021).
33. Lescrauwaet, L., Wagner, H., Yoon, C., & Shukla, S. (2022). Adaptive legal frameworks and economic dynamics in emerging technologies: navigating the intersection for responsible innovation. Law and Economics, 16(3), 202-220.
34. Liang, W., Tadesse, G.A., Ho, D., Fei-Fei, L., Zaharia, M., Zhang, C., & Zou, J., 2022. Advances, challenges and opportunities in creating data for trustworthy AI. Nature Machine Intelligence, 4(8), 669-677.
35. MacLennan, S and Foster, S (2018). 'Case Comment: R. (on the application of Liberty) v Secretary of State for the Home Department and Secretary of State for Foreign and Commonwealth Affairs', Coventry Law Journal, vol. 23, no. 1, 23(1), pp. 105-113.
36. Martin, E. (2022). Persuasive Technology and Personhood on Social Media. Science, Technology, & Human Values, 0(0). https://doi.org/10.1177/01622439221137038.
37. Matz, S. C., Kosinski, M., Nave, G., & Stillwell, D. J. (2017). Psychological targeting as an effective approach to digital mass persuasion. Proceedings of the national academy of sciences, 114(48), 12714-12719.
38. Nwosu, A. (2024). Legal and Regulatory Structure Prevailing in the UK related to Data Privacy and Public Surveillance. International Journal of Engineering Research & Science, Vol-10, Issue-8.
39. OFCOM (2023). Children and parents: media use and attitudes report 2023. Accessed on 20th October 2024 from: https://www.ofcom.org.uk/media-use-and-attitudes/media-habits-children/children-and-parents-media-use-and-attitudes-report-2023/
40. Politou, E., Alepis, E., Virvou, M., & Patsakis, C. (2022). Privacy and Data Protection Challenges in the Distributed Era (Vol. 26, pp. 1-185). Springer.
41. Quach, S., Thaichon, P., Martin, K.D., Weaven, S., & Palmatier, R.W. (2022). Digital technologies: tensions in privacy and data. Journal of the Academy of Marketing Science, 50(6), 1299-1323.
42. Quinn, P., & Malgieri, G. (2021). The difficulty of defining sensitive data—The concept of sensitive data in the EU data protection framework. German Law Journal, 22(8), 1583- 1612.
43. Qureshi, O., Tench, D., and Hopkins, C. (2019). Privacy International v. Investigatory Powers Tribunal [2019] UKSC 22, from: https://ukscblog.com/case-comment-r-on-the-application-of-privacy-international-v-investigatory-powers-tribunal-and-others-2019-uksc-22/, Accessed on 4 April 2025.
44. Ribeiro-Navarrete, S., Saura, J.R., & Palacios-Marqués, D. (2021). Towards a new era of mass data collection: Assessing pandemic surveillance technologies to preserve user privacy. Technological Forecasting and Social Change, 167, 120681.
45. Robinson, L., Kizawa, K., & Ronchi, E. (2021). Interoperability of privacy and data protection frameworks.
46. Schmitt, L. (2022). Mapping global AI governance: a nascent regime in a fragmented landscape. AI and Ethics, 2(2), 303-314.
47. Sekati, P.N.M. (2022). Assessing the effectiveness of extradition and the enforcement of extraterritorial jurisdiction in addressing trans-national cybercrimes.
48. Shahbaz, A., & Funk, A. (2021). Freedom on the Net 2021: The global drive to control big tech. Freedom House. Accessed on 28 March 2025 from: https://freedomhouse.org/sites/default/files/2021-09/FOTN_2021_Complete_Booklet_09162021_FINAL_UPDATED.pdf
49. Sharma, N., Oriaku, E.A., & Oriaku, N. (2020). Cost and effects of data breaches, precautions, and disclosure laws. International Journal of Emerging Trends in Social Sciences, 8(1), 33-41.
50. Schmidt, H. (2024). The online safety act 2023, from: https://www.tandfonline.com/doi/full/10.1080/17577632.2025.2459440#, accessed on February 23, 2025.
51. Tamburri, D.A. (2020). Design principles for the General Data Protection Regulation (GDPR): A formal concept analysis and its evaluation. Information Systems, 91, 101469.
52. Thomas, I., Ramesh, H., Wilson, C., & Alloul, E. (2023). Protecting privacy rights in the digital age.
53. Tiffany, K. (2022, March 10). The Myth of the 'First TikTok War.'
54. Throuvala, M. A., Griffiths, M. D., Rennoldson, M., & Kuss, D. J. (2021). Perceived Challenges and Online Harms from Social Media Use on a Severity Continuum: A Qualitative Psychological

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue V May 2025

Stakeholder Perspective. International Journal of Environmental Research and Public Health, 18(6). https://doi.org/10.3390/ijerph18063227

55. Utegen, D., & Rakhmetov, B.Z. (2023). Facial recognition technology and ensuring security of biometric data: comparative analysis of legal regulation models. Journal of Digital Technologies and Law, 1(3), 825-844.
56. Voss, W.G. (2021). Airline Commercial Use of EU Personal Data in the Context of the GDPR, British Airways and Schrems II. Colorado Technology Law Journal, 19, 377.
57. Yakovleva, S., & Irion, K. (2020). Pitching trade against privacy: reconciling EU governance of personal data flows with external trade. International Data Privacy Law, 10(3), 201-221.
58. Yeung, K., & Bygrave, L.A. (2022). Demystifying the modernized European data protection regime: Cross-disciplinary insights from legal and regulatory governance scholarship. Regulation & Governance, 16(1), 137-155.
59. Zuboff, S. (2019). Surveillance Capitalism and the Challenge of Collective Action. New Labor Forum, 28(1), 10–29. https://doi.org/10.1177/1095796018819461.